Guide to U.S. Anti-Money Laundering Requirements

Frequently Asked Questions

Fifth Edition

protiviti®
Risk & Business Consulting.
Internal Audit.

Powerful Insights. Proven Delivery.®

PREFACE

"The World Bank and International Monetary Fund estimate that global money laundering linked to corruption, criminal activity, and tax evasion constitutes about 3 to 5 percent of the world's gross domestic product — or between roughly $2.17 and $3.61 trillion a year."

Source: Malcolm Beith, July 19, 2012, *THE DAILY BEAST*

Protiviti is pleased to publish this fifth version of its *Guide to U.S. Anti-Money Laundering Requirements.* As with the previous editions of the Guide, this 2012 edition contains questions that have surfaced in our discussions with clients, attorneys, regulators and others, both in the United States and other markets. Over the years, the number of questions and answers included in the Guide has expanded from 140 in the initial version to more than 1,700 in this edition. This reflects both the complexity of the topic as well as the continuing evolution of regulatory expectations and industry-leading practices. Among the new and expanded information included in this version are questions and answers related to the intersection between anti-money laundering (AML) and the Foreign Account Tax Compliance Act (FATCA), expanded discussion of human trafficking, new and proposed regulations affecting nonbank mortgage lenders and housing government-sponsored enterprises (GSEs), recent changes to currency transaction reports (CTRs) and suspicious activity reports (SARs), updated Financial Action Task Force (FATF) recommendations and other international developments.

The Guide begins by addressing the major AML and sanction compliance requirements in the United States, namely the Bank Secrecy Act (BSA), the USA PATRIOT Act and the Office of Foreign Assets Control (OFAC) requirements. This is followed by sections on Know Your Customer (KYC), Risk Assessments (including an expanded discussion of high-risk customers), Transaction Monitoring and Investigations, Third-Party Reliance, AML Technology, Nonbank Financial Institutions and Nonfinancial Businesses, and International Perspectives and Initiatives. Also included in the resource sections at the back of the Guide are a glossary of useful acronyms and terms, a listing of key AML laws and regulations, and website addresses for some of the sources used to develop the questions and answers. Although the focus of the Guide is on U.S. requirements, we have included some highlights of international requirements and believe the Guide is instructive to companies outside of the United States because of the convergence of AML requirements and industry-leading practices across the globe.

It is important to note that this Guide is provided for general information only and focuses primarily on federal AML requirements; it is not intended to be legal analysis or advice, nor does it purport to address, except in a few instances, state or international money laundering requirements that may affect U.S. companies. Companies should seek the advice of legal counsel or other appropriate advisers on specific questions as they relate to their unique circumstances.

The development and maintenance of effective AML Compliance Programs remain dynamic. Accordingly, we expect many of the responses included in this booklet to continue to evolve.

Protiviti Inc.
November 2012

Acknowledgements

This booklet was developed through the collaborative effort of Protiviti's AML team, working under the direction of our colleague and former associate Karen L. Wilkes and Kaitlin Lemmo. The Protiviti AML team extends special thanks to Deborah Thoren-Peden and Christopher Wall of Pillsbury Winthrop Shaw Pittman LLP, who served as reviewers.

CONTENTS AT A GLANCE

TABLE OF CONTENTS 3

ANTI-MONEY LAUNDERING FUNDAMENTALS 10

BANK SECRECY ACT 26

USA PATRIOT ACT 77

OFFICE OF FOREIGN ASSETS CONTROL AND INTERNATIONAL GOVERNMENT SANCTIONS PROGRAMS 126

KNOW YOUR CUSTOMER, CUSTOMER DUE DILIGENCE AND ENHANCED DUE DILIGENCE 171

RISK ASSESSMENTS 183

TRANSACTION MONITORING, INVESTIGATIONS AND RED FLAGS 258

AML TECHNOLOGY 274

NONBANK FINANCIAL INSTITUTIONS AND NONFINANCIAL BUSINESSES 288

CONVERGENCE OF AML WITH FRAUD AND OTHER REGULATORY TOPICS 356

INTERNATIONAL PERSPECTIVES AND INITIATIVES 403

ACRONYMS AND GLOSSARY 442

KEY U.S. AML LAWS AND REGULATIONS AND USEFUL WEBSITES 462

ABOUT PROTIVITI 471

TABLE OF CONTENTS

ANTI-MONEY LAUNDERING FUNDAMENTALS 10

Key Definitions 10

Overview of U.S. AML Laws and Regulations 11

Overview of the U.S. Regulatory Framework 13
- Key U.S. Regulatory Authorities and Law Enforcement Agencies 13
- Financial Crimes Enforcement Network 18
- Enforcement Actions 20

AML Compliance Program 24

BANK SECRECY ACT 26

Overview of BSA 26

Reporting Requirements 27
- Currency Transaction Reports 27
  - CTR Basics 27
  - CTR Threshold and Aggregation 30
  - Completion of a CTR Form 32
  - CTR Exemptions 32
  - CTR Evasion 36
- Form 8300 37
  - Form 8300 Basics 37
  - Annual Notification 40
  - Filing of Form 8300 41
  - Reporting Suspicious Activity on Form 8300 42
- Suspicious Activity Reports 42
  - SAR Basics 43
  - SAR Filing Time Frame and Date of Initial Detection 47
  - Completion of a SAR 49
  - Confidentiality 51
  - Joint Filings of SARs 53
  - Safe Harbor 53
  - Monitoring and Terminating Relationships with SAR Subjects 54
  - Law Enforcement 55
  - SAR Trends 57
- Report of Foreign Bank and Financial Accounts 59
  - FBAR Basics 59
  - FBAR Filing 62
  - Recent Tax Scandals 63
- Report of International Transportation of Currency or Monetary Instruments 63
  - CMIR Basics 63
  - CMIR Filing 65

Recordkeeping Requirements 66
Funds Transfer Recordkeeping Requirement and the Travel Rule 67
Funds Transfer Recordkeeping Requirement and the Travel Rule Basics 67
Addresses and Abbreviations 70
Verification of Identity 71
Joint Party Transmittals and Aggregation 71
Retrievability 72
Cross-Border Electronic Transmittal of Funds 72
Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments 73

USA PATRIOT ACT 77

Overview of the USA PATRIOT Act 77

USA PATRIOT Act – Analysis of Key Sections 82
Section 311 – Special Measures 82
Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts 84
Overview 84
Due Diligence for Correspondent Accounts 87
Enhanced Due Diligence for Correspondent Accounts 89
Due Diligence for Private Banking Accounts 90
Enhanced Due Diligence for Private Banking Accounts 92
Senior Foreign Political Figure 92
Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks 94
Section 314 – Cooperative Efforts to Deter Money Laundering 95
Section 314(a) – Cooperation among Financial Institutions, Regulatory Authorities and Law Enforcement Authorities 95
Section 314(b) – Cooperation among Financial Institutions 98
Section 319 - Forfeiture of Funds in U.S. Interbank Accounts 100
Section 319(a) Requirements – Forfeiture from U.S. Interbank Accounts 100
Section 319(b) Requirements – Bank Records 101
Domestic Financial Institution Records (“120-Hour Rule”) 101
Foreign Bank Records 101
Foreign Bank Certifications 101
Section 325 – Concentration Accounts at Financial Institutions 103
Section 326 – Verification of Identification 104
Overview 104
Customer Defined 105
Account Defined 107
Verification 107
Updating CIP for Existing Customers 110
Record Retention 110
List Matching 111
Customer Notice 111
Third-Party Reliance 111
Section 352 – AML Program 112
Overview 112
Policies and Procedures 114
Designation of AML Compliance Officer and the AML Compliance Organization 115
AML Training 118
Independent Testing 120
Section 505 – Miscellaneous National Security Authorities 124

OFFICE OF FOREIGN ASSETS CONTROL AND INTERNATIONAL GOVERNMENT SANCTIONS PROGRAMS 126

OFAC Basics 126

Specially Designated Nationals and Blocked Persons List 130

Country- and Regime-Based Sanctions Programs 132

Non-Specially Designated Nationals Palestinian Council List 132

U-Turn Payments 132

Iranian Sanctions Overview 133
- Overview 133
- Comprehensive Iran Sanctions, Accountability and Divestment Act (CISADA) in 2010 and the Iran Threat Reduction and Syria Human Rights Act in 2012 137
  - Impact on Financial Institutions 140
- National Defense Authorization Act for Fiscal Year 2012 147
- Executive Orders and Other Sanctions 150

Screening Customers and Transactions 152
- Automated Clearing House Transactions and IATs 155
- Trade Finance Transactions 157

Blocking and Rejecting Transactions 158

Investigating Potential Matches 159

Reporting Requirements 160
- Blocked/Rejected Transaction Reports 160
- Licensing 161
- 602 Letter and Prepenalty Notice 164

Voluntary Disclosure 164

Independent Testing 165

Consequences of Noncompliance 166

Common Gaps and Challenges 167

Other U.S. and International Government Sanctions Programs 168

KNOW YOUR CUSTOMER, CUSTOMER DUE DILIGENCE AND ENHANCED DUE DILIGENCE 171

Overview 171

Beneficial Owners 177

Know Your Employee 180

Know Your Third Parties 180

RISK ASSESSMENTS 183

Overview 183

Enterprise-wide Risk Assessment 185

Business Line Risk Assessment 186

Customer Risk Assessment 187
- High-Risk Geographies 190
- High-Risk Customers 192
  - Nonresident Aliens and Foreign Persons 194

Professional Service Providers 196
Trust and Asset Management Services 197
Deposit Broker 200
Private Banking 201
Politically Exposed Persons 202
Foreign Embassy and Consulates 204
Business Entities: Shell Companies, Private Investment Companies 206
Correspondent Banking 208
Nonbank Financial Institutions 210
Charitable Organizations and Nongovernmental Organizations 211
Third-Party Payment Processors 212
Privately Owned Automated Teller Machines (ATMs) 216
High-Risk Products, Services and Transactions 217
Currency Transactions 217
Bulk Shipments of Currency 219
Funds Transfers 221
Automated Clearing House Transactions 223
Monetary Instruments 227
U.S. Dollar Drafts 228
Pouch Activity 229
Payable Through Accounts 231
Concentration Accounts 232
Electronic Banking 233
Online Banking 234
Automated Teller Machines 235
Remote Deposit Capture 235
Prepaid Access, Stored-Value and E-Cash 238
Trade Finance Activities 242
Lending Activities 249
Nondeposit Investment Products 251
Insurance Products 253
Administration of Customer Risk Assessment 254

Office of Foreign Assets Control Risk Assessment 255

TRANSACTION MONITORING, INVESTIGATIONS AND RED FLAGS 258

Monitoring Process 258

Roles and Responsibilities 260

Investigation Process 261

Suspicious Activity Red Flags 263
Account Opening Red Flags 264
Account Activity and Transaction Execution Red Flags 264
Currency Red Flags 265
Privately Owned ATM Red Flags 265
Bulk Shipments of Currency Red Flags 266
Branch and Vault Shipments Red Flags 266
Monetary Instrument Red Flags 266
U.S. Dollar Draft Red Flags 267
Wire Transfer Red Flags 267
Certificate of Deposit Red Flags 268
Safe Deposit Box Red Flags 268
Lending Red Flags 268
Mortgage and Real Estate Red Flags 268
Credit Card Red Flags 268

Trade Finance Red Flags 269
Capital Market Products Red Flags 269
Insurance Products Red Flags 270
Casino Red Flags 270
Retail Red Flags 270
Consumer Products Red Flags 271
Human Trafficking 271
Elder Financial Abuse 272
Informal Value Transfer System (IVTS) Red Flags 272
Terrorist Financing Red Flags 273
Employee Red Flags 273

AML TECHNOLOGY 274

Overview 274

Suspicious Transaction Monitoring and Suspicious Activity Report Filing Software 276

Case Management Software 282

Large Currency Transaction Monitoring and Currency Transaction Report Filing Software 283

Customer Information Database and Customer Risk Assessment Software 283

Customer Verification Software 284

List Providers 285

Interdiction Software 286

Training Software 287

NONBANK FINANCIAL INSTITUTIONS AND NONFINANCIAL BUSINESSES 288

Nonbank Financial Institutions 288
Money Services Businesses 290
Definition 290
Issuers and Sellers of Money Orders and Traveler's Checks 291
Check Cashers 291
Dealer in Foreign Exchange 292
Providers or Sellers of Prepaid Access 292
Money Transmitters 293
Guidance on the Applicability of the Definition of Money Services Businesses 294
Key AML and Sanction Requirements 295
Registration 299
Agents 301
Informal Value Transfer Systems 303
Definition 303
Black Market Peso Exchange 304
Reintegro 305
Providers and Sellers of Prepaid Access 305
Definitions 305
Key AML and Sanction Requirements 311
Broker-Dealers 314
Definition 314
Key AML and Sanction Requirements 316
Futures Commission Merchants and Introducing Brokers 320
Definition 320
Key AML and Sanction Requirements 321
Commodity Trading Advisers 323
Definition 323

Key AML and Sanction Requirements 323
Mutual Funds 324
Definition 324
Key AML and Sanction Requirements 325
Insurance Companies 326
Definition 326
Key AML and Sanction Requirements 327
Casinos or Card Clubs 329
Definition 329
Key AML and Sanction Requirements 330
Operators of Credit Card Systems 335
Definition 335
Key AML and Sanction Requirements 336
Dealers in Precious Metals, Stones or Jewels 337
Definition 337
Key AML and Sanction Requirements 338
Investment Advisers and Unregistered Investment Companies 339
Definition 339
Key AML and Sanction Requirements 340
Persons Involved in Real Estate Settlements and Closings 342
Definition 342
Key AML and Sanction Requirements 343
Nonbank Residential Mortgage Lenders and Originators 344
Definition 344
Key AML and Sanction Requirements 346
Housing Government Sponsored Enterprises 349
Definition 349
Key AML and Sanction Requirements 350

Nonfinancial Businesses 353
Definition 353
Key AML and Sanction Requirements 354

CONVERGENCE OF AML WITH FRAUD AND OTHER REGULATORY TOPICS 356

AML and Anti-Fraud Programs 356

CIP vs. Identity Theft Prevention Program 358

Mortgage Fraud 362

Unlawful Internet Gambling Enforcement Act 367

Human Trafficking 374

Elder Financial Abuse 386

Foreign Account Tax Compliance Act 391
FATCA Basics 391
Participating Foreign Financial Institutions 395
FFI Agreement 395
Registration 396
Due Diligence 397
Identification of U.S. Account holders 397
Pre-Existing Individual Accounts 397
New Individual Accounts 398
Pre-Existing Entity Accounts 398
Pre-Existing New Entity Accounts 399
Recalcitrant Account holders 399
Withholding 400

Certification 401
Reporting 401
U.S. Financial Institutions/Withholding Agents 402

INTERNATIONAL PERSPECTIVES AND INITIATIVES 403

International Perspectives 403
Key International Groups and Initiatives 404

Financial Action Task Force 416
FATF Basics 416
FATF Recommendations 422
Definitions 425
High-Risk and Non-Cooperative Jurisdictions 427
Members and Observers 431
Mutual Evaluations 434

ACRONYMS AND GLOSSARY 442

KEY U.S. AML LAWS AND REGULATIONS AND USEFUL WEBSITES 462

ABOUT PROTIVITI 471

ANTI-MONEY LAUNDERING FUNDAMENTALS

Key Definitions

1. What is money laundering?

Money laundering is the attempt to disguise the proceeds of illegal activity so that they appear to come from legitimate sources or activities.

2. How does money laundering work?

Money laundering can and does take many forms. It typically occurs in three stages: placement, layering and integration.

- **Placement** is the stage in which funds derived from illegal activities are introduced into the financial system anywhere in the world.
- **Layering** involves conducting one or more transactions designed to disguise the audit trail and make it more difficult to identify the initial source of funds.
- **Integration** is the stage in which the funds are disbursed back to the money launderer in what appear to be legitimate transactions.

3. What types of crimes may give rise to a charge of money laundering?

Although money laundering is often equated with drug trafficking, the proceeds of many crimes can be associated with money laundering. These include, but are not limited to, financial fraud, computer crimes, alien smuggling, illegal arms sales, foreign official corruption, exchange control violations, illegal gambling and terrorist financing.

4. What is the current scale of the money laundering problem?

Measuring the current scale of money laundering is extremely difficult. The World Bank and International Monetary Fund estimated the volume of money laundering to be between 3 and 5 percent of global gross domestic product (GDP), equivalent to approximately $2.17 to $3.61 trillion annually.

5. What is terrorism?

Terrorism is often defined as an activity that involves a violent act or an act dangerous to human life, property or infrastructure that appears to be intended to:

- Intimidate or coerce a civilian population
- Influence the policy of a government by intimidation or coercion
- Affect the conduct of a government by mass destruction, assassination, kidnapping or hostage taking

6. What is terrorist financing?

Terrorist financing is a financial crime that uses funds to support the agenda, activities or cause of a terrorist organization. The funds raised may be from legitimate sources, such as charitable organizations or donations from supporters, as well as criminal sources, such as drug trade, weapons smuggling, fraud, kidnapping and extortion for illegal activities.

7. What is the difference between money laundering and terrorist financing?

In contrast to money laundering, which involves the disguising of funds derived from illegal activity so they may be used without detection of the illegal activity, terrorist financing can involve the use of legally derived money to carry out illegal activities. The objective of money laundering is financial gain or the hiding or disguising of illicit proceeds, whereas with terrorism, the objective is to promote the agenda or cause of the terrorist organization. For example, it is widely believed that the terrorist activities of September 11, 2001, were partially financed by legally obtained funds that had been donated to charities. Both money launderers and terrorists, however, do need to disguise the association between themselves and their funding sources.

8. Is the approach to combat money laundering and terrorist financing the same?

Although some of the risk factors and red flags that apply to other types of money laundering also may apply to terrorist financing, the patterns of activity tend to be very different. Terrorist financing often involves very small amounts of funds, which may be moved through charities or nontraditional banking systems, whereas other types of money laundering may involve large volumes of funds. It is important to understand the different patterns to protect against the risks.

Overview of U.S. AML Laws and Regulations

9. What are the key U.S. AML laws and regulations?

The key U.S. AML laws and regulations are the Bank Secrecy Act of 1970 (BSA) and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (commonly referred to as the USA PATRIOT Act).

The BSA was the first major money laundering legislation in the United States. It was designed to deter the use of secret foreign bank accounts and provide an audit trail for law enforcement by establishing regulatory reporting and recordkeeping requirements to help identify the source, volume and movement of currency and monetary instruments into or out of the United States or deposited in financial institutions. For additional guidance on the Bank Secrecy Act, please refer to the Bank Secrecy Act section.

The USA PATRIOT Act was signed into law by President George W. Bush on October 26, 2001, following the terrorist activity of September 11. Title III, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, deals with money laundering and terrorist financing. Title III made significant changes to money laundering regulations, imposed enhanced requirements for AML programs, and significantly expanded the scope of coverage to nonbank financial institutions. It requires financial institutions to establish AML programs that include policies, procedures and controls, designation of a compliance officer, training, and independent review. It also requires, among other things, that certain financial institutions establish customer identification procedures for new accounts as well as enhanced due diligence (EDD) for correspondent and private banking accounts maintained by non-U.S. persons. For additional guidance on the USA PATRIOT Act, please refer to the USA PATRIOT Act section.

10. What other AML laws have been enacted in the United States?

In addition to the BSA and Title III of the USA PATRIOT Act, other AML laws include the Money Laundering Control Act of 1986 (MLCA), the Anti-Drug Abuse Act of 1988, the Annunzio-Wylie Anti-Money Laundering Act of 1992, the Money Laundering Suppression Act of 1994 (MLSA), and the Money Laundering and Financial Crimes Strategy Act of 1998.

The MLCA established two AML criminal statutes that, for the first time, made money laundering a criminal offense, with penalties of up to 20 years and fines of up to $500,000 for each count. Additionally, the MLCA prohibits the structuring of currency transactions to avoid filing requirements and requires financial institutions to develop BSA compliance programs.

The primary purpose of the Anti-Drug Abuse Act of 1988 was to provide funding and technical assistance to state and local units of government to combat crime and drug abuse. This Act increased the civil and criminal penalties for money laundering and other BSA violations to include forfeiture of any property or asset involved in an illegal transaction related to money laundering. It introduced the “sting” provision, which enables law enforcement to represent the source of funds involved in a transaction as the proceeds of unlawful activity. This Act also required the identification and recording of purchases of monetary instruments, including bank checks or drafts, foreign drafts, cashier’s checks, money orders or traveler’s checks in amounts between $3,000 and $10,000 inclusive. This legislation, in conjunction with the Office of National Drug Control Policy (ONDCP) Reauthorization Act of 1998,

authorized the Director of the ONDCP to designate areas within the United States that exhibit serious drug trafficking problems and harmfully impact other areas of the country as High Intensity Drug Trafficking Areas (HIDTAs). The HIDTA program aims to improve the effectiveness and efficiency of drug control efforts among local, state and federal law enforcement agencies.

The Annunzio-Wylie Anti-Money Laundering Act of 1992 gave protection from civil liability to any financial institution, or director, officer or employee thereof, who/that makes a Suspicious Activity Report (SAR) under any local, state or federal law. The Annunzio-Wylie Act made it illegal to disclose when a SAR is filed. It also made it illegal to operate a money transmitting business without a license where such a license is required under state law, and required all financial institutions to maintain records of domestic and international funds transfers. In addition, this Act introduced the "death penalty," mandating that bank regulators consider taking action to revoke the charter of any banking organization that is found guilty or pleads guilty to a charge of money laundering.

The Money Laundering Suppression Act of 1994 (MLSA) specifically addressed money services businesses (MSBs), requiring each MSB to register and maintain a list of its agents. In addition to making it a federal crime to operate an unregistered MSB, the MLSA encouraged states to adopt uniform laws applicable to MSBs. It also established procedures that allowed banks to exempt certain customers from Currency Transaction Report (CTR) filing.

Continuing with the trend of developing a national strategy to combat money laundering, the Money Laundering and Financial Crimes Strategy Act of 1998 called for the designation of areas at high-risk for money laundering and related financial crimes by geography, industry, sector or institution. Some of these areas were later designated as High Risk Money Laundering and Related Financial Crimes Areas (HIFCAs). The HIFCA program was created to coordinate the efforts of local, state and federal law enforcement agencies in the fight against money laundering.

The Intelligence Reform and Terrorism Prevention Act of 2004 amended the BSA to require the U.S. Treasury Secretary to prescribe regulations requiring certain financial institutions to report cross-border electronic transmittals of funds, if the Secretary determines such reporting is "reasonably necessary" to aid in the fight against money laundering and terrorist financing.

11. What is the role of the Office of Foreign Assets Control (OFAC) and how does it fit into AML laws and regulations?

The purpose of OFAC is to promulgate, administer and enforce economic and trade sanctions against certain individuals, entities and foreign government agencies and countries whose interests are considered to be at odds with U.S. policy. Sanctions programs target, for example, terrorists and terrorist nations, drug traffickers and those engaged in the proliferation of weapons of mass destruction.

Overviews and details of the OFAC Sanctions programs can be found on OFAC's website at www.treas.gov/ofac.

OFAC regulations are not part of AML compliance per se, but since the OFAC Sanctions lists include alleged money launderers and terrorists and USA PATRIOT Act requirements mandate that certain financial institutions vet customer names against the OFAC list, institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

12. How can one measure the effectiveness of an AML regime?

A number of factors can be considered when assessing the effectiveness of an AML regime, including the number of money laundering/terrorist financing investigations, prosecutions and convictions, number and amount of frozen/seized assets, identification of deficiencies in financial institutions in examinations by regulatory authorities, and quality of coordination among financial institutions, regulatory and law enforcement authorities. For additional guidance on tools and techniques used to assess the effectiveness of AML systems, please refer to the Financial Action Task Force section.

13. How do U.S. regulations compare to international AML regulations?

The United States' role as a leader in the fight against money laundering and terrorist financing dates back 40 years to the passage of the Bank Secrecy Act in 1970. Through the ensuing decades and especially following the terrorist activities of September 11, 2001, the United States has reinforced its commitment through the passage of a number of additional money laundering-related laws, issuance of extensive regulatory guidance and aggressive enforcement.

That said, the United States, as with many other major jurisdictions, is not in full compliance with the FATF Recommendations. In fact, FATF in its most recent assessment of the United States' anti-money regime, identified several areas in need of improvement, including: customer due diligence relating to beneficial owners, authorized

signers, legal persons and trusts; ongoing due diligence; and general requirements for designated nonfinancial businesses and professions (DNFBPs) (e.g., casinos, accountants, attorneys, dealers in precious metals and stones, real estate agents).

For additional guidance, please refer to the Financial Action Task Force and Mutual Evaluations sections.

For additional guidance on international perspectives, please refer to the International Perspectives and Initiatives section.

14. What are the consequences of not complying with AML laws and regulations?

The consequences of noncompliance with AML laws and regulations may include regulatory enforcement actions, civil and criminal penalties, seizure and forfeiture of funds, and incarceration for the individuals involved. Depository institutions also may be subject to restrictions on growth and expansion and, in the extreme, may have their charters/licenses revoked, a consequence known as the "death penalty." For additional guidance, please refer to the Enforcement Actions section.

15. What factors are considered by law enforcement when it assesses whether an institution or its personnel are guilty of aiding and abetting money laundering or terrorist financing?

When assessing whether an institution or its personnel are guilty of aiding and abetting money laundering or terrorist financing, the authorities consider, among other factors, the following "standards of knowledge":

- **Reckless Disregard** – Careless disregard for legal or regulatory requirements and sound business practice
- **Willful Blindness** – Deliberate ignorance and failure to follow up in the face of information that suggests probable money laundering or illicit activity
- **Collective Knowledge** – Aggregates/attributes the knowledge of employees to the employing company

It is important to remember that under U.S. law, a company may, in general, be held liable for the actions of its employees, regardless of the number or level of employees involved in the wrongdoing.

Overview of the U.S. Regulatory Framework

Key U.S. Regulatory Authorities and Law Enforcement Agencies

16. Who has the authority to assess penalties for violations of AML laws and regulations?

Authority to assess civil penalties rests with the Secretary of the Treasury and is delegated to the Financial Crimes Enforcement Network (FinCEN) and the primary federal regulators or Self-Regulatory Organizations (SROs) (e.g., Financial Industry Regulatory Authority [FINRA]). Some state regulatory agencies have their own authority to assess civil penalties, as well. Criminal penalties are determined through legal proceedings at state or federal levels. The Department of Justice (DOJ) can bring criminal and civil actions, as well as forfeiture actions.

17. Who are the primary federal banking regulators and what are their responsibilities?

The five federal banking regulators include:

- **The Board of Governors of the Federal Reserve System (FRB)** oversees state-chartered banks and trust companies that belong to the Federal Reserve System, financial holding companies, bank holding companies (BHC) and thrift holding companies.
- **The Federal Deposit Insurance Corporation (FDIC)** regulates federally charted banks (e.g., state-chartered banks that do not belong to the Federal Reserve System) as well as state-chartered thrifts.
- **The Office of the Comptroller of the Currency (OCC)** regulates federally chartered banks (e.g., banks that have the word "National" in or the letters "N.A." after their names as well as federal thrifts).
- **The National Credit Union Administration (NCUA)** regulates federally chartered credit unions.

- **Consumer Financial Protection Bureau (CFPB):** Established by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank), the CFPB is a federal regulator charged with regulating consumer protection for financial products and services.

Other regulatory bodies were authorized by the Dodd-Frank Act, but their mandates deal more specifically with broad prudential considerations and consumer protection.

18. What is the Federal Financial Institutions Examination Council (FFIEC)?

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards and report forms, and to make recommendations to promote uniformity in the supervision of financial institutions. Council members include the four federal regulators: FRB, FDIC, OCC, NCUA, and the State Liaison Committee (SLC). The SLC includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS).

19. Who are the key nonbanking regulatory agencies?

Nonbanking regulatory agencies include but are not limited to:

- **Securities and Exchange Commission (SEC):** The SEC is the federal regulator of the securities markets and administers the federal securities laws (including the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Company Act of 1940, the Investment Advisers Act of 1940 and the Trust Indenture Act of 1939), with direct regulatory and oversight responsibilities of securities exchanges, securities brokers and dealers, investment advisers and investment companies, and self-regulatory organizations (SROs).
- **Commodity Futures Trading Commission (CFTC):** The CFTC is the federal regulator of U.S. commodity futures and options markets in the United States. It administers and enforces the federal futures and options laws as set forth in the Commodity Exchange Act (CEA) and the accompanying regulations.
- **Financial Industry Regulatory Authority (FINRA):** Formerly known as the National Association of Securities Dealers (NASD), FINRA is an SRO for broker-dealers.
- **Consumer Financial Protection Bureau (CFPB):** Established by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank), the CFPB is a federal regulator charged with regulating consumer protection for financial products and services.
- **National Futures Association (NFA):** The NFA is the SRO for the futures market.
- **New York Stock Exchange (NYSE):** The NYSE is the SRO for exchange member organizations (i.e., registered broker-dealer organized as a corporation, a partnership or an LLC that holds an NYSE trading license or opts for NYSE regulation).
- **National Indian Gaming Commission (NIGC):** The NIGC is an independent federal regulatory agency whose primary mission is to regulate gaming activities on Indian lands.
- **IRS Tax Exempt and Government Entities Division (IRS-TEGE):** The IRS-TEGE provides federal oversight to all nonprofit organizations in the United States, including reviews to determine if nonprofit organizations are facilitating terrorist financing.
- **IRS Small Business and Self-Employment Division (IRS-SBSE):** The IRS-SBSE has been delegated examination authority over all financial institutions that do not have a federal functional regulator as defined in the BSA, including MSBs, insurance companies, credit card companies, nonfederally insured credit unions, casinos (tribal and nontribal), and dealers in precious metals, stones and jewels. The IRS-SBSE also has responsibility for auditing compliance with currency transaction reporting requirements that apply to any trade or business (Form 8300).

For further guidance on the AML responsibilities of broker-dealers, money services businesses and other nonbank entities, please refer to the Nonbank Financial Institutions and Nonfinancial Business section.

20. What are the key law enforcement agencies responsible for combating money laundering and terrorist financing?

Key law enforcement agencies responsible for combating money laundering and terrorist financing include:

- Drug Enforcement Administration (DEA)

- Federal Bureau of Investigation (FBI)
- Department of Homeland Security, Immigration and Customs Enforcement (ICE)
- Department of Homeland Security, Customs and Border Protection (CBP)
- Internal Revenue Service Criminal Investigation (IRS-CI)

21. What are examples of other key agencies with responsibilities to combat money laundering and terrorist financing?

Key agencies with responsibilities to establish policies and strategies to combat money laundering and terrorist financing include, but are not limited to, the following:

U.S. Department of the Treasury

- Office of Terrorism and Financial Intelligence (TFI)
- Office of Terrorist Financing and Financial Crime (TFFC)
- Office of Intelligence and Analysis (OIA-T)
- Financial Crimes Enforcement Network (FinCEN)
- Office of Foreign Assets Control (OFAC)
- Treasury Executive Office for Asset Forfeiture (TEOAF)

U.S. Department of Justice (DOJ)

- Asset Forfeiture and Money Laundering Section, Criminal Division (AFMLS)
- Counterterrorism Section, Criminal Division (CTS)
- National Drug Intelligence Center (NDIC)
- Office of International Affairs, Criminal Division (OIA)

U.S. State Department

- Bureau of Economic and Business Affairs (EB)
- Bureau of International Narcotics and Law Enforcement Affairs (INL)
- State's Office of the Coordinator for Counterterrorism (S/CT)

22. What publications and resources have been provided to the public by U.S. regulatory and/or law enforcement authorities?

Examples of publications and resources include, but are not limited to, the following:

- **FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Handbook** – Provides guidance to examiners for carrying out BSA/AML and OFAC examinations for depository institutions. The manual contains an overview of AML Compliance Program requirements, AML risks (e.g., products, services, transactions and customer types of heightened risk), risk management expectations, industry sound practices and examination procedures. The development of this manual was a collaborative effort of the Federal Reserve, the OCC, the NCUA, the OTS (which has since been dissolved and replaced on the FFIEC by the Consumer Financial Protection Bureau (CFPB), the FDIC and FinCEN to ensure consistency in the application of AML requirements.
- **Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses** – Provides guidance to examiners for carrying out BSA/AML and OFAC examinations for MSBs. The manual contains an overview of AML Compliance Program requirements, risk management expectations, industry sound practices, examination procedures, overviews of the different types of MSBs (i.e., check cashers, currency dealers or exchangers, issuers of traveler's checks and money orders, money transmitters), overview of the relationship between principals and agents, and additional guidance on MSB registration requirements, foreign agent or foreign counterparty due diligence, and recordkeeping and retention requirements for all types of MSBs. The development of this manual was a collaborative effort by the IRS, state agencies responsible for MSB

regulations, the Money Transmitter Regulators Association (MTRA), the Conference of State Bank Supervisors (CSBS), and FinCEN.

- **Bank Secrecy Act Exam Resources** – Developed by the NCUA, this publication provides guidance to examiners for carrying out AML and OFAC examinations for credit unions.
- **FFIEC Information Technology Examination Handbook** – Developed through a collaborative effort of the Federal Reserve, the OCC, the NCUA, the CFPB and the FDIC, the IT Examination Handbook covers key technology topics as they relate to financial services in separate booklets, including:
    - Audit
    - Operations
    - Management
    - Business continuity planning
    - Outsourcing technology services
    - Development and acquisition
    - Retail payment systems
    - Wholesale payment systems
    - E-banking supervision of technology service providers
    - Information security

  The IT Examination Handbook provides guidance on topics such as risks and suggested controls on third-party payment processors (e.g., Automated Clearing House [ACH] providers, remote deposit capture [RDC] providers) and electronic payments (e.g., electronic banking, automated teller machine [ATM]).
- **Anti-Money Laundering (AML) Source Tool for Broker-Dealers** – Developed by the SEC to assist broker-dealers with fulfilling their responsibilities to establish an AML Compliance Program, as required by AML laws and regulations.
- **Template for Small Firms** – This template, available on FINRA's website, is designed to assist small firms in fulfilling their responsibilities to establish an AML Compliance Program, as required by the BSA and its implementing regulations and FINRA Rule 3310, by providing text examples, instructions, relevant rules, websites and other resources.
- **Compliance Self-Assessment Guide** – Developed by the NCUA, this guide is intended for use by a credit union's board of directors and management, compliance officers, and others having responsibility for compliance as part of their duties. While the guide covers most federal consumer protection laws and regulations that affect credit unions, it does not address all federal laws or any state laws.
- **AML e-learning courses** – FINRA offers several e-learning courses and interactive scenarios on AML-related topics, ranging from customer identification procedures to recognizing red flags.
- **U.S. Money Laundering Threat Assessment (MLTA)** – Published in 2005, the MLTA was written by the following agencies, bureaus and offices:
    - Office of Terrorist Financing and Financial Crime (TFFC)
    - Financial Crimes Enforcement Network (FinCEN)
    - Office of Intelligence and Analysis (OIA)
    - Office of Foreign Assets Control (OFAC)
    - Executive Office for Asset Forfeiture (TEOAF)
    - Internal Revenue Service (IRS) – Criminal Investigation (CI)
    - IRS – Small Business/Self-Employed Division (SB/SE)
    - Federal Bureau of Investigation (FBI)
    - Drug Enforcement Administration (DEA)
    - Asset Forfeiture Money Laundering Section (AFMLS)

- National Drug Intelligence Center (NDIC)
- Organized Crime Drug Enforcement Task Force (OCDETF)
- Immigration and Customs Enforcement (ICE)
- Customs and Border Protection (CBP)
- Federal Reserve
- United States Postal Inspection Service (USPIS)

The MLTA contains detailed analyses of money laundering vulnerabilities across banking, insurance, casinos and MSBs including, but not limited to, the following:

- Banking (e.g., correspondent banking, cash letters/pouch activities, private banking, online banking, remote deposit capture [RDC])
- MSBs (e.g., provision of check cashing, money transmission, prepaid access, monetary instrument, currency exchange services to "noncustomers") and informal value transfer systems (IVTS)
- Emerging electronic and remote payment systems
- Bulk cash smuggling
- Trade-based money laundering (e.g., Black Market Peso Exchange [BMPE], foreign trade zones [FTZs])
- Legal entities (e.g., trusts, shell companies, corporations, limited liability companies)

- **National Money Laundering Strategy (NMLS)** – Written by the U.S. Departments of Homeland Security, Justice, Treasury, and State, as well as by the Federal Reserve, the OCC, and the FDIC, the NMLS was published in 2007 in direct response to the MLTA. Nine key goals were outlined:
  - Continuing to safeguard the banking system
  - Enhancing financial transparency in money services businesses (MSBs)
  - Stemming the flow of illicit bulk cash out of the United States
  - Attacking trade-based money laundering at home and abroad
  - Promoting transparency in the ownership of legal entities
  - Examining anti-money laundering regulatory oversight and enforcement at casinos
  - Implementing and enforcing anti-money laundering regulations for the insurance industry
  - Supporting global anti-money laundering capacity building and enforcement efforts
  - Improving how to measure progress
- **International Narcotics Control Strategy Report (INCSR)** – An annual report issued by the U.S. Department of State that describes the efforts to attack, country by country, all aspects of the international drug trade, as well as chemical control, money laundering and financial crimes.
- **Country Reports on Terrorism** – An annual report, previously known as Patterns of Global Terrorism, issued by the Department of State that provides overviews of terrorist activity in countries in which acts of terrorism occurred, countries that are state sponsors of terrorism, and countries determined by the U.S. Secretary of State to be of particular interest in the global war on terror. The Country Reports on Terrorism also cover major terrorism-related events involving Americans, information on terrorist groups, terrorist sanctuaries, terrorist attempts to acquire weapons of mass destruction, statistical information provided by the National Counterterrorism Center (NCTC) on individuals killed, injured or kidnapped by terrorist groups, and bilateral and multilateral counterterrorism cooperation.

For additional guidance issued by key international groups, please refer to the Key International Groups and Initiatives section. For details on guidance specific to a particular topic (e.g., Suspicious Activity Reports [SARs], correspondent banking, politically exposed persons [PEPs], trade finance), please refer to the respective sections throughout this publication.

Financial Crimes Enforcement Network

23. What is the Financial Crimes Enforcement Network, and what is its role in AML regulation?

The Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Treasury Department, was established in 1990 by Treasury Order 105-08. Its mission is to safeguard the financial system from abuses of financial crime. It is the Financial Intelligence Unit (FIU) of the United States, formed to support law enforcement and the financial community in the fight against money laundering, terrorist financing and other financial crimes through the collection, analysis and sharing of BSA information. FinCEN seeks to provide adequate financial intelligence to law enforcement without overburdening the financial community or compromising the privacy of individuals.

The many partnerships of FinCEN are not limited to the United States, but expand internationally to law enforcement, financial institutions and regulatory authorities in foreign countries, as well.

While FinCEN relies primarily on federal functional regulators to examine financial institutions and enforce AML compliance, the regulators look to FinCEN for guidance in the implementation of the BSA and USA PATRIOT Act. FinCEN has issued regulations, in concert with federal functional regulators and the Internal Revenue Service (IRS), related to BSA and AML compliance. FinCEN may issue enforcement actions for violations of the BSA and USA PATRIOT Act through its Office of Enforcement jointly or unilaterally. The Office of Enforcement evaluates enforcement matters, including the assessment of civil money penalties.

24. In what types of initiatives does FinCEN engage?

In 1992, as part of the Annunzio-Wylie Anti-Money Laundering Act, FinCEN formed the Bank Secrecy Act Advisory Group (BSAAG), a task force established to coordinate and inform the financial community about BSA-related matters. The BSAAG includes senior representatives from financial institutions, federal law enforcement agencies, regulatory agencies, and others from the public and private sectors. In 2009, the Financial Fraud Enforcement Task Force (FFETF) was established as a multi-agency task force with federal, state and local partners to improve efforts to investigate and prosecute significant financial crimes, recover proceeds for victims, and address financial discrimination in the lending and financial markets.

FinCEN also has created several communication systems to facilitate the sharing of information among both domestic and international entities. The BSA E-Filing System allows financial institutions to file electronic BSA forms, such as CTRs and SARs, quickly and securely. The Gateway program enables law enforcement agencies and financial industry regulators to have expedited access to BSA records filed with FinCEN. The Law Enforcement and Financial Institution Information Sharing (LEFIIS) system allows law enforcement to receive feedback from financial institutions on subjects of money laundering and terrorism investigations, and is used to facilitate information sharing among financial institutions. FinCEN also developed the Egmont Secure Web (ESW), which is a private network that allows connected FIUs to interface with FinCEN and each other to access information related to money laundering trends, analytical tools and technological developments via e-mail.

Additional tools include the Geographic Threat Assessments and Nontraditional Methodologies Sections, a resource center for emerging methods of money laundering and terrorist financing.

FinCEN also collaborates with other FIUs globally to exchange information supporting AML and counterterrorism initiatives worldwide, and assists other countries with developing their FIUs. For additional guidance on FIUs, please refer to the Key International Groups and Initiatives section.

25. What resources has FinCEN provided to the public?

Among the issuances and resources provided by FinCEN are the following:

- **Statutes and Regulations** – Resource that contains links to BSA and USA PATRIOT Act statutes and codified regulations.
- **Federal Register Notices** – Links to final regulations issued after the date of codification as well as Notices of Proposed Rulemaking (NPRs) in the Federal Register.
- **Guidance** – Clarification of issues or responses to questions related to FinCEN regulations (e.g., completion and filing of Suspicious Activity Reports [SARs]; applicability of the definition of a money services business [MSB] to a particular business activity; applicability of the Safe Harbor provision when sharing SARs under certain circumstances).

- **Administrative Rulings** – Rulings that provide a new interpretation of the BSA or any other statute granting FinCEN authority, express an opinion about a new regulatory issue, and/or outline the effect of the various releases on covered financial institutions.
- **Advisories/Bulletins/Rulings/Fact Sheets** – An archive of advisories, advisory withdrawals, bulletins, rulings and fact sheets dating back to 1996.
- **Answers to Frequently Asked Bank Secrecy Act (BSA) Questions** – A list of basic questions and answers about BSA and USA PATRIOT Act laws and regulations.
- **Reports and Publications** – Reports published periodically on key regulatory issues and strategies to address these issues including, but not limited to, the following:
    - **The SAR Activity Review: "Trends, Tips & Issues"** – A publication produced approximately once or twice each year by FinCEN in cooperation with many regulatory, law enforcement and industry partners. The publication gives the public information and insight concerning the preparation, use and value of SARs filed by institutions.
    - **The SAR Activity Review: "By the Numbers"** – A publication that is generally produced twice each year as a companion to The SAR Activity Review: "Trends, Tips & Issues" and provides numerical data on SAR filings.
    - **Financial Institutions Outreach Initiative** – Reports sharing information gathered through various outreach initiatives with representatives in the financial industry (e.g., large depository institutions, MSBs).
    - **Strategic Analytical Reports and Other Publications** – Publications addressing other trends and issues, such as Mortgage Loan Fraud: An Update of Trends Based upon an Analysis of Suspicious Activity Reports (April 2008).
    - **Annual Report** – Provides an overview of FinCEN's current state and details the strategies and outcomes of the year's operations.
    - **Report to Congress** – An archive of reports made to Congress by the U.S. Secretary of the Treasury dating back to 2002, including the required annual 361(b) report.
    - **The Strategic Plan** – Published periodically, the Strategic Plan details how FinCEN intends to achieve its current goals in the near future.
- **Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses** – Guidance on the examination process of MSBs, in English and Spanish.
- **Enforcement Actions** – Links to enforcement actions dating back to 1999.
- **Law Enforcement** – A summary of support services for law enforcement and links to law enforcement case examples that have been assisted by information reported under BSA regulations.
- **News Releases** – An archive of important FinCEN news releases dating back to 1994.
- **Speeches** – An archive of speeches given by the director of FinCEN dating back to 2004.
- **Testimony** – An archive of testimony given by the director of FinCEN dating back to 2004.

26. How does FinCEN interact with banking and securities regulators?

In 2004, FinCEN entered into a Memorandum of Understanding (MOU) with federal banking regulators. The MOU sets forth procedures for the administration of the BSA, Titles I and II of Pub. L. 91-508, as amended, codified at 12 U.S.C. § 1829b, 12 U.S.C. §§ 1951-1959, and 31 U.S.C. §§ 5311-5332; information relating to the primary federal regulators' policies and procedures for examination of BSA compliance; significant BSA compliance issues at banking organizations supervised by the regulators; and analytical data based on or derived from information provided by the regulators. The MOU also gives FinCEN authority to issue its own enforcement actions, even when regulators may not think it is necessary. On April 26, 2005, FinCEN and the New York State Banking Department entered into a similar MOU; shortly thereafter, a number of other states followed suit.

In late 2006, the SEC and FinCEN entered into an MOU under which the SEC provides FinCEN with detailed information on a quarterly basis regarding the AML examination and enforcement activities of the SEC and the Self-Regulatory Organizations (SROs). In return, FinCEN provides assistance and analytical reports to the SEC.

In June 2011, FinCEN entered into an MOU with the Consumer Financial Protection Bureau (CFPB), which provides the CFPB direct electronic access to BSA information and analytical materials (e.g., analytical tools, BSA information reviews, etc.) as required and appropriate for the exercise of the CFPB's regulatory authority. In return, the CFPB, upon request, will provide reports on the results of its investigations or examinations and statistical information related to any inquiries to assist FinCEN in understanding and analyzing the value of BSA information.

Enforcement Actions

27. What types of enforcement actions are available to regulators for addressing AML Compliance Program deficiencies and violations?

Regulators have a range of enforcement tools available to address AML Compliance Program deficiencies and violations of AML laws and regulations.

While enforcement actions against nonbanks have increased in recent years, the number of enforcement actions issued by bank regulators continues to outnumber those of other agencies, at least in the United States. Examples of enforcement actions available to U.S. bank regulators in order of severity are:

- **Commitment Letter**: A Commitment Letter is an agreement between a bank's board of directors and a bank regulator in which the board, on behalf of a bank, agrees to take certain actions to address issues or concerns surfaced by the regulator. A Commitment Letter is not legally binding, but the failure of a bank to live up to the terms of the Commitment Letter may subject the bank to more formal regulatory action.
- **Memorandum of Understanding**: A Memorandum of Understanding (MOU) is an agreement between a bank's board of directors and one or more regulatory agencies. The content of an MOU may be similar or identical to more formal enforcement actions, but MOUs are nonpublic documents and, similar to Commitment Letters, not legally binding.
- **Formal Agreements**: A Formal Agreement is an agreement between a bank's board of directors and one or more regulatory agencies. While the contents of a Formal Agreement may mirror those of an MOU, violations of a Formal Agreement can provide the legal basis for assessing civil money penalties (CMPs) against directors, officers and other institution-affiliated parties.
- **Consent Order or Order to Cease and Desist (C&D)**: Consent Orders and Orders to Cease and Desist are agreements between a bank's board of directors and one or more regulatory agencies. Violations of a Formal Agreement can provide the legal basis for assessing civil money penalties (CMPs) against directors, officers and other institution-affiliated parties. The regulator's decision to issue a Consent Order or Order to Cease and Desist rather than a formal agreement is based on its assessment of the severity of the bank's problems.
- **Civil Money Penalties (CMPs)**: Civil money penalties are financial penalties that may be imposed by a regulator against a bank or an individual(s) for a violation of law or regulation or noncompliance with a formal enforcement action.
- **"Death Penalty"**: Under the Annunzio-Wiley Act of 1992, bank regulators have the option – in fact, are obligated to consider – whether the license/charter of a depository institution that is found guilty or pleads guilty to money laundering charges should be revoked. The revocation of a license/charter is known as the "Death Penalty."

Unlike the formal enforcement actions issued by bank regulators, which are usually very prescriptive as to the actions that must be taken to address the identified deficiencies, the enforcement actions taken by securities and futures/commodities regulators generally report findings that detail the nature of the deficiency, but do not prescribe specific corrective action (and accompanying fines have been modest compared to those levied against banks).

28. Does FinCEN have enforcement authority?

FinCEN does have enforcement action authority, which it often uses in conjunction with a financial institution's functional regulators.

29. Beyond the actions and penalties that may be imposed by regulators, are U.S. companies subject to any other potential actions?

Yes. Other actions, such as Deferred Prosecution Agreements (DPA), may result from legal actions.

30. What is a Deferred Prosecution Agreement?

A DPA is an agreement entered into between a prosecutor and a defendant in a criminal case whereby in exchange for successful completion of agreed-upon commitments, the criminal charges against the defendant will be dismissed in their entirety by the prosecutor.

31. What enforcement actions have had a significant impact on the AML landscape?

Certain enforcement actions stand out because of the size of the penalties imposed on the institutions and/or the media attention they received. Examples would include:

- Banking Organizations:
  - **ABN Amro**: In December 2005, ABN Amro was assessed an $80 million Civil Money Penalty (CMP) for failure to implement an adequate system of internal controls reasonably designed to assure compliance with U.S. AML laws and regulations. The CMP cited deficiencies within the North American Regional Clearing Center (NARCC), a unit within the New York Branch of ABN Amro that operated as a clearing center for funds transfers in U.S. dollars for members within the ABN Amro network and more than 400 third-party financial institutions. Specific findings included the following:
    - Failure to staff the compliance function and train compliance personnel adequately
    - Failure to file accurate and timely Suspicious Activity Reports (SARs)
    - Lack of formal procedures for collecting and reviewing due diligence and assessing the risks of foreign financial institutions accessing correspondent banking services
    - Lack of adequate monitoring of funds transfers for potentially suspicious activity, particularly funds transfers conducted by financial institutions independent of the ABN Amro network
    - Failure to incorporate information on subjects of previous SAR filings, terminated relationships, and publicly available information on shell companies into its suspicious activity monitoring program
    - Failure to investigate alerts and utilize the capabilities of its automated monitoring software to manage its money laundering and terrorist financing risk effectively
  - **American Express**: In August 2007, American Express International Bank (AEIB) was issued a Cease and Desist (C&D) order and assessed a $20 million CMP and $55 million forfeiture. American Express Travel Related Services Co. (AETRSC) also was assessed a $5 million CMP. Cross-border payment made total effective charges, including forfeiture, $65 million. AEIB provided private banking services to high net worth clients and AETRSC operated as a money services business (MSB). Specific findings included the following:
    - Failure to implement comprehensive customer due diligence (CDD) and enhanced due diligence (EDD) processes
    - Failure to implement effective control measures for bearer shares and other private investment companies (PICs)
    - Failure to adhere to the internal policies for periodic reviews of high-risk accounts
    - Inadequate transaction monitoring system due to data integrity and other problems
    - Inadequate independent testing of the AML Compliance Program
    - Failure to provide adequate oversight of and accountability for the AML Compliance Program by management of AEIB and its parent company, AEB
  - **Wachovia**: In March 2010, the Office of the Comptroller of the Currency (OCC), FinCEN and the U.S. Department of Justice (DOJ) announced that Wachovia Bank, N.A., had agreed to a Deferred Prosecution Agreement with a forfeiture of $110 million with the DOJ, a civil money penalty of $50 million, a C&D with the OCC, and a civil money penalty (CMP) of $110 million with FinCEN. FinCEN agreed its CMP would be satisfied by the payment of the DOJ forfeiture. Specific findings included the following:
    - Failure to implement adequate policies, procedures and controls for bulk cash transactions conducted by high-risk *casas de cambio* and other foreign correspondent banking customers

- Failure to conduct monitoring of the high volume of monetary instruments through *casas de cambio* and other foreign correspondent customers using Remote Deposit Capture (RDC) service
- Failure to monitor sequentially numbered traveler's checks used by *casas de cambio* and other foreign correspondent customers in a manner compliant with internal policy on these transactions
- Failure to institute appropriate risk-based monitoring of foreign correspondent banking customers – primarily as a result of setting alert parameters based on staffing capacity
- Failure to file timely SARs on several foreign correspondent banking customers
- Failure to report cash structuring activity

o **HSBC:** In October 2010, the Federal Reserve Board announced that it had issued a Cease and Desist Order between HSBC North America Holdings, Inc. (HNAH), New York, New York, a registered bank holding company (BHC), and the Federal Reserve Board. The order requires HNAH to take corrective action to improve its firm-wide compliance risk management program, including its anti-money laundering compliance risk management. Concurrent with the Federal Reserve Board's announcement of its enforcement action, the Office of the Comptroller of the Currency announced its issuance of a Cease and Desist Order against HSBC Bank USA, N.A., McLean, Virginia (HBUS, a subsidiary of HNAH), for violating the Bank Secrecy Act and its underlying regulations.

HSBC was directed to use its financial and managerial resources as a source of strength for its bank subsidiaries, and in particular HBUS, to ensure that it complies with the OCC Consent Order regarding HBUS' BSA/AML program. It was also directed to "retain an independent consultant acceptable to the [Chicago Federal] Reserve Bank to complete a review of the effectiveness of the firm-wide BSA/AML Compliance Program adopted by HNAH (the 'BSA/AML Review'), and to prepare a written report of findings and recommendations (the 'BSA/AML Report')." In another section of the Order, HNAH was directed to "submit to the [Chicago Federal] Reserve Bank an acceptable written program designed to reasonably ensure the identification and timely, accurate, and complete reporting by HNAH and its subsidiaries of all known or suspected violations of law or suspicious transactions to law enforcement and supervisory authorities, as required by applicable suspicious activity reporting laws and regulations."

The OCC Order states that the agency found deficiencies in HBUS' BSA/AML Compliance Program – in particular, deficiencies in internal controls for customer due diligence, procedures for monitoring suspicious activity and independent testing. The Order also cited aggravating factors "such as highly suspicious activity creating a significant potential for unreported money laundering or terrorist financing." Specific cited deficiencies included special handling of wire transfers of customers domiciled in countries risk-rated as "standard" or "medium," resulting in limited and ineffective BSA/AML monitoring of two-thirds of the bank's wire activity; failure from 2006 to 2009 to monitor bulk cash transactions with foreign affiliates; failure to perform customer due diligence or enhanced due diligence for its foreign affiliates, inhibiting its assessment of customer risk and the identification of suspicious activity in accounts of those affiliates; failure to address a backlog of suspicious activity alerts (due to inadequate staffing), which caused the bank to file many late SARs; and failure to appropriately designate customers as "high-risk" for BSA/AML monitoring, even when a customer's association with PEPs could harm the bank's reputation. In July 2012, HSBC was the subject of a hearing held by the Senate Permanent Subcommittee on Investigations entitled "U.S. Vulnerabilities to Money Laundering and Terrorist Financing: HSBC Case History."

o **Citibank:** In April 2012, the OCC issued a Cease and Desist Order against Citibank, N.A. for violations of the Bank Secrecy Act (BSA) and underlying regulations. According to the OCC, the order requires the bank to take comprehensive corrective actions to improve its BSA compliance program.

The compliance program allegedly had deficiencies with respect to internal controls, customer due diligence, the independent BSA and the anti-money laundering audit function, monitoring of its remote deposit capture and international cash letter instrument processing in connection with foreign correspondent banking, and suspicious activity reporting related to that monitoring. These findings resulted in violations by the bank of statutory and regulatory requirements to maintain an adequate BSA compliance program, file suspicious activity reports, and conduct appropriate due diligence on foreign correspondent accounts.

As part of the Order, the Bank is required to arrange for an independent look back for suspicious activity covering areas (and presumably time frames) to be designated by the bank's Examiner-in-Charge.

- Broker-Dealers:
  - **E*TRADE**: In January 2009, FINRA assessed a $1 million penalty against E*Trade Securities and E* Trade Clearing LLC for failure to implement AML policies and procedures to reasonably detect and report potentially suspicious securities transactions. Alerts triggered in the automated monitoring system were limited to those with money movements, thereby eliminating detection and review of potentially suspicious matched or washed trades. The firms relied upon analysts to monitor high-volume online trading activity for potentially suspicious activity manually, without providing necessary automated monitoring tools.

    Additionally, in July 2008, both firms reached a $1 million settlement with the SEC for failure to document their Customer Identification Program (CIP) and verify the identities of more than 65,000 clients from October 2003 to June 2005.
- Money Services Businesses (MSBs):
  - **Sigue Corporation**: In January 2008, FinCEN assessed a $12 million CMP on Sigue Corporation for failure to implement an effective AML Compliance Program in all four core elements as defined in the USA PATRIOT Act: internal controls, designation of compliance officer/personnel, training, and independent testing. The U.S. Department of Justice assessed a $15 million forfeiture and entered into a Deferred Prosecution Agreement (DPA). Payment of the forfeiture satisfied the FinCEN penalty. Specific findings included the following:
    - Lack of defined roles and responsibilities of the compliance function
    - Failure to implement a risk-based suspicious activity monitoring program commensurate with dollar volume and geographic reach
    - Lack of effective supervision and control over agents (e.g., agents advising customers to structure transactions to evade AML reporting requirements)
    - Failure to investigate alerts in a timely manner
    - Failure to file complete, accurate or timely Suspicious Activity Reports (SARs)
    - Inadequate and untailored training program and/or training program not completed by all employees/agents
    - Inadequate independent testing (e.g., not risk-based, insufficient testing, narrow scope) that failed to identify system problems within the AML Compliance Program
  - From 2010 to 2011, seven MSBs were subject to enforcement actions primarily for failure to register with FinCEN as an MSB. All were acting as independent money transmitters. A summary of findings included the following:
    - Failure to register as an MSB or complete biennial renewals with FinCEN
    - Failure to implement an AML program as required for money transmitters
    - Failure to report potentially suspicious transactions on SARs
    - Structuring currency transactions to evade BSA reporting requirements
    - Conspiracy to commit food stamp fraud

32. What have been the most common deficiencies in AML Compliance Programs?

Some common themes have been:

- **Program Violations**: Overall failures supported by "pillar" violations, i.e., the failure of an institution to address adequately its obligation to designate a qualified AML compliance officer; develop and implement appropriate policies, procedures and controls; provide adequate training; and perform periodic independent testing of its AML Compliance Program.
- **Systemic and Recurring Violations**: Pervasive control breakdowns

- **Isolated and Technical Violations**: Limited instances of noncompliance that do not threaten overall program effectiveness

Some common problems and issues include, but are not limited to, the following:

- AML compliance officer (as well as other employees) lacks sufficient experience and/or knowledge regarding AML policies, procedures and tools
- Insufficient/inadequate resources dedicated to AML compliance
- Lack of specific and customized training of employees with critical functions (e.g., account opening, transaction processing, risk management)
- Failure to conduct adequate risk assessments (e.g., customer risk assessment, business line risk assessment, OFAC risk assessment)
- Failure to incorporate risk assessments into a transaction-monitoring process, customer acceptance standards, audits, testing or training
- Inadequate Know Your Customer (KYC) procedures (e.g., CIP, CDD and EDD at or after account opening, including inadequate controls over required fields, inadequate methods of obtaining and/or maintaining current information, lack of reporting capabilities over missing information, and lack of verification procedures)
- Poor documentation maintained for investigations that did not lead to SAR filings
- Poor follow-up on SAR actions (e.g., close, monitor)
- Lack of reporting of key SAR information to senior management/board of directors
- Inadequate tuning, validation and documentation of automated monitoring systems
- Overreliance on software to identify transactions for which CTRs and/or SARs must be filed without fully understanding how the software is designed and what information it does/does not capture
- Exclusion of certain products from transaction monitoring (e.g., loans, letters of credit, capital markets activities)
- Lack of timeliness when filing CTRs and SARs (e.g., reports are manually filed via certified mail, and the date postmarked is not noted)
- Lack of or inadequate independent testing of the AML Compliance Program
- Lack of or untimely corrective actions to prior examination or audit findings

To identify potential gaps in a financial institution's AML Compliance Program, regulatory enforcement actions for AML deficiencies against other (similar) financial institutions should be reviewed to identify the specific violations and related action steps. This enables financial institutions to recognize and correct any potential weaknesses of their own before their next regulatory examination.

AML Compliance Program

33. What types of financial institutions are required to comply with AML laws and regulations?

Under the USA PATRIOT Act, the definition of "financial institutions" was expanded to include more than 20 different types of businesses that provide financial services, including, but not limited to, broker-dealers, currency exchangers, insurance companies, trust companies, dealers in precious metals, stones or jewels, and issuers of traveler's checks, money orders or similar instruments.

For additional guidance on the other types of financial institutions now required to comply with AML laws and regulations, please refer to the USA PATRIOT Act and Nonbank Financial Institutions and Nonfinancial Businesses sections.

34. What are the key components of an AML Compliance Program?

Key components of an AML Compliance Program include, but are not limited to, the following:

- **Designated Compliance Officer** – For further guidance, please refer to the Designation of AML Compliance Officer and the AML Compliance Organization section.
- **Risk Assessments** – For further guidance, please refer to the Enterprise-wide Risk Assessment, Business Line Risk Assessment, Customer Risk Assessment and OFAC Risk Assessment sections.
- **Customer Acceptance and Maintenance Program** – For further guidance, please refer to the Know Your Customer, Due Diligence and Enhanced Due Diligence, Section 326 – Verification of Identification, Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts and High Risk Customers sections.
- **Large Currency Monitoring and Currency Transaction Report Filing Program** – For further guidance, please refer to the Currency Transaction Reports section.
- **Monitoring, Investigating and Suspicious Activity Report Filing Program** – For further guidance, please refer to the Transaction Monitoring, Investigations and Red Flags and Suspicious Activity Reports sections.
- **Sanctions Program** – For further guidance, please refer to the Office of Foreign Assets Control section.
- **Information Sharing** – For further guidance, please refer to Section 314(a) – Cooperation among Financial Institutions, Regulatory Authorities and Law Enforcement Authorities, Section 314(b) Requirements – Cooperation among Financial Institutions and National Security Letters sections.
- **Recordkeeping and Retention Program** – For further guidance, please refer to the Funds Transfer Recordkeeping Requirement and the Travel Rule, Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments, Form 8300 and Report of Foreign Bank and Financial Accounts sections.
- **Independent Testing** – For further guidance, please refer to the Independent Testing section.
- **Training** – For further guidance, please refer to the AML Training section.
- **Management and Board Reporting** – For further guidance, please refer to the Designation of AML Compliance Officer and AML Compliance Organization section.

It is important to note that not all types of financial institutions are required to have each of the key components listed above. For additional guidance on the AML requirements of nonbank financial institutions, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

35. How can technology be used to support a financial institution's AML program?

Technology can be used, for example, to support:

- **Monitoring for Suspicious Transactions and Facilitating Suspicious Activity Report Filing** – For further guidance, please see the Suspicious Transaction Monitoring and Suspicious Activity Report Filing Software section.
- **Monitoring for Large Currency Transactions and Facilitating Currency Transaction Report Filing** – For further guidance, please see the Large Currency Transaction Monitoring and Currency Transaction Report Filing Software section.
- **Verification of Customer Information (e.g., CIP)** – For further guidance, please see the Customer Verification Software section.
- **Storage of Customer Information (e.g., CIP, EDD)** – For further guidance, please see the Customer Information Database and Customer Risk Assessment Software section.
- **Calculation of Customer Risk Ratings** – For further guidance, please see the Customer Information Database and Customer Risk Assessment Software section.
- **Searching Against Special Lists of Prohibited and/or High-Risk Individuals/Entities** (e.g., Office of Foreign Assets Control [OFAC], 314(a), Subpoenas, Media Searches, Internal "Deny" Lists, Politically Exposed Persons [PEPs]) for Customers and Transactions – For further guidance, please see the Interdiction Software and List Providers sections.
- **AML Training** – For further guidance, please see the Training Software section.
- **Case Management** – For further guidance, please see the Case Management Software section.

BANK SECRECY ACT

Overview of BSA

The sections that follow outline BSA reporting requirements, including Currency Transaction Reports (CTRs), Suspicious Activity Reports (SARs), Form 8300, Reports of Foreign Bank and Financial Accounts (FBARs) and Reports of International Transportation of Currency or Monetary Instruments (CMIRs). The sections also outline additional recordkeeping requirements, including the Funds Transfer Recordkeeping Requirement, the Travel Rule, and the Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments.

36. What does the term “financial institution” mean for Bank Secrecy Act purposes?

As originally defined in the BSA, "financial institution" meant each agent, agency, branch or office within the United States of any person doing business, whether or not on a regular basis or as an organized business concern, in one or more of the capacities listed below:

- Bank (except bank credit card systems)
- Broker or dealer in securities
- Money services business (MSB)
- Telegraph company
- Casino
- Card club
- Person subject to supervision by any state or federal bank supervisory authority
- Futures commission merchant (FCM)
- Introducing broker (IB) in commodities

The definition of “financial institution” was significantly expanded by the USA PATRIOT Act. For further details on the expanded definition of “financial institution,” please refer to the USA PATRIOT Act section. For additional guidance on the definitions of nonbank financial institutions (NBFIs) (e.g., MSBs, casinos), please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

37. Are foreign financial institutions subject to the requirements of the BSA?

The requirements of the BSA apply to the U.S. operations of foreign financial institutions in the same manner as they apply to domestic financial services companies. As a practical matter, however, non-U.S. offices of foreign financial institutions will find they are directly and indirectly affected by BSA requirements in their efforts to support the AML Compliance Programs of their U.S.-based affiliates.

38. What is the value to law enforcement of the various reporting and recordkeeping requirements imposed by the BSA?

In general, BSA reports have become extremely useful to law enforcement in the identification, investigation and prosecution of money laundering and other criminal activity, especially those generating large amounts of cash. Data contained in BSA reports also are used to identify and trace the disposition of proceeds from illegal activity for

possible seizure and forfeiture. In addition, agencies can analyze reports on a strategic level to obtain trends and assess the threat(s) in particular areas.

Reporting Requirements

Currency Transaction Reports

The sections that follow outline general Currency Transaction Report (CTR) requirements for depository institutions, securities brokers or dealers, futures commission merchants (FCMs), introducing brokers (IBs), and money services businesses (MSBs), including CTR Basics, CTR Threshold and Aggregation, Completion of a CTR Form, CTR Exemptions, CTR Evasions and CTR Trends.

For additional guidance on the CTR filing requirements for casinos, please refer to the Casinos or Card Clubs section. For guidance on the reporting requirement for large currency transactions received by persons engaged in trade or business, please refer to the Form 8300 section.

CTR Basics

39. What is a Currency Transaction Report?

A Currency Transaction Report (CTR) is a report filed by certain types of financial institutions, identified below, for cash currency transactions of more than $10,000 in one business day. Multiple transactions must be treated as a single transaction (aggregated) if the financial institution has knowledge that they are by or on behalf of the same person and result in cash-in or cash-out totaling more than $10,000 in any one business day.

40. What does the term “currency” mean for CTR filing purposes?

Currency means the coin and paper money of the United States or any other country that is circulated and customarily used and accepted as money.

41. What does the term “business day” mean for CTR aggregation purposes?

A business day is the reporting period on which transactions are routinely posted to customers’ accounts each day. For additional guidance on the definition of “business day,” please refer to the Casinos or Card Clubs section.

42. What types of currency transactions require CTR filings?

Any physical transfer of currency from one person to another requires the filing of a CTR. This would include, for example:

- Cash withdrawals
- Cash deposits
- Foreign currency exchange
- Check cashing paid in cash
- Cash payments
- Cash purchase of monetary instruments (e.g., bank check or draft, foreign draft, cashier’s check, money order, traveler’s check)
- Automated Teller Machine (ATM) cash transactions
- Incoming or outgoing wire transactions paid in cash

Wire and check transactions that do not involve the physical transfer of cash would not be considered currency transactions for CTR filing requirements.

43. What financial institutions are obligated to file CTRs?

The following financial institutions are subject to CTR filing requirements:

- Banks
- Credit unions
- Depository institutions
- Securities brokers or dealers
- Mutual funds
- Futures commission merchants (FCMs) and introducing brokers (IBs)
- Money services businesses (MSBs)
- Casinos
    - Casinos formerly used a form customized to the gaming industry, Currency Transaction Report for Casinos (CTR-C, Form 103). (Note: Form 103-N for casinos in Nevada was rescinded as of July 1, 2007.) Casinos are required to file the same new CTR as other financial institutions. For additional guidance on the CTR filing requirements for casinos, please refer to the Casinos or Card Clubs section.

With limited exceptions, businesses not subject to CTR requirements must file Form 8300. For additional guidance on Form 8300, please refer to the Form 8300 section.

44. What significant changes were made to CTRs?

In 2012, CTRs were redesigned to accommodate the different types of industries required to file these reports, to more effectively capture critical data and to facilitate mandatory e-filing of CTRs. Significant changes to CTRs include, but are not limited to, the following:

- Elimination of the CTR-C for casinos and addition of field identifying the type of financial institution filing the CTR
- Dynamic and interactive fields that adjust subsequent required fields based on inputted information (e.g., type of financial institution, etc.) or pre-populate with enhanced data (e.g., High Intensity Financial Crime Area (HIFCA) or High Intensity Drug Trafficking Area (HIDTA) designations, etc.)
- Critical fields marked as mandatory that must be completed before acceptance
- Updated list of prohibited words and phrases
- Updated type of filing (e.g., initial, corrected/amended, FinCEN directed backfiling, prior report)
- Addition of new transaction types (e.g., currency to/from prepaid access, etc.)
- Addition of North American Industry Classification System (NAICS) Code field for SAR subjects
- Addition of a gender field for SAR subjects

45. Are new obligations created for financial institutions based on these changes to CTRs?

No. Changes to CTRs do not create any new obligations for financial institutions (e.g., requirement to change internal procedures to capture information for a new data field on the CTR, such as gender or NAICS code, etc.). Financial institutions are expected to provide information for which they have direct knowledge consistent with existing regulatory expectations.

46. What are 'legacy' reports?

Legacy reports are expired CTRs and SARs that FinCEN has replaced. The expired reports include FinCEN Form 104, FinCEN Form 103 (CTR by Casinos) and all industry-specific SAR forms (TD F 90-22.47, FinCEN Form 101, FinCEN Form 102 and FinCEN Form 109). For further guidance on the changes to SARs, please refer to the SAR Basics section.

47. When must a financial institution start using the new CTR?

In December 2011, FinCEN extended the period for financial institutions to start using the new CTRs from June 30, 2012 to March 31, 2013. During this period, FinCEN will accept both the new and legacy CTRs through the e-filing system.

48. How do financial institutions submit CTRs to FinCEN?

Beginning July 1, 2012, financial Institutions must submit CTRs through the BSA E-Filing System, an Internet-based e-filing system developed by FinCEN to enable financial institutions to file CTR and SAR forms electronically. While the use of the BSA E-Filing System can be beneficial for all financial institutions, its use is generally more cost-effective for financial institutions with large volumes of CTR and SAR filings since it enables the batching of forms.

49. What is the time frame for filing CTRs?

If filing manually, CTRs must be filed within 15 calendar days of the date of the reportable transaction. If filing electronically, CTRs must be filed within 25 calendar days of the transaction date up until March 31, 2013, after which, CTRs filed electronically must be filed within 15 days of the transaction date.

50. How long should a financial institution retain CTRs?

CTRs must be retained for a minimum of five years from the date of filing.

51. Can a financial institution inform a customer of the requirement to file CTRs?

Yes. A financial institution can inform a customer of the CTR filing requirement. However, financial institutions and/or their employees cannot assist customers in evading the reporting requirement by "structuring" their transactions. For additional guidance on evasion, please refer to the CTR Evasion section.

If, after being informed of the CTR filing requirement, the customer breaks his or her transaction into smaller amounts in an attempt to evade reporting requirements, the financial institution, in most cases, should consider filing a SAR on the basis of structuring.

52. Are financial institutions obligated to inform the customer that the financial institution will file a CTR on the customer's activity since it is over the reporting threshold?

No. Financial institutions are not obligated to notify customers when filing CTRs.

53. What should a financial institution do if it discovers it has failed to file CTRs on reportable transactions?

If a financial institution finds it has failed to file CTRs on reportable transactions, it should move forward to file the CTRs as soon as the failure is discovered. If there are a significant number of CTRs at issue, or if they cover transactions that are not relatively recent in time, the financial institution should contact the IRS Enterprise Computing Center – Detroit (formerly the Detroit Computing Center) to request a determination on whether the back-filing of unreported transactions is necessary. Prior to doing this, the institution may wish to seek advice from counsel to ensure that communication with the authorities is handled properly.

54. Are financial institutions required to file CTRs for bulk currency shipments?

Yes. For all receipts or disbursement of currency in excess of $10,000, financial institutions are required to file a CTR. For additional guidance on bulk currency shipments, please refer to the Bulk Shipments of Currency section.

55. What guidance has been issued related to CTRs?

The following, though not intended to be all inclusive, lists key guidance that has been issued on the completion and filing of CTRs and exemptions:

- Completion and filing of CTRs
    - **FinCEN Educational Pamphlet on the Currency Transaction Reporting Requirement** (2009) by FinCEN
    - **BSA E-Filing System Frequently Asked Questions** (2010) by FinCEN

- **BSA Electronic Filing Requirements for the Currency Transaction Report (CTR) (FinCEN Form 104) and Designation of Exempt Person (DOEP) (FinCEN Form 110)** (2012) by FinCEN
- **Notice to Customers: A CTR Reference Guide** (2009) by FinCEN
- **FinCEN Currency Transaction Report (FinCEN CTR) Electronic Filing Requirements** (2012) by FinCEN
- **Filing FinCEN's New Currency Transaction Report and Suspicious Activity Report** (2012) by FinCEN
- **Reporting of Certain Currency Transactions for Sole Proprietorships and Legal Entities Operating Under a "Doing Business As" (DBA) Name** (2008) by FinCEN
- **Currency Transaction Report Aggregation for Businesses with Common Ownership** (2012) by FinCEN

- Exemptions
  - **Guidance on Determining Eligibility for Exemption from Currency Transaction Reporting Requirements** (2012) by FinCEN
  - **Bank Secrecy Act Designation of Exempt Person (FinCEN Form 110) Electronic Filing Requirements** (2012) by FinCEN
  - **Designation of Exempt Person (DOEP) and Currency Transaction Reporting (CTR): Assessing the Impact of Amendments to the CTR Exemption Rules Implemented on January 5, 2009** (2010) by FinCEN
  - **Report to Congressional Committee: Bank Secrecy Act: Increased Use of Exemption Provisions Could Reduce Currency Transaction Reporting While Maintaining Usefulness to Law Enforcement Efforts** (2008) by the United States Government Accountability Office (GAO)
  - **Guidance on Supporting Information Suitable for Determining the Portion of a Business Customer's Annual Gross Revenues that Is Derived from Activities Ineligible for Exemption from Currency Transaction Reporting Requirements** (2009) by FinCEN
  - **Definition of Motor Vehicles of Any Kind, Motor Vehicles, Vessels, Aircraft, and Farm Equipment as it Relates to Potential CTR Exemption for a Non-Listed Business** (2012) by FinCEN
  - **CTR Exemption Regulation Amended to Include MMDAs** (2000) by FinCEN
- Casinos
  - **Frequently Asked Questions: Casino Recordkeeping, Reporting, and Compliance Program Requirements** (2007, 2009, 2012) by FinCEN
  - **Casino Industry Currency Transaction Reporting: An Assessment of Currency Transaction Reports Filed by Casinos between July 1, 2006, and June 30, 2008**, by FinCEN
  - **FinCEN's Guidance on Determining Whether Tribally Owned and Operated Casinos Are Eligible for Exemption from CTR Requirements** (2002) by FinCEN

CTR Threshold and Aggregation

56. At what threshold must a CTR be filed for currency transactions?

CTRs must be filed for currency transactions in excess of $10,000. For example, a currency transaction of exactly $10,000 does not require the filing of a CTR. However, a currency transaction of $10,000.01 would.

57. Are there any circumstances under which a financial institution would need to file a CTR for amounts of $10,000 or less?

Yes. A Geographic Targeting Order (GTO) gives the U.S. Treasury Department, and in some instances states, the authority to require a financial institution or a group of financial institutions in a geographic area to file additional reports or maintain additional records above and beyond the ordinary requirements for CTRs (e.g., less than $10,000). GTOs are used to collect information on individuals/entities suspected of conducting transactions under reportable thresholds.

58. How does the $10,000 threshold apply to foreign-currency transactions?

For transactions conducted in foreign currency, the CTR requirements are applicable at the amount equivalent to more than $10,000 in U.S. dollars.

59. Has there been any consideration given to increasing the minimum threshold for CTR filing?

Periodically, there have been discussions about the benefits to the industry and law enforcement of increasing the reporting threshold. In March 2007, a bill was introduced in the U.S. House of Representatives that would, among other things, increase the CTR filing threshold to $30,000 and allow for more CTR exemptions. Such legislation could significantly reduce the burden of reporting requirements for financial institutions. In 2008, the bill expired prior to being passed by Congress. However, later that year, FinCEN amended CTR exemption rules in an effort to simplify the process for depository institutions. For further guidance, please refer to the CTR Exemptions section.

60. What does it mean to aggregate transactions for CTR filing purposes?

Multiple cash transactions conducted on a single business day by one customer must be aggregated if the financial institution has knowledge that they are by, or on behalf of, one person, and result in either cash-in or cash-out totaling more than $10,000 during any one business day. For example, if a customer deposits $6,000 in cash into his or her account at 9:30 a.m. and returns at 2:30 p.m. to make a cash loan payment of $5,000, the two transactions must be aggregated. The cash transactions of this customer total $11,000, and a CTR must be filed.

61. Are financial institutions required to aggregate transactions conducted by related entities for CTR filing purposes?

In some instances, currency transactions should be aggregated across different entities (e.g., businesses with different taxpayer identification numbers) for CTR reporting purposes. For example, if businesses are not "operated separately and independently" and the financial institution is aware of this fact, then multiple currency transactions conducted in the accounts of the related businesses must be aggregated and reported on a CTR. Factors to determine if multiple businesses are operated "separately and independently" include, but are not limited to, the following:

- Businesses are staffed by the same employees
- Bank accounts of one business are used to pay the expenses of another business
- Bank accounts are used to pay the personal expenses of the owner

62. In practice, how should financial institutions with multiple tellers and/or multiple locations identify multiple cash transactions by the same customer in a single business day?

Financial institutions with multiple tellers/locations may not always be able to identify, on a real-time basis, multiple transactions by the same customer in a single business day. For purposes of CTR filings, a "financial institution" includes all of its branches and agents. For example, a customer may make a cash deposit of $6,000 in the morning and return in the afternoon to a different teller with an additional $5,000 cash deposit. A financial institution may not be able to identify the need to file a CTR for the customer immediately. If there are multiple transactions that trigger a CTR, but the financial institution only learns a CTR is required after the customer has left, and the financial institution does not have all the information required on a CTR form, then certain items on the CTR form may be left blank and the "multiple transactions" box on the CTR form should be checked.

However, financial institutions should have procedures to monitor transactions at the close of business or on the following day to identify multiple cash transactions conducted by the same customer. Numerous software products are available to assist organizations with this effort. For additional guidance, please refer to the Large Currency Transaction Monitoring and Currency Transaction Report Filing Software section.

63. Should deposits and withdrawals be netted for CTR purposes?

No. CTRs are reported on a gross cash-in and/or cash-out basis. Deposits and withdrawals should not be netted. For example, if a customer deposits $7,500 in cash and on the same day withdraws $3,000 in cash from an ATM machine, even though the total value of cash transactions exceeds $10,000, neither the gross value of the withdrawal nor the deposit exceeds $10,000. However, in this case, a financial institution might question why the customer would want to deposit cash and withdraw cash separately on the same day. There could be a legitimate business reason for these two cash transactions, but the two transactions raise the question of whether this is suspicious activity that warrants further investigation by the financial institution and, possibly, a SAR filing.

Completion of a CTR Form

64. What identification is required for the filing of a CTR?

Prior to completing any transaction that would require a financial institution to file a CTR, financial institutions are required to do the following:

- Review an acceptable form of identification (in most cases) and verify and record the name and address of the individual presenting the transaction
- Record the full name and address, type and account number of the identification obtained, and the taxpayer identification number (TIN) (e.g., Social Security Number [SSN] or employer identification number [EIN]) of any person or entity on whose behalf such transaction is to be effected

65. What identification requirements should a financial institution implement when conducting cash transactions for noncustomers?

If cash transactions are processed for individuals who are not customers of the financial institution, procedures should exist to review an acceptable form of identification and record the name and address of individuals who conduct cash transactions at a certain threshold below the CTR requirement, so that a CTR (and, if warranted, a SAR) can be completed if multiple cash transactions are detected through monitoring.

66. What identification method is acceptable for a non-U.S. person for CTR filing purposes?

For an individual who is an alien or nonresident of the United States, a passport, cedular card, alien identification card or other official document evidencing nationality or residence can be used to verify the identity of that person. Leading practice dictates that the form of identification be current (i.e., unexpired) and bear a photograph and address.

67. If the person conducting the reportable transaction is a customer of the financial institution, does the information need to be obtained prior to the completion of the transaction?

If the financial institution previously obtained acceptable identification information and maintained it in its records, then such information may be used. For example, if documents verifying the individual's identity were reviewed and recorded on a signature card at account opening, then this may suffice. However, the financial institution still must record the method, type and number of identification on the CTR, and a statement such as "signature card on file" or "known customer" is not sufficient. Leading practice suggests that the employee handling the transaction verify, at a minimum, that all necessary information is available and accurate while the customer is present.

68. Should the amount reported in the CTR be rounded?

Yes. The dollar amount reported in the CTR should be rounded up to the nearest whole dollar.

CTR Exemptions

69. What are CTR exemptions?

CTR exemptions are designations filed by eligible financial institutions that alleviate the requirement for filing CTRs when "exempted" customers conduct (deposit or withdraw) transactions in currency that exceed $10,000 in one business day. Financial institutions that have complied properly with the exemption requirements are not liable for any failure to file a CTR for the exempt customer during the period of the exemption.

70. What is the value of CTR exemptions to depository institutions and law enforcement?

CTR exemptions reduce the compliance burden and liability on depository institutions. Additionally, they reduce the filing of CTRs that have little or no value for law enforcement investigations.

71. What types of financial institutions can grant CTR exemptions?

Only depository institutions (banks, savings associations, thrift institutions or credit unions) can grant exemptions.

72. What types of customers can be granted CTR exemptions?

The following types of customers of depository institutions can be exempted from CTR filing requirements under what are referred to as “Phase I” or “Tier I” exemptions:

- Banks, to the extent of the bank’s U.S. subsidiaries (including U.S. branches and agencies of international banks)
- Entities, to the extent of an entity’s U.S. operations that have shares or other equity interests listed on the NYSE, Amex or NASDAQ (except stock listed under “NASDAQ Small-Cap Issuers”)
- Certain subsidiaries of listed entities (see bullet point above) that are organized under U.S. law and for which at least 51 percent of the common stock is owned by the listed entity that qualifies for exemption
- Departments and agencies of federal, state or local governments
- Any entity exercising governmental authority within the United States

“Phase II” or “Tier II” exemptions permit certain nonlisted businesses as well as payroll customers to be exempted, as explained further below.

73. How can a depository institution apply for CTR exemptions?

If a depository institution wishes to designate an “exempt person,” the Designation of Exempt Person (DOEP) form must be completed and filed within 30 calendar days after the first reportable transaction to be exempted. For customers that are themselves depository institutions operating in the United States and for customers that are federal or state governmental entities, no DOEP form or annual review of the customer is required. However, the depository institution is required to file a DOEP form for, and conduct an annual review of, all other Phase I-exempt customers.

74. How do financial institutions submit DOEPs to FinCEN?

Beginning July 1, 2012, financial institutions must submit DOEPs electronically through the BSA eFiling system.

75. What significant changes were made to new DOEP forms?

Changes to the DOEP were made to more effectively capture critical data and to facilitate mandatory e-filing of DOEPs. Significant changes include, but are not limited to, the following:

- Dynamic and interactive fields that adjust subsequent required fields based on inputted information (e.g., type of financial institution, etc.) or pre-populate with enhanced data (e.g., High Intensity Financial Crime Area (HIFCA) or High Intensity Drug Trafficking Area (HIDTA) designations, etc.)
- Critical fields marked as mandatory that must be completed before acceptance
- Elimination of references to “biennial renewals” (e.g., Part V: Biennial Renewal Certification, etc.).

76. If a depository institution exempts a publicly traded company, are all the franchises of that company automatically exempt?

A depository institution must determine whether the franchisee itself is a publicly traded corporation, rather than the franchisor. In many cases, the depository institution will find that the franchise is not exempt. Only to the extent of domestic operations, subsidiaries meeting the following criteria may qualify for exemption:

- Organized under the laws of the United States.
- At least 51 percent of the common stock is owned by the listed entity that qualifies for exemption. Bank subsidiaries may not be exempted on this basis.

77. What types of nonlisted businesses are eligible for exemption?

A nonlisted business is any other commercial enterprise, to the extent of its domestic operations and only with respect to transactions conducted through its exemptible accounts, that:

- Has maintained a transaction account at the bank for at least two months
- Frequently engages in currency transactions at the bank for amounts in excess of $10,000

- Is incorporated or organized under the laws of the United States or a state, or is registered as and eligible to do business within the United States or a state and where 50 percent of its gross revenues (as opposed to sales) per year are not derived from one or more of the following ineligible activities:
    - Serving as financial institutions or agents of financial institutions of any type
    - The purchase or sale to customers of motor vehicles of any kind, or vessels, aircraft, farm equipment or mobile homes
    - The practice of law, accountancy or medicine
    - The auctioning of goods
    - The chartering or operation of ships, buses or aircraft
    - Pawn brokerage
    - Gaming of any kind (other than licensed pari-mutuel betting at race tracks)
    - Investment advisory services or investment banking services
    - Real estate brokerage
    - Title insurance and real estate closings
    - Trade union activities
    - Any other activities that may be specified by FinCEN

78. What guidance has been issued on the definition of "motor vehicles and other vessels" as it relates to CTR exemption eligibility?

FinCEN has issued an informal guide on the definitions of "motor vehicles, vessels, aircraft and farm equipment." Relying upon other federal statutes and results, these terms have been defined as follows:

- Motor vehicle includes "self-propelled vehicle or machine" (e.g., automobiles, trucks, low-speed vehicles, motorized wheelchairs, snowmobiles, scooters, mopeds, etc.)
- Vessel includes "every description of watercraft or other artificial contrivance used, or capable of being used, as a means of transportation on water" (e.g., jet skis, non-motorized boats, paddle boats, canoes, submarines, rafts, etc.)
- Aircraft includes a "device that is used or intended to be used for flight in the air" (e.g., airplanes, hang gliders, experimental planes, gliders, hot-air balloons, blimps, etc.)
- Farm equipment includes "equipment used in the production of livestock or crops, including, but not limited to, mowers, harvesters, loaders, slaughter machinery, agricultural tractors, farm engines, farm trailers, farm carts, and farm wagons, excluding automobiles and trucks"

79. How can a depository institution determine if a nonlisted business derives greater than 50 percent of gross revenue from an ineligible activity?

According to FinCEN's "Guidance on Supporting Information Suitable for Determining the Portion of a Business Customer's Annual Gross Revenues that Is Derived from Activities Ineligible for Exemption from Currency Transaction Reporting Requirements" issued in April 2009, a depository institution is not required to establish an exact percentage of gross revenue derived from ineligible activity. Instead, it is expected to conduct due diligence in order to make a reasonable determination that a nonlisted business derives no greater than 50 percent of gross revenue from an ineligible activity. At minimum, the due diligence conducted should include examining the nature of the customer's business, the purpose of the account, and the actual or expected account activity.

80. What does the term "transaction account" mean for CTR exemption purposes?

As defined in 19(b)(1)(C) of the Federal Reserve Act, 12 U.S.C. 461(b)(1)(C) and its implementing regulation, 12 CFR Part 204, the term "transaction account" means a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others. The term "transaction account" includes demand deposit accounts (DDAs), negotiable order of withdrawal (NOW) accounts, savings deposits subject to automatic transfers, and share draft accounts.

81. What does the term “payroll customer” mean for CTR exemption purposes?

A payroll customer is one that:

- Has maintained a transaction account at the bank for at least two months
- Operates a firm that frequently (i.e., five or more times per year) withdraws more than $10,000 in order to pay its U.S. employees in currency
- Is incorporated or organized under the laws of the United States or a state, or is registered as and is eligible to do business within the United States or a state

82. Are all transactions conducted by an exempted person excluded from the reporting requirement?

Exemptions may not apply to all accounts maintained or transactions conducted by an exempt customer. For example, accounts and/or transactions that are maintained or conducted other than in connection with the exempted commercial enterprise are not exemptible accounts or transactions. Therefore, a CTR would be required for reportable transactions conducted in these related accounts.

83. Can individuals be exempted from CTR filing requirements?

No. CTR exemptions cannot be granted to individuals.

84. What does the term “frequent” mean for CTR exemption purposes?

According to FinCEN’s “Guidance on Determining Eligibility for Exemption from Currency Transaction Reporting Requirements,” issued in June 2012, a customer should be conducting at least five large currency transactions throughout the year to be considered for exemption.

85. Can a depository institution grant an exemption to a new customer?

Depository institutions can immediately grant a new customer an exemption if it qualifies as a Phase I exemption. Phase II exemptions may be granted two months after establishing a transaction account, or before two months if the institution makes a risk-based decision that the customer has a legitimate business purpose for making frequent deposits based on the customer’s nature of business, customers served, location, and past relationship with the customer.

86. If customers meet the exemption criteria, are depository institutions required to grant them CTR exemption status?

Exemptions are not mandatory, and a depository institution can choose to file CTRs on the customers.

87. Should depository institutions file separate exemptions for each account or one for all accounts an eligible customer has?

A single designation of exemption should be filed for each customer at a financial institution who/that is eligible for exemption, regardless of the number of accounts held by the customer.

88. How often does a depository institution need to recertify its exempt customers?

Depository institutions that exempt customers need only make a one-time filing of the DOEP form.

89. How often should CTR-exempt customers be reviewed?

Depository institutions should review, on at least an annual basis, all their Phase II-exempt persons and entities listed on the major national stock exchanges, or subsidiaries (at least 51 percent-owned) of entities listed on the major national stock exchanges, to ensure the determination to exempt the customer continues to be valid and justified.

90. Does a financial institution need to report the revocation of exempt status to FinCEN?

No. Financial institutions are not required to file a report with FinCEN; however, they should document the reason the customer no longer meets the exemption criteria. In addition, once it is determined a customer is no longer exempt, the financial institution should begin to file CTRs for reportable transactions.

91. Is a financial institution required to back file CTRs on reportable transactions after the revocation of exempt status?

No. Financial institutions are not required to back file CTRs with respect to designated Phase II customers that were previously eligible for exemption in a preceding year.

92. If an exempt customer conducts a transaction as an agent for another customer, does the exemption apply?

No. Exemption status cannot be transferred to another customer. It is critical that employees be trained to ask customers if they are acting on their own behalf or as an agent for another person when processing a reportable transaction.

93. Can an exemption be transferred from one financial institution to another?

No. CTR exemptions do not travel with the customer from institution to institution. The new institution must follow either the Phase I or Phase II exemption requirements when granting exemptions.

94. Can an exemption be revoked?

Yes. An exemption can be revoked at any time by the depository institution that applied for it or at the request of FinCEN.

95. What are some of the reasons an exemption would be revoked?

Customers lose their automatic exemption status if they cease to be listed on an applicable stock exchange, if a subsidiary of a listed company ceases to be owned at least 51 percent by the listed company, or if they no longer meet the requirement of an exempt person and the depository institution knows of such a change.

96. Are depository institutions that do not file CTRs on exempt customers afforded any protection under the law?

A depository institution that has complied with the exemption requirements in general is not liable for any failure to file a CTR for the exempt customer for the period of the exemption. This safe harbor, however, is provided to financial institutions that did not knowingly provide false or incomplete information or have reason to believe the customer did not qualify as an exempt customer.

97. Should a depository institution maximize its ability to exempt qualified customers from the CTR filing requirement?

FinCEN encourages depository institutions to use exemption provisions to reduce the filing of CTRs that have little or no value for law enforcement investigations.

98. What are some of the reasons a depository institution does not participate in the CTR exemption process?

The most common reasons a depository institution chooses not to exempt qualified customers are:

- Additional costs associated with the exemption process (e.g., resources, system modifications)
- Fear of regulatory criticism surrounding the depository institution's exemption process
- Difficulty in determining whether a customer is eligible for exemption

CTR Evasion

99. What are some ways customers attempt to evade the filing of CTRs?

Customers can attempt to evade the filing of a CTR by structuring or "smurfing" transactions, omitting material information, providing misstatements of facts, or refusing to complete the transaction(s) altogether. All of these actions are considered criminal activities.

100. What does the term “structuring” mean?

Structuring is the attempt to evade CTR filing requirements by breaking transactions into smaller amounts, typically just below the reportable threshold (e.g., $9,999). For example, a customer may deposit $9,900 cash into his or her account on one business day and return later that day or the next day with an additional $9,000 cash deposit. The funds may be deposited in one or multiple accounts held by the customer. Without any further information about the customer, it would appear he or she may be intentionally trying to avoid the CTR filing requirement, which is a crime.

101. What does the term “microstructuring” mean?

Microstructuring is a form of structuring that involves breaking transactions into small amounts, typically ranging from $500 to $1,500, and more frequent depositing of currency into a higher number of accounts than is done in classic structuring schemes. A microstructuring scheme often involves small cash deposits followed by withdrawals conducted through international ATMs.

102. What does the term “smurfing” mean?

Smurfing is the attempt to evade CTR filing requirements and/or detection by conducting numerous transactions at different locations of either the same institution or different institutions. For example, a group of individuals may go to multiple branches of a bank and send monies to the same beneficiary, acting on behalf of the same organization or person.

103. Can a financial institution advise a customer that it can avoid reporting if it conducts transactions under the reporting limit?

Neither financial institutions nor their employees may suggest to their customers that they disaggregate transactions into smaller amounts in order to avoid reporting requirements; this would be deemed as structuring or assisting in structuring, both of which are prohibited by the Bank Secrecy Act (BSA) and are criminal acts.

104. If it appears a customer is structuring transactions, should financial institutions file a CTR?

If a customer’s cash transactions do not meet the CTR filing requirements of aggregated deposits or withdrawals in excess of $10,000 in one business day, a CTR is not warranted. However, if a financial institution suspects a customer is structuring transactions, the financial institution should file a SAR, as structuring is a criminal offense.

105. Is it a problem if a customer deliberately evades CTR filing requirements even though the source of the customer’s funds is known to be legitimate?

Yes. The CTR requirement deals with reporting of the specified currency transactions and not with the legitimacy of the funds, per se. If a financial institution believes a customer is deliberately evading a reporting requirement for any reason, it should file a SAR, regardless of the perceived legitimacy of the customer’s source of funds.

Form 8300

Form 8300 Basics

106. What is Form 8300, and when should it be used?

Form 8300 should be completed and submitted to the IRS if a person engaged in trade or business who, in the course of that trade or business, receives more than $10,000 in single or multiple related transactions in (a) cash, or (b) covered monetary instruments that are either received in a “designated reporting transaction” or in a transaction in which the recipient knows the monetary instrument is being used to try to avoid the reporting of the transaction.

107. What is the value of Form 8300?

Form 8300 is useful to the IRS and law enforcement because it can be used to trace cash movements into the retail sector of the economy and link abnormal uses of cash with possible illicit sources of that cash. Additionally, it can be used by businesses not subject to Suspicious Activity Report (SAR) filing requirements to report suspicious activity.

108. Who is subject to the Form 8300 reporting requirements?

Most businesses that receive more than $10,000 in cash while conducting their trade or business and are not subject to Currency Transaction Report (CTR) requirements must file Form 8300. Individuals also are covered under this reporting requirement. For additional guidance on who is subject to Form 8300 requirements, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

109. Do Form 8300 filing requirements also apply to government units?

Government units are not subject to Form 8300 reporting requirements, with the exception of clerks of federal or state criminal courts who receive more than $10,000 in cash as bail for the following offenses:

- Any federal offense involving a controlled substance;
- Racketeering;
- Money laundering; or
- Any state offenses substantially similar to the three listed above.

This exception became effective as of July 9, 2012.

110. What does the term "cash" mean for Form 8300 purposes?

"Cash" is defined, for Form 8300 purposes, as:

- U.S. and foreign coin and currency received in any transaction
- A cashier's check, money order, bank draft or traveler's check having a face amount of $10,000 or less received in a designated reporting transaction, or received in any transaction in which the recipient knows the instrument is being used in an attempt to avoid reporting requirements

111. What does the term "transaction" mean for Form 8300 purposes?

A "transaction" is the underlying event resulting in the transfer of more than $10,000 in cash, such as the following:

- Sale of goods, services or real or intangible property
- Rental of goods or real or personal property
- Cash exchanged for other cash
- Establishment, maintenance of or contribution to a trust or escrow account
- A loan repayment
- Conversion of cash to a negotiable instrument, such as a check or a bond

112. What does the term "designated reporting transactions" mean for Form 8300 purposes?

Designated reporting transactions include retail sales of a consumer durable (e.g., automobile, boat), a collectible (e.g., art, rug, antique, metal, gem, stamp) or travel or entertainment activity (e.g., single trip, events). However, a cashier's check, money order, bank draft or traveler's check is not covered if it constitutes the proceeds of a bank loan or is received as payment on certain promissory notes, installment sales contracts or down-payment plans.

113. Do cash payments of exactly $10,000 require a Form 8300?

No. Cash payments that aggregate to $10,000 or less do not require Form 8300 to be submitted.

114. Can Form 8300 be submitted if the $10,000 threshold is not met?

Yes, although Form 8300 would not be required to report the cash payment, it may be filed voluntarily with the Internal Revenue Service (IRS) for any suspicious transaction(s), even if the total does not exceed $10,000. For example, a business may opt to file Form 8300 to report a transaction that does not exceed $10,000 because a customer is attempting to evade reporting requirements. For additional guidance on common red flags, please refer to the Suspicious Activity Red Flags section.

115. What does the term “related transactions” mean for Form 8300 purposes?

The term “related transactions” means transactions between a buyer or agent of the buyer and a seller that occur within a 24-hour period.

In addition, transactions more than 24 hours apart are “related” if the recipient of the cash knows, or has reason to know, that each transaction is one of a series of connected transactions. A series of connected transactions occurring within a 12-month period is considered reportable on Form 8300. For example, on February 1, a customer makes an initial payment in currency to a jewelry store in the amount of $13,000 for a diamond necklace. The jewelry store receives subsequent currency payments for the necklace from the customer on March 30, April 1, and April 28 in the amounts of $5,000, $4,000 and $11,000, respectively. All payments would be considered related transactions.

116. Should additional Form 8300 be filed on subsequent related payments aggregating to over $10,000?

Each time payments aggregate in excess of $10,000, the business must file another Form 8300 within 15 calendar days of the payment that causes the payments to exceed $10,000. Using the previous example, the jewelry store must make a report by February 16 with respect to the payment received on February 1. The jewelry store also must make a report by May 13 with respect to the payments totaling $20,000 received from March 30 through April 28 (i.e., within 15 days of the date that the subsequent payments, all of which were received within a 12-month period, exceeded $10,000).

117. Are there exceptions to the Form 8300 reporting requirement?

Cash or covered monetary instruments are not required to be reported if received:

- By financial institutions required to file CTRs
- By certain casinos having gross annual gaming revenue in excess of $1 million
- By an agent who receives the cash from a principal, if the agent uses all of the cash within 15 days in a second transaction that is reportable on Form 8300 or a CTR, and discloses the name, address and taxpayer identification number (TIN) of the principal to the recipient of the cash in the second transaction
- In a transaction occurring entirely outside the United States, Puerto Rico, or a U.S. territory or possession (the negotiation of the transaction payment and delivery must all take place outside the United States)
- In a transaction that is not in the course of a person’s trade or business
- Governmental units are not required to file Form 8300, except for criminal court clerks

118. Are wholesalers subject to Form 8300 reporting requirements?

Wholesalers are required to file Form 8300 only for cash payments greater than $10,000.

They are not required to report transactions paid with cashier’s checks, bank drafts, traveler’s checks or money orders, unless they know such instruments are being used to attempt to avoid the CTR or Form 8300 reporting requirements.

119. If a retailer also conducts wholesale transactions, must it report all transactions or just the retail ones?

If the trade or business of the seller principally consists of sales to ultimate consumers, then all sales, including wholesale transactions, are considered “retail sales” and are subject to Form 8300 reporting requirements. Retail sales also include the receipt of funds by a broker or other intermediary in connection with a retail sale.

120. Who has the authority to enforce compliance of the Form 8300 requirement?

The IRS Criminal Investigation Division (IRS-CI) has the authority to investigate possible criminal violations of the Form 8300 requirement. FinCEN retained the authority to assess civil money penalties against any person who violates the Form 8300 requirement.

121. What are the consequences for failing to file Form 8300?

Businesses can be subject to civil and/or criminal penalties for failure to: file timely forms; include complete and correct information on the forms; and furnish annual notifications to the subjects of Form 8300 filings. The type and size of assessed penalties are based on the following:

- Whether the failure was negligent or willful
- Whether the failure was rectified in a timely manner (e.g., within 30 days of the date of detection)
- Whether annual gross receipts of the business exceed $5 million

Civil penalties for negligent failures to file Form 8300 may be up to $25,000 for each occurrence (not to exceed $500,000 for businesses with gross receipts under $5 million and $1.5 million for businesses with gross receipts in excess of $5 million). Criminal penalties may include fines up to $250,000 ($500,000 in the case of a corporation) and/or imprisonment up to five years, plus the costs of prosecution.

122. What is the procedure for seeking a "Reasonable Cause Penalty Waiver"?

A "Reasonable Cause Penalty Waiver" is an administrative decision from the IRS that the failure to properly file Form 8300 was due to reasonable cause and not willful neglect. Penalties for failure to file Form 8300 can be waived if the failure is due to reasonable cause and not due to willful neglect.

To obtain a Reasonable Cause Penalty Waiver, a business must submit a written statement to the IRS campus to which it must file Form 8300 with the following information:

- Specific provision(s) under which the waiver is requested (e.g., mitigating factors, events contributing to the failure)
- The facts alleged as the basis for reasonable cause
- The signature of the person required to file the forms
- Declaration that the statement is made under penalties of perjury

The filer must establish that the failure arose from events beyond the filer's control; that the filer acted in a responsible manner before and after the failure occurred; and that attempts to rectify the failure were made promptly (e.g., within 30 days after the date the impediment was removed or the failure was discovered). Special rules apply to Taxpayer Identification Number (TIN) issues.

123. What should a business do if it discovers it has failed to file Form 8300 on reportable transactions?

If a business finds it has failed to file Form 8300 on reportable transactions, it should move forward to file Form 8300 as soon as the failure is discovered. If there are a significant number of reports at issue, or if they cover transactions that are not relatively recent in time, the business should contact the IRS to request a determination on whether the back-filing of unreported transactions is necessary. Prior to doing this, the business may wish to seek advice from counsel to ensure that communication with the authorities is handled properly.

Annual Notification

124. Is a company required to inform the customer if a Form 8300 is filed?

Yes. The company must give a written or electronic statement to each person named on a required Form 8300 on or before January 31 of the year following the calendar year in which the cash is received.

125. Is a business required to notify a customer of the filing of Form 8300 at the time of sale?

No. A business is only required to inform the customer annually, as stated above. If there is only one Form 8300 filed on a customer during the year, a copy of Form 8300 can satisfy the annual statement requirement if it is sent to the last known address of the customer.

If more than one Form 8300 were filed, a single statement that aggregates the reportable transactions is required. Copies of Form 8300 are not required to be sent with the annual notification. Providing copies of Form 8300 to the payer at the time of sale does not satisfy the annual notification requirement.

It is important to note that if the suspicious transaction box was checked on Form 8300, a copy cannot be provided to the customer to satisfy the annual notification requirement. In this case, the business must send a statement with the required information in lieu of a copy of the form.

126. Is there a specific format for or guidance on how the customer should be notified of the filing of Form 8300?

There is no guidance on the format of the statement and only minimum requirements on the content of the statement. The statement can be written or electronic and must include the following:

- The name, telephone number, address and contact information of the business filing Form 8300
- The aggregate amount of reportable cash received by the person who filed Form 8300 during the calendar year in all related cash transactions
- A notification that the information contained in the statement is being reported to the IRS

127. If a business filed Form 8300 on an individual and checked the suspicious transaction box and Form 8300 was not required, does the business have to inform the individual that it filed Form 8300?

No. A business is only required to notify individuals if the filing of Form 8300 is required. More important, similar to Suspicious Activity Reports (SARs), a business is prohibited from informing the buyer that the suspicious transaction box was checked.

Filing of Form 8300

128. What is the time frame for filing Form 8300 with the IRS?

Each Form 8300 must be filed within 15 calendar days of the initial cash payment if it is more than $10,000 or within 15 calendar days after receiving the payment that causes the aggregate amount to exceed $10,000.

129. If the business is unable to obtain the TIN of a customer making a cash payment of more than $10,000, should the business file a Form 8300 anyway?

Yes. The business should file Form 8300 with a statement explaining why the taxpayer identification number (TIN) is not included. Nevertheless, as a business is required to ask for the person's TIN, it may be subject to penalties for an incorrect or missing TIN.

130. Is the business required to verify the identity of the person from whom the currency is received?

Yes. The business is required to verify the identity of the person from whom the currency is received.

131. How long should a copy of Form 8300 be retained?

A company should retain each Form 8300 for a minimum of five years from the date of filing.

132. In addition to Form 8300, should additional documentation relating to the filing be maintained?

A copy of the notice to the person named on Form 8300 also should be maintained for a minimum of five years from the date of filing.

133. Are there additional filing requirements for court clerks subject to Form 8300 reporting requirements?

Yes. By the 15th day after reportable cash bail is received, court clerks must send a copy of each Form 8300 to the U.S. attorney in the jurisdiction in which the individual charged with the specified crime resides, and the jurisdiction in which the specified crime occurred, if different.

134. How can businesses submit Form 8300 to the IRS?

Although it is not yet mandatory, Form 8300 can be submitted electronically to the IRS through the BSA E-Filing System. Paper forms should be mailed to the IRS Enterprise Computing Center – Detroit.

135. Has any guidance been issued on the reporting requirements of Form 8300?

Yes. The following guidance has been issued by the IRS on the reporting requirements of Form 8300:

- **Publication 1544, Reporting Cash Payments of Over $10,000 (Received in a Trade or Business)** (2012)
- **Form 8300 – Report of Cash Payments Over $10,000 Received in a Trade or Business (Online Video)** (2011)
- **When Businesses Should File Form 8300 for Cash Transactions (Webinar)** (2009)
- **Workbook on Reporting Cash Payments of Over $10,000** (2012)
- **FAQs Regarding Reporting Cash Payments of Over $10,000 (Form 8300)** (2012)

Reporting Suspicious Activity on Form 8300

136. Can potentially suspicious activity be reported on Form 8300?

Yes. There is a checkbox on the top of Form 8300 that indicates if the reported transaction is considered suspicious.

137. Do the details of the suspicious nature of the transaction need to be provided on Form 8300?

The details of the suspicious nature of the transaction can be provided in the "Comment" field on Form 8300. The local IRS Criminal Division or other law enforcement also can be contacted to report suspicious transactions and provide additional detail.

138. Does the Safe Harbor provision apply to reports of suspicious activity made on Form 8300?

Yes. The Safe Harbor provision applies to all reports of suspicious activity to FinCEN, whether mandatory or voluntary, including suspicious activity reported on Form 8300. For further guidance, please refer to the Safe Harbor section.

139. Can Form 8300 be submitted for suspicious activity if the $10,000 threshold is not met?

Yes. Form 8300 is not required to report the cash payment, but may be filed voluntarily with the IRS for any suspicious transaction(s), even if the total does not exceed $10,000. For example, a business may opt to file Form 8300 to report a transaction that does not exceed $10,000 because a customer is attempting to evade reporting requirements.

For additional guidance on common red flags, please refer to the Suspicious Activity Red Flags section.

Suspicious Activity Reports

The sections that follow generally outline the Suspicious Activity Report (SAR) filing requirements for depository institutions, including SAR Basics, SAR Filing Time Frame and Date of Initial Detection, Completion of a SAR Form, Confidentiality, Joint Filings of SARs, Safe Harbor, Monitoring and Terminating Relationships with SAR Subjects, Law Enforcement and SAR Trends.

For additional guidance on the SAR reporting requirements for NBFIs, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

SAR Basics

140. What is a Suspicious Activity Report?

A Suspicious Activity Report (SAR) is a report that documents suspicious or potentially suspicious activity (e.g., has no business purpose or apparent lawful purpose) attempted or conducted at or through a financial institution.

141. What is the value of SARs to law enforcement?

SARs have been instrumental in enabling law enforcement to initiate or supplement major money laundering or terrorist financing investigations. Information provided in SARs also presents FinCEN with a method of identifying emerging trends and patterns associated with financial crimes, which is vital to law enforcement agencies.

142. Who is required to file SARs?

As of the time of this publication's preparation, the following entities were required to file SARs:

- Depository institutions (including insured banks, savings associations, savings associations service corporations, credit unions, U.S. branches and agencies of foreign banks)
- Broker-dealers
- Futures commission merchants (FCM)
- Introducing brokers (IBs) in commodities
- Money services businesses (MSBs)
- Providers and sellers of prepaid access
- Casinos, card clubs
- Mutual funds
- Insurance companies
- Nonbank residential mortgage lenders or originators (RMLOs)

Additionally, bank holding companies (BHC), nonbank subsidiaries of bank holding companies, Edge and agreement corporations (and any branch thereof) are required to file SARs.

As AML regulations continue to evolve, other types of financial institutions also may be required to file SARs. Many other types of financial institutions may voluntarily file SARs. Suspicious activity can also be reported voluntarily to FinCEN through Form 8300. For further guidance, please refer to Form 8300.

143. Are there different types of SAR reports for various filers?

Beginning March 29, 2012, FinCEN replaced industry-specific SARs with a single report that must be submitted electronically. However, FinCEN will continue to accept legacy versions of the new SAR via electronic means until March 31, 2013. If a financial institution decides to continue to submit legacy reports, depository institutions (e.g., banks, thrifts, credit unions) are required to file the Suspicious Activity Report by Depository Institutions (SAR-DI). Broker-dealers, mutual funds and futures commission merchants and IBs in commodities are required to file the Suspicious Activity Report by Securities and Futures Industries (SAR-SF) for suspicious activity. MSBs file the Suspicious Activity Report by Money Services Businesses (SAR-MSB). Casinos and card clubs file the Suspicious Activity Report by Casinos and Card Clubs (SAR-C). Insurance companies should use SAR-SF and enter the words "Insurance SAR" on the first line of the narrative section until the SAR-IC is released.

For additional guidance on the SAR reporting requirements for NBFIs, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

144. What significant changes were made to SARs?

In 2012, SARs were redesigned to accommodate the different types of industries required to file these reports, to more effectively capture critical data and to facilitate mandatory e-filing of SARs. Significant changes to SARs include, but are not limited to, the following:

- Elimination of industry-specific SARs (i.e., SAR-DI, SAR-SF, SAR-MSB, SAR-C) and addition of field identifying the type of financial institution filing the SAR
- Revised sequence of sections for ease of input with ability to auto-populate certain fields based on inputs from previous sections
- Dynamic and interactive fields that adjust subsequent required fields based on inputted information (e.g., type of financial institution, etc.) or pre-populate with enhanced data (e.g., High Intensity Financial Crime Area (HIFCA) or High Intensity Drug Trafficking Area (HIDTA) designations, etc.)
- Ability to add multiple responses to certain questions (e.g., subject information, account number, etc.) or select more than one answer (e.g., suspicious activity characterization, etc.)
- Critical fields marked as mandatory that must be completed before acceptance
- Expanded suspicious activity characterization list
- Reduction of maximum number of characters in the SAR narrative from 39,000 to 17,000
- Ability to attach single, comma-separated values (CSV) files with SARs in the new section "Spreadsheet Attachments"
- Addition of North American Industry Classification System (NAICS) Code field
- Addition of fields related to Internet presence, including email address and website address
- Addition of a gender field for SAR subjects

145. What types of activities require a SAR to be filed for depository institutions?

Upon the detection of the following activities, a depository institution should file a SAR:

- **Insider abuse involving any amount** – An institution should file a SAR whenever it detects any known or suspected federal criminal violations or pattern of violations to have been committed or attempted through it or against it. An institution also should file a SAR for any transactions, regardless of the transaction amount(s) conducted through it, where the institution believes that one of its directors, officers, employees, agents or any other institution-affiliated party has committed or aided in any criminal act of which the financial institution believes it was either an actual or potential victim of a crime, or series of crimes, or was used to facilitate a criminal transaction.
- **Violations aggregating to $5,000 or more where a suspect can be identified** – A SAR should be filed in any instance where the financial institution detects or feels it was either an actual victim or a potential victim of a federal criminal violation, or detects or feels it was used as a vehicle to facilitate illicit transactions that total or aggregate $5,000 or more in funds or other assets by an identified suspect or group of suspects that it had a substantial basis for identifying. If the financial institution believes the suspect used an alias, it should document as much information as is available pertaining to the true identification of the suspect or group of suspects, including any of the alias identifiers (e.g., driver's license number, SSN, address, telephone number) and report such information.
- **Violations aggregating to $25,000 or more regardless of a potential suspect** – A SAR should be filed in any instance where the financial institution detects or feels it was either an actual victim or a potential victim of a federal criminal violation, or detects or feels it was used as a vehicle to facilitate illicit transactions that total or aggregate $25,000 in funds or other assets even if there is no substantial basis for identifying a possible suspect or group of suspects.
- **Transactions aggregating to $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act (BSA)** – A SAR should be filed when any transaction(s) totaling or aggregating to at least $5,000 conducted by a suspect through the financial institution where the institution knows, suspects or has reason to suspect that the transaction involved illicit funds or is intended or conducted to hide or disguise funds or assets derived from illegal activities (including, but not limited to, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any law or regulation or avoid any transaction reporting requirement under federal law; is designed to evade any BSA regulations; or has no business nor apparent lawful purpose or is not the type in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining available facts, including the background and possible purpose of the transaction.
- **Computer intrusion** – A SAR should be filed whenever it is discovered that access has been gained to a computer system of a financial institution either to remove, steal, procure or otherwise affect funds of the

institution, funds of the institution's customers, critical information of the institution, including customer account information, or to damage, disable or otherwise affect critical systems of the institution. Computer intrusion does not include attempted intrusions of websites or other noncritical information systems of the financial institution or customers of the institution.

For additional types of activities requiring a SAR filing for nonbank financial institutions, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section. For red flags to assist in identifying suspicious activity as outlined above, please refer to the Suspicious Activity Red Flags section.

146. What does the term "transaction" mean for SAR filing purposes?

The term "transaction" includes deposits, withdrawals, inter-account transfers, currency exchanges, extensions of credit, purchases/sales of stocks, securities or bonds, certificates of deposit or monetary instruments or investment security, automated clearing house (ACH) transactions, ATM transactions or any other payment, transfer or delivery by, through or to a financial institution, by any means.

147. Should a financial institution refuse to execute the transaction if it believes the transaction will be outlined in a future SAR filing?

In circumstances where a SAR is warranted, the financial institution is not expected to stop the processing of the transaction. However, financial institutions proceed at their own risk when continuing to allow the suspect transactions to occur.

148. Are there exceptions to the SAR filing requirement?

Yes. Robberies and burglaries that are reported to local authorities (except for savings associations and service corporations), or lost, missing, counterfeit or stolen securities that are reported through the Lost and Stolen Securities Program Database (LSSP), do not require SAR filings.

For additional guidance on exceptions to the SAR reporting requirements for NBFIs, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

149. Are transactions that were not executed exempt from the SAR filing requirement?

No. Transactions that were not executed (e.g., customer changed his or her mind before the transaction was executed) are not exempt from the requirement.

150. Where are SARs filed?

SARs are filed with FinCEN at the IRS Enterprise Computing Center – Detroit (formerly the Detroit Computing Center). They are then made available to appropriate law enforcement agencies to assist with the investigation and prosecution of criminal activity. Some states require that copies of SARs involving their state be sent to them as well.

151. How can financial institutions submit SARs to FinCEN?

Beginning July 1, 2012, FinCEN required that all SAR reports be filed through the BSA Direct E-Filing System. Further information can be found on the U.S. Treasury Department website: http://bsaefiling.fincen.treas.gov/main.html.

152. How long should financial institutions retain SARs?

SARs and the supporting documentation (original or business record equivalent) to the SAR must be retained for a minimum of five years from the date of the SAR filing. An institution also should check applicable state documentation retention laws to understand if the state requires the institution to submit to it a copy of the SAR. All supporting documentation related to a SAR must be made available to appropriate authorities upon request.

153. What does the term "supporting documentation" mean for SAR filing purposes?

The term "supporting documentation" refers to all documents or records that assisted a financial institution with making the determination that certain activity required a SAR filing and any related investigation. The amount of supporting documentation obtained during the course of the investigation (e.g., transaction records, new account information, tape recordings, e-mail messages) depends on the facts and circumstances of each investigation. A financial institution's procedures should outline how documentation is collected and stored.

Financial institutions have the ability to electronically submit supporting documentation as a CSV file within the narrative section of the SAR. While the submission of a CSV file is not required nor does it constitute a completed narrative, financial institutions should consider any additional documentation that may aid law enforcement.

154. Who should make the final decision on whether to file a SAR?

The filing of a SAR should not be a business decision, but rather a compliance decision. As such, the decision usually rests with a member of the compliance department, often the AML compliance officer.

Alternatively, some financial institutions assign the decision-making role to an AML compliance committee that should include representatives of the compliance department and senior management.

It is important to note that the board of directors only need to be notified of SAR filings – they do not need to be involved in the decision to file or not file a SAR. Prudent risk management dictates that senior management, aside from AML compliance personnel, also be apprised.

155. What information and guidance have been issued with respect to SARs?

FinCEN has issued the following key guidance to assist persons with the completion, filing and sharing of Suspicious Activity Reports (SARs):

- **The SAR Activity Review: "Trends, Tips & Issues"**
- **The SAR Activity Review: "By the Numbers"**
- **Index to Topics for The SAR Activity Review: An Assessment Based Upon Suspicious Activity Report Filing Analysis**
- **Suspicious Activity Report Supporting Documentation** (2007)
- **Unitary Filing of Suspicious Activity and Blocking Reports/Interpretation of Suspicious Activity Reporting Requirements to Permit the Unitary Filing of Suspicious Activity and Blocking Reports** (2004)
- **Unauthorized Disclosure of Suspicious Activity Reports** (2004)
- **Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies** (2006)
- Confidentiality
    - **Confidentiality of Suspicious Activity Reports** (2011)
    - **SAR Confidentiality Reminder for Internal and External Counsel of Financial Institutions** (2012)
    - **FinCEN Rule Strengthens SAR Confidentiality** (2010)
    - **Guidance on Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities** (2006)
- **BSA E-Filing System: Frequently Asked Questions (FAQs)** (2010)
- **Filing FinCEN's New Currency Transaction Report & Suspicious Activity Report** (2012)
- **Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting** (2007)
- **Requirements for Correcting Errors in Electronically Batch-Filed Suspicious Activity Reports** (2009)
- **Reporting Suspicious Activity – A Quick Reference Guide for MSBs** (No date found)
- **Suspicious Activity Reporting Guidance for Casinos** (2003)
- **How Casino SAR Reporting Has Increased Since 2004** (2012)
- **Frequently Asked Questions Suspicious Activity Reporting Requirements for Mutual Funds** (2006)
- **Frequently Asked Questions Anti-Money Laundering Program and Suspicious Activity Reporting Requirements for Insurance Companies** (2006)
- **Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption** (2008)

- **Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering** (2010)
- **FinCEN Examines Identity-Theft Related SARs Filed by Securities & Futures Firms** (2011)
- **FinCEN Study Examines Rise in Identity Theft SARs** (October 2010)
- Mortgage Fraud Related Guidance
    - **Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding Loan Modification/Foreclosure Rescue Scams** (2009)
    - **Mortgage Loan Fraud Update: Suspicious Activity Report Filings from July 1-September 30, 2009** (2010)
    - **Mortgage Loan Fraud Update** (published in *The SAR Activity Review* – Trends, Tips & Issues (Issue 16, October 2009)
    - **Suspicious Activity Related to Mortgage Loan Fraud** (August 16, 2012)
    - **FinCEN Assesses Suspicious Activity Involving Title and Escrow Companies** (2012)
    - **California, Nevada, Florida Top Mortgage Fraud SAR List** (2012)
    - **FinCEN Attributes Increase in Suspicious Activity Reports Involving Mortgage Fraud to Repurchase Demands** (2011)
    - **Mortgage Loan Fraud Connections with Other Financial Crime** (2009)
    - **Filing Trends in Mortgage Loan Fraud** (2007)
    - **Mortgage Loan Fraud: An Update of Trends Based Upon an Analysis of Suspicious Activity Reports** (2008)
    - **FinCEN Mortgage Loan Fraud Assessment** (2006)
    - **FinCEN's 2010 Mortgage Fraud Report: SAR Filings Up; Potential Abuse of Bankruptcy Identified** (2011)

The U.S. Government Accountability Office (GAO) has also issued reports to Congress on SARs and the sharing of information on suspicious activities, including, but not limited to, the following:

- **Bank Secrecy Act: FinCEN Needs to Further Develop Its Form Revision Process for Suspicious Activity Reports** (2010)
- **Bank Secrecy Act: Suspicious Activity Report Use is Increasing, but FinCEN Needs to Further Develop and Document its Form Revision Process** (2009)
- **Information Sharing: Federal Agencies are Sharing Border and Terrorism Information with Local and Tribal Law Enforcement Agencies, but Additional Efforts are Needed** (2009)
- **Information Sharing Environment: Definition of the Results to be Achieved in Improving Terrorism-Related Information Sharing is Needed to Guide Implementation and Assess Progress** (2008)
- **Intellectual Property: Better Data Analysis and Integration Could Help U.S. Customs and Border Protection Improve Border Enforcement Efforts** (2007)
- **Money Laundering: Oversight of Suspicious Activity Reporting at Bank-Affiliated Broker-Dealers Ceased** (2001)

SAR Filing Time Frame and Date of Initial Detection

156. What is the time frame for filing SARs?

SARs must be filed within 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a SAR. If the identity of the suspect is not known on the date of initial detection of the incident, a financial institution may delay filing the SAR for an additional 30 calendar days to identify the suspect. In no case may the reporting be delayed more than 60 calendar days after the date of initial detection of a reportable transaction.

157. What does the term “date of initial detection” mean for SAR filing purposes?

The period for filing a SAR begins when the financial institution, during its review of transaction or account activity or because of other factors, knows, or has reason to suspect, that the activity or transactions under review meet one or more of the definitions of suspicious activity. FinCEN recognizes that it can take some time for an institution to conduct the research to reach this conclusion, but recommends that internal reviews be as expeditious as possible. The term “date of initial detection” does not necessarily mean the moment a transaction is highlighted for review. However, an expeditious review of the transaction or account should occur, and in any event, the review should be completed in a reasonable amount of time.

In instances where a financial institution uses automated software to detect unusual transactions, the date of initial detection is usually considered the date on which the financial institution concludes that the activity is suspicious, not the date an alert was generated by the system. However, the financial institution should have protocols in place to establish the length of time after which a transaction, flagged by the system, should be investigated, and those procedures should be documented and followed.

158. What if 30 calendar days are not a sufficient amount of time for a financial institution to investigate fully the circumstances surrounding suspicious activity?

Regardless of the status of a financial institution’s internal investigation, a SAR must be filed within 30 calendar days after the date of detection, except as described below. If a financial institution has not completed its internal investigation, a SAR should be filed with the qualification that the filing is on a preliminary basis and that a follow-up SAR will be filed once the institution has completed its investigation and has more information.

Financial institutions that file follow-up SARs should ensure the follow-up SAR provides full details of the initial SAR to aid law enforcement agencies in their investigative efforts.

159. Are there any exceptions to the 30-calendar-day time frame for filing SARs?

A financial institution may take 60 calendar days after the date of initial detection to file a SAR if the identity of the suspect is not known, in order to identify the suspect.

160. What is an example in which a financial institution would have 60 calendar days to file a SAR?

One example of this might be where an individual unsuccessfully attempts a fraudulent transaction at a bank teller line. In this case, the individual may walk away without the bank obtaining any information about the customer. The bank can use the 30-calendar-day extension to obtain the identity of the individual.

In reality, the 30-calendar-day filing extension is applied in very limited circumstances, as financial institutions generally will know or will not be able to obtain at all the identity of the potential suspect(s).

161. What should a financial institution do if it “detects” reportable suspicious activity at a significantly later time than its occurrence?

The SAR filing requirements indicate that a financial institution is required to file a SAR no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a SAR. If the financial institution did not discover the suspicious activity until later, the financial institution still likely will need to file the SAR, but should consult with counsel on how best to handle the filings.

162. Should a financial institution file SARs on activity outside of the United States?

Consistent with SAR requirements, financial institutions should file SARs on suspicious activity even when a portion of the activity occurs outside of the United States or when suspicious funds originate from, or are disbursed outside of, the United States.

Although, in general, non-U.S. operations of U.S. organizations are not required to file SARs in the United States, an institution may wish, for example, to file a SAR voluntarily on activity that occurs outside of the United States, especially if it has the potential to have an impact on the reputation of the overall institution. In any case, institutions also should report suspicious activity to local authorities consistent with local laws and regulations.

Financial institutions should seek the advice of legal counsel or other appropriate advisers regarding their regulators’ expectations on filing a SAR on activity that occurs outside of the United States, but the transaction data flows through one, or more, of their U.S. systems, or otherwise involves an individual or business in the United States.

163. FinCEN has discouraged the filing of defensive SARs. What does the term “defensive SAR” mean?

A defensive SAR is one not necessarily supported by a thoughtful and thorough investigation, which may be made on cursory facts to guard against receiving citations during regulatory examinations for not filing SARs. Defensive SARs can dilute the quality of information forwarded to FinCEN and used by law enforcement and, therefore, are discouraged. Financial institutions are encouraged to implement a risk-based process for identifying potentially suspicious activity and document all decisions to file or not file a SAR to prevent regulatory criticism. Regulatory agencies continue to emphasize that examinations are focused on whether a financial institution has an effective SAR decision-making process in place, and not on individual SAR decisions, unless the failure to file a SAR is significant or accompanied by evidence of bad faith.

Completion of a SAR

164. Who should be included in Subject Information on the SAR?

A person who or an entity that is a subject of the investigation should be included in the Subject Information, on the SAR. The subject might be the account holder; it might be a party transacting business with the account holder; or, in the case of correspondent banking relationships or other clearing arrangements, it might be the customer of the financial institution’s customer. The narrative should describe the occupation, position or title of the subject, and the nature of the subject’s business. However, if more than one individual or business is involved in the suspicious activity, all subjects and any known relationships should be described in the SAR narrative.

In cases where the account holder is not the subject of the investigation, but is involved (e.g., a victim of identity theft), the names of related parties should be captured in the narrative of the SAR.

165. Should all signers of an account be included in Subject Information on the SAR?

It is at a financial institution’s discretion whether to list all signers as subjects on a SAR. For example, if there are two signers on an account, yet the activity or actions of only one is deemed suspicious, the financial institution should list only one subject on the SAR, but include the other signer in the narrative of the report.

166. What dates should be entered in Date or Date Range of Suspicious Activity on the SAR?

The Date or Date Range on the SAR is reserved for the beginning and end dates of the reported suspicious activity, not the date range in which the customer’s accounts were reviewed. For example, an account may be reviewed from January 1, 2012, to June 30, 2012, as part of an internal investigation; however, the reportable activity only may have occurred from February 4, 2012, to February 28, 2012. It is this latter date range that should be entered as the date range of suspicious activity on the SAR.

Additionally, if the activity occurred on one day, the same date will be entered for the beginning date and end date of suspicious activity.

167. What steps should a financial institution take to calculate Total Dollar Amount involved in Known or Suspicious Activity?

Suspicious activity should be reported on a gross transaction-in and transaction-out basis. Deposits and withdrawals should not be netted. Additionally, all transactions identified as suspicious should be included in the total. For example, if an individual structured cash deposits in the amount of $100,000 into his or her commercial account, and the funds were later wired out of the account to a luxury auto dealer, the total reportable suspicious activity would be $200,000. In all instances, the amount reported should be rounded up to the nearest whole dollar.

168. What steps should a financial institution take to calculate Total Dollar Amount involved in Known or Suspicious Activity, if the activity is conducted in foreign currency?

The financial institution should convert the foreign currency amount(s) into U.S. currency. The type of foreign currency should be detailed in the SAR narrative.

169. What accounts should be included in Account Number(s) Affected on the SAR?

All accounts at a financial institution in which the reportable activity was discovered should be included on the SAR with the status of the account at the time of the filing (opened/closed).

Even when it is not necessary to include additional accounts in a SAR (such as where it is determined the account was not affected by the suspicious activity), financial institutions should identify and document the review of related accounts in internal investigations leading to the SAR. As stated above, the final action of the financial institution (e.g., close account, monitor relationship, exit relationship) should be documented in the narrative of the SAR.

170. What level of detail should a financial institution include in Suspicious Activity Information Narrative on the SAR?

The Suspicious Activity Information Narrative on the SAR requires an explanation of the nature of the suspicious activity. The purpose of this section is to provide law enforcement agencies with as much information as possible to investigate the activity further. It is important that financial institutions provide sufficient detail in this section to transfer their knowledge of the activity to law enforcement agencies.

This section should provide the facts of the activity, and the narrative should cover who, what, where, when and why, including, but not limited to, the date(s), amount(s), location(s), type(s) of transaction(s), name(s) of the party(ies) involved in the transaction(s) and the alert(s)/trigger(s) that initiated the SAR. All account numbers at the institution affected by the suspicious activity should be identified and, when possible, account numbers, names and locations at other institutions as well. Transactions should be listed chronologically, individually and by type (e.g., cash, wires, checks).

Financial institutions can submit a CSV file as an attachment that details the potentially suspicious transactions to supplement information provided in the SAR narrative.

If the subject of the filing is a customer of the institution, sufficient background information about the customer should be provided, including, but not limited to, additional Know Your Customer (KYC) information, known relationships and customer statements. If the subject is not a customer, information must be provided about the party(ies) involved to the extent possible.

If previous SARs have been filed on the same party, it is important to provide references, such as the date and details of these previous filings. The narrative should “tell the story” of why the financial institution believes the transaction activity is suspicious, and clearly state the final action taken (e.g., exit relationship, monitor the relationship) in the investigation.

171. Should financial institutions submit CSV files with detailed transaction activity as a substitute for the SAR narrative?

No. The CSV attachments are considered a part of the SAR narrative and should not be submitted in lieu of a detailed SAR narrative.

172. Is a financial institution required to identify the underlying predicate crime of the SAR?

No. A financial institution is required to report suspicious activity that may involve illicit activity; a financial institution is not obligated to determine, confirm or prove the underlying predicate crime (e.g., terrorist financing, money laundering, identity theft, wire fraud). The investigation of the underlying crime is the responsibility of law enforcement.

When evaluating suspicious activity and completing the SAR report, financial institutions should, to the best of their ability, describe the suspicious activity by selecting all applicable characteristics as provided on the SAR (e.g., bribery/gratuity, defalcation/embezzlement).

173. What should a financial institution do if the SAR it submitted has errors?

FinCEN has issued specific guidance regarding correcting errors in SARs filed through the BSA Direct E-Filing System. FinCEN guidance divides the errors into two categories: Primary and Secondary Errors. Primary Errors are errors that make locating the SAR difficult or seriously degrade the quality of the SAR. Financial institutions are required to file a corrected SAR for a Primary Error. Secondary Errors are errors that violate the form’s instructions, but still allow law enforcement to understand the nature and details of the suspicious activity. Financial institutions are not required to file a corrected SAR for a Secondary Error.

Institutions should take a similar approach to correcting SARs filed manually. If an institution is uncertain whether or not it should re-file, it should consult with counsel.

174. What date should be used when filing a SAR correcting the previously filed report?

When filing a SAR that corrects a previously filed report, financial institutions should use the date that the current filing was prepared as the date of preparation.

175. When filing a SAR, should a financial institution forward supporting documentation to FinCEN?

Beginning July 1, 2012, financial institutions have the ability to electronically submit supporting documentation as a CSV file within the narrative section of the SAR. Submitting supporting documentation is not required. Whether or not the documents are submitted, such documentation should be retained by the institution for at least five years from the date the SAR is filed, or possibly longer, if a state or self-regulatory organization (SRO) has more stringent requirements. Law enforcement and/or regulators may request additional information about or supporting documentation for SARs after they are filed. The importance of a solid case management and filing system is critical in satisfying these requests within the specified time frame. The SAR should, however, within the SAR narrative, disclose the available documentation.

Confidentiality

176. What obligations do financial institutions have with respect to SAR filings?

Financial institutions are obligated to file SARs in good faith and maintain the confidentiality of the SAR filing and any information that would reveal the existence of a SAR ("SAR information"). In other words, no financial institution, and no director, officer, employee or agent of the institution which files a SAR, may notify any person or entity (or their agent, such as their attorney) involved in the transactions on which the SAR was filed that it has been reported. It is a crime to do so.

177. Does the SAR disclosure prohibition apply to supporting documentation created in an investigation that results in a SAR filing?

No. The SAR disclosure prohibition does not apply to the underlying facts, transactions and documents upon which a SAR is based. However, the confidentiality provision would apply to any documentation stating that a SAR has or has *not* been filed, as it would implicitly reveal the existence of a SAR.

178. Are there exceptions to the SAR disclosure prohibition?

Provided that no person involved in the transaction is notified that the transaction has been reported, the SAR disclosure prohibition does not include disclosures of SAR information to the following:

- FinCEN
- Any federal, state or local law enforcement agency (with jurisdiction)
- Any federal regulatory agency that examines the depository institution for compliance with the BSA
- Any state regulatory authority that examines the depository institution for compliance with state laws requiring compliance with the BSA

Guidance has also been provided by FinCEN on a depository institution's ability to share SAR information within its organizational structure to fulfill its duties under the BSA. Depository institutions may share SAR information with the following (subject to the limitation on disclosing a SAR to a party involved in the suspicious activity):

- Head office or controlling companies, whether domestic or foreign
- Domestic affiliates and subsidiaries that are also subject to SAR requirements

179. Does the confidentiality requirement for SARs prohibit a financial institution from notifying its business units that a SAR was filed involving one of its customers?

The confidentiality requirements do not preclude telling business units, although financial institutions must consider balancing "need to know" against the need to protect confidentiality. One argument for telling a business unit about a SAR filing or information that would reveal the existence of a SAR is to prevent the business unit from soliciting additional business from a client about which the compliance department may have concerns. However, the same

message may be able to be sent by alerting the business unit to the underlying activity without detailing the filing of the SAR itself.

180. Can financial institutions share SARs or any information that would reveal the existence of the SAR with its head office and controlling companies?

A U.S. branch or agency of a foreign bank may share SARs and any information that would reveal the existence of the SAR with its head office outside of the United States. Likewise, a financial institution may disclose a SAR to its holding company, no matter where the entity is located. Financial institutions should have written confidentiality agreements or arrangements in place specifying that the head office or holding company must protect the confidentiality of the SAR through appropriate internal controls.

Depository institutions are permitted to share the SAR or information related to the SAR with individuals within its corporate structure, such as directors or officers, provided "the purpose is consistent with regulations and/or guidance" and as long as the subject of the SAR is not notified the transactions have been reported.

181. Can SARs be shared with subsidiaries and affiliates?

Depository institutions are permitted to share SARs and information related to SARs to U.S. subsidiaries and affiliates as long as the subsidiary or affiliate is also subject to SAR regulations.

182. Can SARs be shared with foreign affiliates?

No. SARs or information that would reveal the existence of a SAR cannot be shared with foreign affiliates at the time of this publication.

183. Can SARs be shared under information sharing under Section 314(b) of the USA PATRIOT Act?

Information sharing under Section 314(b) of the USA PATRIOT Act enables qualifying financial institutions that have notified FinCEN, regardless of relationship, to share information concerning suspected money laundering or terrorist activity with other financial institutions. Even under this information-sharing agreement, financial institutions are not allowed to disclose the filing of SARs; only the underlying transactional and customer information may be shared. For further guidance on information sharing under 314(b), please refer to Section 314 – Cooperative Efforts to Deter Money Laundering.

184. Does contacting the customer under investigation or witnesses to obtain explanations of the potentially suspicious activity violate the confidentiality of the SAR?

No, if no mention of the SAR is made. Institutions are expected to conduct a thorough investigation of all potentially suspicious activity, which may include requesting an explanation from customers or witnesses of the purpose of the underlying transactions. However, staff members responsible for contacting customers must protect the confidentiality of the SAR filing itself, and it may be appropriate to remind them of the need for confidentiality and careful preparation for the conversation with the customer. Breaching confidentiality could jeopardize investigations conducted by law enforcement agencies and result in sanctions.

185. What is an example of a witness and when might a witness be contacted?

Witnesses might include financial institution personnel who observed a transaction taking place, or a party to a transaction who is not the suspect. A witness could be contacted at any point during an investigation by the financial institution or a law enforcement agency to clarify the facts of an investigation.

186. Should FinCEN be notified when an inquiry regarding a SAR filing is made by an unauthorized person (e.g., suspect, suspect's relatives)?

Yes. If an unauthorized person makes an inquiry regarding a SAR filing, the institution's regulator and FinCEN should be notified within a reasonable period. Except for disclosures to FinCEN, law enforcement and appropriate regulators, any person or financial institution subpoenaed, requested to produce documents that would include the SAR filing or information regarding the SAR filing within its scope, or otherwise requested to disclose a SAR or the information contained in a SAR is required to refuse to produce the SAR or provide any information that would disclose the SAR, and FinCEN should be notified promptly of the request.

Joint Filings of SARs

187. Can financial institutions jointly file a SAR?

Under certain circumstances, a joint SAR may be filed when two or more financial institutions subject to suspicious activity reporting requirements are involved in a common or related transaction, each financial institution has information about the transaction, and the SAR subject(s) is not an insider of either financial institution. However, sharing of such information must be done in compliance with regulatory guidance and applicable privacy laws.

188. What is the purpose of joint SAR filings?

Joint SAR filings by multiple financial institutions can help to reduce redundant filings on the same transactions.

189. Are there situations in which a joint SAR filing is not permissible?

Yes. A joint SAR may not be filed if the subject of the SAR is an insider of the financial institution (i.e., employed, terminated, resigned or suspended).

Safe Harbor

190. What protection is available to a financial institution when filing a SAR?

The Annunzio-Wylie Anti-Money Laundering Act of 1992 gives protection from civil liability to any covered financial institution that, or director, officer or employee who, makes a suspicious transaction report under any federal, state or local law. Section 351 of the USA PATRIOT Act further clarifies the terms of the Safe Harbor from civil liability when filing SARs. This protection does not apply if an action against an institution is brought by a government entity.

It is important to note that the Safe Harbor is applicable if a SAR is filed in good faith by a covered financial institution, regardless of whether such reports are filed pursuant to the SAR instructions. The Safe Harbor may not apply to SARs filed maliciously.

191. Have the courts upheld the Safe Harbor provision?

In 1999, in the case *Lee v. Bankers Trust Co.,* docket 98-7504, the U.S. 2nd Circuit Court of Appeals issued a verdict in favor of Bankers Trust by ruling that any statements made by Bankers Trust in a SAR could not serve as the basis of a defamation claim by the plaintiff because of the immunity provided by the Safe Harbor provision.

In 2003, in the case *Stoutt v. Banco Popular de Puerto Rico,* docket 01-2275, the U.S. 1st Circuit Court of Appeals granted summary judgment in favor of Banco Popular de Puerto Rico, dismissing Palmer Paxton Stoutt's claims for malicious prosecution, unlawful arrest and incarceration, and defamation. Stoutt argued that the original Criminal Referral Form (CRF), a predecessor of the SAR, was not filed in good faith and that the follow-up discussions with federal authorities regarding the activity reported in the CRF fell outside the scope of the statute's protection. Although criminal charges against Stoutt were later dismissed, the court upheld that Banco Popular de Puerto Rico did, by any objective test, identify a "possible violation" of the law and had filed the CRF in "good faith" and that all ordinary follow-up answers to investigators with respect to the original CRF would be footnotes to the CRF and thereby should be similarly protected.

192. Are there any examples of financial institutions losing their Safe Harbor protection?

In 2001, Carroll County Circuit Court, Western Division, found Bank of Eureka Springs and John Cross, the Bank's President and Chief Executive Officer, guilty of the malicious prosecution of their client, Floyd Carroll Evans. Bank of Eureka Springs was found to have maliciously filed two SARs on its client, misrepresented material facts to the prosecutor in regards to Evans' loan and mortgage, and attempted to derive financial benefit from the criminal prosecution by attempting to settle the case. In 2003, the Bank and Cross attempted to appeal the decision, arguing that financial institutions that file SARs in error still should be protected under the Safe Harbor provision. The original ruling was upheld by the Supreme Court of Arkansas, docket 02-623, due to a finding of overwhelming evidence of malicious intent on behalf of Bank of Eureka Springs in the first trial.

193. Does the Safe Harbor provision apply in cases of voluntary SAR filings?

Yes. The Safe Harbor provision applies to all SAR filings filed by a covered financial institution, as that term is defined in the USA PATRIOT Act, whether mandatory or voluntary.

194. Does the Safe Harbor provision apply to all parties in cases of joint SAR filings?

Yes. The Safe Harbor provision applies to all parties to a joint filing and not simply the party who files the SAR with FinCEN.

195. Does the Safe Harbor provision apply to methods of reporting suspicious activity other than actually filing a SAR?

Yes. Certain other forms of reporting, whether written or verbal, are covered by the Safe Harbor provision, so long as the other forms of suspicious activity reporting are through methods considered to be in accordance with the regulations of the applicable agency and applicable law.

196. Does the Safe Harbor provision apply to disclosure of SARs to appropriate law enforcement and supervisory agencies?

Yes. Disclosure of SARs and supporting documentation to a SAR to appropriate law enforcement and supervisory agencies with jurisdiction is protected by the Safe Harbor provisions applicable to both voluntary and mandatory suspicious activity reporting by financial institutions.

197. Does the Safe Harbor provision apply to disclosure of SARs to self-regulatory organizations (SROs)?

No. However, in 2009, FinCEN's proposed rule, "Confidentiality of Suspicious Activity Reports," would permit disclosure of SARs and supporting documentation to a SAR to SROs, with the protection of the Safe Harbor provisions applicable to both voluntary and mandatory suspicious activity reporting to FinCEN.

198. Is the Safe Harbor provision limited to SARs?

No. A "bank, and any director, officer, employee or agent of any bank, that makes a voluntary disclosure of any possible violation of law or regulation to a government agency with jurisdiction, including a disclosure made jointly with another institution involved in the same transaction, shall be protected" under the Safe Harbor provision of Section 351 of the USA PATRIOT Act.

Monitoring and Terminating Relationships with SAR Subjects

199. Who should make the final decision on whether to exit a relationship with a SAR subject?

The decision to exit a relationship with a SAR subject is really a business decision; however, increasingly, regulators are expecting that AML compliance officers will provide credible challenge to decisions that may not appear to be in the best interest of an institution. In many institutions, this decision is made by a SAR committee or other management committee that includes representation from both AML compliance and the institution's business lines.

200. Should a financial institution automatically close all accounts of customers on which SARs were filed?

Financial institutions are not obligated to close an account on which a SAR has been filed. However, because leaving an account open may subject a financial institution to legal actions, enforcement actions and reputation risk, financial institutions should have procedures in place for considering account closure, particularly in instances where multiple SARs may have been filed on the same account or customer.

201. When a financial institution decides to close an account, should the entire relationship be exited across all business units and subsidiaries?

An AML program should be managed at an enterprise level. Therefore, if a relationship is exited in one business unit or subsidiary, at a minimum, the customer's related accounts should be examined across the enterprise to determine if they should be subject to enhanced monitoring or closure. The fluid exchange of information across business units and subsidiaries, subject to applicable laws and regulations, can be just as critical in implementing an effective AML program as information sharing among financial institutions and law enforcement is in fighting money laundering and terrorist financing nationally and globally.

202. What should a financial institution do if the subject of a previous SAR filing continues to conduct suspicious transactions through the financial institution?

Regulatory agencies have recommended, as a general rule of thumb, that repeat SARs be filed at least every 90 days if suspicious transactions continue for the same party. Subsequent SARs should reference all previous SARs to assist law enforcement with following the investigation trail.

In the case of recurring suspicious activity, it is also important for a financial institution to consider the risks of continuing the business relationship with the subject of the SAR filing. A financial institution may consider the time burden of repeatedly filing SARs, as well as the potential risk of legal enforcement actions related to continuing to service such a customer, and risk to its reputation. As a result, it may consider terminating its relationship with the subject of the SAR filing, especially if suspicious activity continues. The institution may also need to immediately notify law enforcement of current ongoing suspicious activity, as further discussed in the Law Enforcement section.

203. If a financial institution exits a relationship that it deemed to be suspicious but does not file a SAR on reportable suspicious activity, has it failed to meet its SAR filing obligations?

Yes. Exiting a relationship does not absolve a financial institution's obligation to file a SAR if it detected suspicious activity. A SAR still should be filed.

204. Can law enforcement force a financial institution to exit a relationship or, conversely, request that a relationship remain open?

Law enforcement may ask a financial institution to maintain a customer relationship in order to gather more information for an investigation, or so as not to alert the suspect of a potential investigation. However, law enforcement cannot mandate that an account remain open unless there is an appropriate court order. Although unusual, regulators and law enforcement agencies can require accounts to be closed as part of an enforcement action. A financial institution should receive and maintain written records of such requests.

205. For what period should the subject of a SAR be subject to heightened scrutiny?

At a minimum, subjects of SAR filings should be monitored for 90 days to determine if the suspicious activity continues and a subsequent SAR filing is warranted. Financial institutions have taken various stances on extending the monitoring period beyond 90 days. Some financial institutions conduct enhanced scrutiny on subjects of SAR filings for a few years after the date of SAR filing (e.g., a business owner structuring $100,000 in one month).

206. What is the difference between an amended SAR and a repeat SAR filing?

An amended SAR corrects a SAR previously submitted to FinCEN. A repeat or follow-up SAR details recurring suspicious activity not included in the previous SAR(s).

Law Enforcement

207. Are there instances in which a financial institution should notify law enforcement in advance of filing a SAR?

Whenever violations require immediate attention, such as when a reportable transaction is ongoing, including, but not limited to, ongoing money laundering schemes or detection of terrorist financing, financial institutions should immediately notify law enforcement, even before the SAR is filed.

Additionally, FinCEN has established a hotline, 1.866.556.3974, for financial institutions to report to law enforcement suspicious transactions that may relate to recent terrorist activity against the United States.

208. Does notifying law enforcement of suspicious activity serve as a replacement or in any way relieve a financial institution's obligation to file a SAR?

No. Notifying law enforcement does not remove or in any way affect a financial institution's obligation to file a SAR if it detects suspicious activity.

209. What should a financial institution do upon receipt of a law enforcement inquiry?

It is important that the first step a financial institution takes upon receipt of a law enforcement inquiry is to be diligent about verifying the identity of the requester of the information. The financial institution should obtain a comfort level that the requester is a representative of an appropriate law enforcement or supervisory agency with jurisdiction, such as FinCEN. Verification procedures may include verifying the requester's employment with the requester's local field office or examining the requester's credentials in person. All procedures for verification should be incorporated into the institution's compliance program.

No information should be given to any requester prior to validating the requester's authority to request the information. Supporting documentation to a SAR is to be provided promptly upon request by law enforcement with jurisdiction; there is no need for a subpoena. However, all other requests for information must be in compliance with applicable privacy laws. A financial institution should contact its counsel if it is unsure about whether to disclose information to a law enforcement agency or needs any further guidance, and also may choose to discuss the request with its regulator or FinCEN when appropriate. Such requests also may serve as red flags for the financial institution to investigate the accounts or customer for suspicious activity.

210. Is a legal process required for disclosure of SARs or supporting documentation?

No. Financial institutions usually must confirm that disclosure of a customer's financial records to government agencies complies with the Right to Financial Privacy Act and other applicable privacy laws. However, no such requirements apply if the financial institution is providing the financial records/information supporting the SAR to FinCEN or a supervisory agency in the exercise of its "supervisory, regulatory or monetary functions" or to law enforcement with jurisdiction in the United States.

211. What transaction and customer records are financial institutions able to provide to law enforcement agencies in the United States?

Any supporting documentation related to SAR filings, such as copies of the SAR or any supporting documentation, can be given to law enforcement agencies upon their request without any need for a grand jury or other subpoena. However, global institutions should consider privacy regulations in the other countries in which they operate prior to sharing any information about foreign transactions with U.S. law enforcement or regulatory agencies that would come from cross-border offices or vice versa.

Financial institutions should consider performing an analysis of privacy regulations in each country where they operate, and seeking the advice of legal counsel when requests for information require information to be provided to cross-border offices.

It is advisable that any time a financial institution is unsure whether to disclose information to a law enforcement agency, it contact its counsel and/or primary regulator. It also may want to contact FinCEN for guidance if there is an unusual request for SAR information.

212. Should financial institutions automatically file a SAR upon receipt of law enforcement inquiries?

No. A financial institution should not automatically file a SAR upon receipt of a law enforcement inquiry. The decision to file a SAR should be based on the institution's own investigation into the activity of the party that/who is the subject of the law enforcement inquiry. A law enforcement inquiry may be relevant to a financial institution's overall risk assessment of its customers and accounts.

213. What is a National Security Letter, and should a financial institution file a SAR upon receipt of such a letter?

National Security Letters (NSLs) are written investigative demands that may be issued by the local Federal Bureau of Investigation (FBI) office and other federal governmental authorities in counterintelligence and counterterrorism investigations to obtain the following:

- Telephone and electronic communications records from telephone companies and Internet service providers
- Information from credit bureaus
- Financial records from financial institutions

NSLs are highly confidential. Financial institutions, their officers, employees and agents are precluded from disclosing to any person that a government authority or the FBI has sought or obtained access to records. Financial institutions that receive NSLs must take appropriate measures to ensure the confidentiality of the letters.

A financial institution should not automatically file a Suspicious Activity Report (SAR) upon receipt of an NSL. The decision to file a SAR should be based on the institution's own investigation into the activity of the party(ies) that/who is the subject of the NSL. If a financial institution files a SAR after receiving an NSL, the SAR should not contain any reference to the receipt or existence of the NSL. The SAR should reference only those facts and activities that support a finding of unusual or suspicious transactions identified by the financial institution.

Questions regarding NSLs should be directed to the financial institution's local FBI field office. Contact information for the FBI field offices can be found at www.fbi.gov.

214. If a financial institution decides not to file a SAR and regulatory or law enforcement agencies subsequently investigate the activity and conclude a SAR was warranted, is the financial institution liable?

If a financial institution investigated potentially suspicious activity and decided not to file a SAR as a result of its own internal investigation, the financial institution's best defense will be to have strong documentation supporting this decision. A financial institution can be liable for the failure to file a SAR if the failure was due to an insufficient AML program, weak due diligence, bad faith or other significant failure.

Thus, it is essential that financial institutions fully document internal investigations whether or not a SAR is filed. In cases where a SAR is not filed, the documentation should support the decision clearly by summarizing the reason for not filing and attaching supporting documentation. One way to help ensure investigative files are supportive of the decision to file or not file a SAR is to use an internal suspicious reporting form for the purpose of recording and summarizing the outcome of investigations.

This documentation should be retained for a minimum of five years or possibly longer (depending on the state or self-regulatory organization [SRO]) for the purpose of demonstrating (a) that the financial institution has a strong transaction-monitoring program, and (b) that an investigation of the activity was conducted in a timely manner, and the decision not to file a SAR was fully supported.

215. Has law enforcement provided any feedback on how SARs have helped with the investigation and prosecution of criminal activity?

Yes. FinCEN's *The SAR Activity Review:* "Trends, Tips & Issues" includes law enforcement investigations that were assisted by SAR information. Additional law enforcement cases can be found on FinCEN's website, www.fincen.gov, in the Law Enforcement link under Law Enforcement Cases Supported by BSA Filings. The Law Enforcement Cases Supported by BSA Filings section on FinCEN's website provides specific cases in which SAR filings assisted law enforcement with initiating, investigating and prosecuting money launderers and terrorist financiers. The section includes archives of specific cases by the following agencies:

- Federal Bureau of Investigation (FBI)
- Bureau of Immigration and Customs Enforcement (ICE)
- Internal Revenue Service-Criminal Investigation (IRS-CI)
- United States Secret Service (USSS)
- State and local law enforcement

SAR Trends

216. Is there a target number or quota of SARs a financial institution should file?

No. The number of SAR filings by a financial institution is not necessarily an indicator of the quality of the AML program. Many factors, including, but not limited to, the products and services a financial institution offers, the size and nature of its client base, and the markets in which it conducts business, will have an impact on the number of SARs filed.

217. Is there data on the number of SAR filings and trends?

Yes. FinCEN periodically issues *The SAR Activity Review:* "By the Numbers" and *The SAR Activity Review: "*Trends, Tips & Issues." "*The SAR Activity Review:* By the Numbers" includes a collection of numerical data on SARs filed by depository institutions, MSBs, casinos and card clubs, and securities and futures industries. It is generally published twice a year to cover two filing periods: January 1 to June 30 and July 1 to December 31. *The SAR Activity Review:* "By the Numbers" complements *The SAR Activity Review: "*Trends, Tips & Issues" and serves to provide information about the preparation, use and utility of SARs.

Additionally, FinCEN publishes an index of topics covered in *The SAR Activity Review* publications on its website.

218. Similar to *The SAR Activity Review*: "By the Numbers" conducted by FinCEN, should a financial institution conduct a trend analysis on its own SAR filings?

Although it is not a requirement, conducting a trend analysis on SAR filings can assist in improving the overall AML program of a financial institution.

Some SAR trends that may be useful include the following:

- Final actions on SARs (e.g., monitor, close/exit relationship)
- Nature of business/occupation of SAR suspect(s)
- Length of relationship with SAR suspect(s)
- SARs by branch(es)/line(s) of business
- SARs by jurisdiction

The better a financial institution understands the risks it faces, the more effective it can be in implementing controls to address these risks.

219. Has any feedback been provided on the quality of SARs filed?

Yes. FinCEN's "Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting," published in October 2007, outlines the most common errors found in SAR filings and ways in which these errors can be addressed. The most common errors found are as follows:

- Empty narrative fields
- Failure to explain information in supporting documents
- Inadequate narratives
- Inaccurate special responses
- Missing filer telephone number
- Missing, incomplete or invalid SSN or EIN
- Incomplete subject information; government-issued identification
- Missing category, type or characterization of suspicious activity
- Incorrect characterization of suspicious activity

220. What are some of the statistics and trends in SAR filings?

According to FinCEN, some of the statistics and trends of SAR filings include, but are not limited to, the following:

- The number of SAR filings increased from approximately 280,000 in 2002 to 1.4 million in 2011; of the 10.1 million SARs filed in the same time period, 98 percent were filed by depository institutions and money services businesses (MSB).
- Twenty-seven percent of suspicious activities reported by depository institutions in 2011 was attributed to fraud-related activities (e.g., check fraud, commercial loan fraud, consumer loan fraud, credit card fraud, debit card fraud, mortgage loan fraud, wire transfer fraud).

- The Financial Fraud Enforcement Task Force (FFETF) highlighted multiple cases in its First Year Report in 2010 in which FinCEN assisted law enforcement, including but not limited to the following:
    - Identification of 320 hedge fund firms involving $150 billion in suspicious activity
    - Identification of 241 barred members involving $382 million in suspicious activity
- The number of SARs with "identity theft" characterizations rose over 120 percent between 2004 and 2009 but has steadily declined since then; approximately 1 out of 4 victims of identity theft were familiar with the SAR subjects.
- FinCEN has issued multiple advisories related to the rise in the targeting of elders in mortgage and healthcare fraud schemes, including but not limited to reverse mortgages and Medicare fraud. According to Issue 20 of FinCEN's "SAR Activity Review," of the approximately 1,700 SARs related to "elder financial exploitation" filed during the first half of 2011:
    - The top states for elder abuse-related filings included California, Florida, Texas, New York, Washington and Hawaii;
    - Of those SARs filed by banks, the most commonly reported activities included credit card fraud, check fraud and identity theft;
    - Of those SARs filed by money services businesses (MSBs), commonly reported activities included wire transfer activity related to advance fee schemes, online dating scams, and scams involving individuals posing as friends or family members in need of emergency funds;
    - Of those SARs filed by the securities and futures industries, commonly reported activities included embezzlement, wire fraud, forgery, identity theft and check fraud.

Report of Foreign Bank and Financial Accounts

FBAR Basics

221. What is a Report of Foreign Bank and Financial Accounts?

Form TD F 90-22.1, Report of Foreign Bank and Financial Accounts (FBAR), is a report that must be filed by a United States person ("U.S. person") who has a financial interest in, or signature authority over, any foreign financial accounts, including bank, securities or other financial accounts in a foreign country, which have a maximum value exceeding US$10,000 (alone or in aggregate) at any time during a calendar year. The report must be filed with the U.S. Department of the Treasury on or before June 30 of the following calendar year.

222. What is the benefit of information reported on the FBAR to law enforcement?

Similar to other reporting mandated under the Bank Secrecy Act (BSA), the FBAR assists law enforcement in the detection of schemes by U.S. persons involving tax evasion, money laundering, terrorist financing or other criminal activities.

223. What does the term "U.S. person" mean for FBAR filing purposes?

A "U.S. person" includes a U.S. citizen, a U.S. resident for tax purposes and legal entities (including, but not limited to, corporations, partnerships, limited liability companies, trusts and estates) organized in the United States or under the laws of the United States, any state, the District of Columbia, the territories and insular possessions of the United States, or Indian Tribes. In addition, a limited liability company that is a disregarded entity for U.S. federal income tax purposes is still required to file a FBAR.

A U.S. resident for tax purposes includes an alien individual who has a permanent resident visa (i.e., "green card") or who meets a substantial presence test (e.g., generally, any alien who is present in the United States for 183 days or more in the current year, or who has been present for a weighted average of 183 days over the current year and the two preceding years, will be treated as a U.S. resident).

224. Do FBAR filing requirements apply to non-U.S. persons "in and doing business in the United States"?

No. Although the FBAR instructions issued in 2008 created uncertainty on this point, the final FBAR rules clarify that non-U.S. persons "in and doing business in the United States" are not subject to the FBAR filing requirement. However, another federal law that was enacted, the Foreign Account Tax Compliance Act (FATCA), requires foreign financial institutions to report directly to the Internal Revenue Service information about financial accounts held by U.S. taxpayers, or held by foreign entities in which U.S. taxpayers hold a substantial ownership interest. For further guidance, please refer to the Foreign Account Tax Compliance Act section.

225. Are U.S. financial institutions required to file FBARs?

Generally, yes. A U.S. financial institution that has a financial interest in a bank account, securities or other financial account in a foreign country in excess of US$10,000 is required to file an FBAR. A financial institution also may be required to file an FBAR if the financial institution maintains customer accounts in which the financial institution has a financial interest, or the financial institution has signature authority.

226. What does the term "foreign country" mean for FBAR filing purposes?

The term "foreign country" includes all geographical areas outside of the United States. For purposes of this requirement, the United States includes the states; the District of Columbia; the Commonwealth of Puerto Rico; the Commonwealth of the Northern Mariana Islands; U.S. territories and possessions, including Guam, American Samoa and the U.S. Virgin Islands; and Indian lands, as defined in the Indian Gaming Regulatory Act.

227. Are accounts held in international offices of U.S. banks exempted from FBAR filing requirements?

The geographical location of a financial account, not the nationality of the financial entity institution in which the account is found, determines whether it is an account in a foreign country. With the exception of a financial account held in a financial institution that is a U.S. military banking facility, any financial account that is located in a foreign country, even if it is held at an affiliate of a U.S. bank or other institution, is to be reported. A financial account maintained with a branch, agency or other office of a foreign bank or other institution that is located in the United States is not to be reported.

228. What does the term "financial interest" mean for FBAR filing purposes?

The term "financial interest" in a bank, securities or other financial account in a foreign country means an interest as described below:

- A U.S. person has a financial interest in each account for which such person is the owner of record or has legal title, regardless of whether the account is maintained for the U.S. person's own benefit or for the benefit of others, including non-U.S. persons.
- A U.S. person has a financial interest in each bank, securities or other financial account (including credit and debit cards) in a foreign country for which the owner of record or holder of legal title is:
    - A person acting as an agent nominee, attorney, or in some other capacity on behalf of the U.S. person with respect to the account;
    - A corporation in which the U.S. person owns directly or indirectly more than 50 percent of the total value of shares of stock or more than 50 percent of the voting power of all shares of stock;
    - A partnership in which the U.S. person owns an interest in more than 50 percent of the profits (distributive share of income) or an interest in more than 50 percent of the partnership capital;
    - A trust of which the U.S. person is the trust grantor and has an ownership interest in the trust for U.S. federal tax purposes;
    - A trust in which the U.S. person either has a present beneficial interest in more than 50 percent of the assets or from which such person receives more than 50 percent of the current income; or
    - Any other entity in which the U.S. person owns directly or indirectly more than 50 percent of the voting power, total value of equity interests or assets, or interest in profits.

229. What does the term “financial account” mean for FBAR filing purposes?

The term “financial account” includes any bank, securities brokerage, securities derivatives or other financial instruments account. Usually, such accounts also include accounts in which the assets are held in a commingled account, and the account owner holds an equity interest in the fund (such as a mutual fund, unless another filing exception applies). Bank accounts include any savings, demand, checking, deposit, time deposit or any other account (including debit card and prepaid credit card accounts) maintained with a financial institution or other person engaged in the business of a financial institution. A financial account also includes any commodity futures or options account, an insurance policy with a cash value, and shares in a mutual fund or similar pooled fund. Individual bonds, notes or stock certificates held by the filer do not qualify as a financial account, nor does an unsecured loan to a foreign trade or business that is not a financial institution.

230. What constitutes “signature authority” over an account for FBAR filing purposes?

For the purposes of FBAR filings, “signature authority” is defined as “the authority of an individual (alone or in conjunction with another individual) to control the disposition of assets held in a foreign financial account by direct communication (whether in writing or otherwise) to the bank or other financial institution that maintains the financial account.”

231. What does the term “maximum value of account” mean for FBAR filing purposes?

The term “maximum value of account” means a reasonable approximation of the greatest value of the account during the calendar year. Periodic account statements may be relied on to determine the maximum value, provided that the periodic account statements fairly reflect the maximum account value during the calendar year. If periodic account statements are not issued, the maximum account value is the largest amount of currency and nonmonetary assets in the account at any time during the year.

In the case of non-U.S. currency, the maximum account value for each account must be determined by converting the foreign currency into U.S. dollars using the U.S. Treasury’s Financial Management Service rate from the last day of the calendar year or, if not available, another verifiable exchange. The value of stock, other securities or other nonmonetary assets in an account is the fair market value at the end of the calendar year. If the asset was withdrawn from the account, the value is the fair market value at the time of the withdrawal.

232. Is an FBAR required if the foreign account did not generate interest or dividend income?

Yes. An FBAR is required regardless of whether the foreign account generated income.

233. Are there exceptions to the FBAR filing requirement?

Yes. FBARs are not required by the following:

- The spouse of an individual who has filed an FBAR if all reportable financial accounts are jointly owned with the filing spouse, the FBAR is filed in a timely manner and both spouses sign the FBAR.
- An entity that is named in a consolidated FBAR filed by its owner (an entity that has a greater than 50 percent ownership stake).
- A governmental entity of the United States (e.g., a college or university that is an agency of, an instrumentality of, owned by, or operated by a governmental entity, or an employee retirement or welfare benefit plan of a governmental entity, etc.).
- The owner or beneficiary of an IRA with respect to foreign accounts held in the IRA.
- A participant in or beneficiary of a tax-qualified retirement plan described in Internal Revenue Code sections 401(a), 403(a) or 403(b) with respect to the foreign accounts held by or on behalf of the retirement plan.
- A trust beneficiary with greater than 50 percent present beneficial interest with respect to the trust’s foreign financial accounts if the trust or the trustee of the trust is a U.S. person and files an FBAR on behalf of the trust disclosing the trust’s foreign financial accounts.
- Correspondent or nostro accounts maintained by banks for the sole purpose of bank-to-bank settlements.
- Foreign financial accounts of any international financial institution if the U.S. government is a member.

- Financial accounts maintained with U.S. military banking facilities, defined as banking facilities operated by a U.S. financial institution designated by the U.S. government to serve U.S. government installations abroad, even if the military banking facility is located in a foreign country.
- Officers or employees who have signature authority over, but no personal financial interest, in a foreign financial account maintained by their employer are not required to file FBARs on foreign financial accounts maintained by the following:
    - Financial institutions that are subject to supervision by the Office of the Comptroller of the Currency (OCC), Federal Reserve Bank (FRB), Federal Deposit Insurance Corporation (FDIC) or the National Credit Union Administration (NCUA)
    - Financial institutions that are registered with and examined by the U.S. Securities and Exchange Commission (SEC) or Commodity Futures Trading Commission (CFTC)
    - Entities that are registered with and examined by the SEC that provide services to an investment company registered under the Investment Company Act of 1940, also known as Authorized Service Providers
    - Entities that have a class of equity securities listed (or American depository receipts [ADR] listed) on any U.S. national securities exchange
    - U.S. subsidiaries of U.S. parent companies that have a class of equity securities listed on any U.S. national securities exchange, and the subsidiaries are included in a consolidated FBAR report of the U.S. parent companies
    - Entities that have a class of equity securities registered (or American depository receipts in respect of equity securities registered) under section 12(g) of the Securities Exchange Act

234. Does the new filing requirement under the Foreign Account Tax Compliance Act (FATCA) obviate the need to file an FBAR?

No. The reporting thresholds for Internal Revenue Form 8938 under FATCA and FBARs are different. Filers may be required to file one or both. Key differences include, but are not limited to, the following:

- Reporting thresholds
- Due dates
- Definition of “interest” in an account or asset
- Types of reportable foreign assets
- Valuation of reportable foreign assets

235. What key guidance has been issued related to FBARs?

The following are examples of key guidance that has been issued related to FBARs:

- **Foreign Bank and Financial Accounts Report (FBAR) Responsibilities** by FinCEN (2011)
- **Guidance on Reports of Foreign Financial Accounts (“FBARs”) Requirements for Former Employees** by FinCEN (2011)
- **Comparison of Form 8938 and FBAR Requirements** by the Internal Revenue Service (IRS) (2012)

FBAR Filing

236. What is the time frame for filing the FBAR?

For each calendar year, the FBAR must be filed with the IRS on or before June 30 of the following calendar year.

237. How should FBARs be submitted to the IRS?

FBARs can be mailed or filed electronically through the BSA Direct E-Filing System. Unlike other BSA reports, FBARs are not required to be filed electronically.

238. Should the maximum value of the account be reported in U.S. currency or the currency of the country in which the foreign account is held?

The maximum value of the account should be reported in U.S. currency.

239. What exchange rate should be used to convert the foreign currency to U.S. currency?

The IRS requires using the official exchange rate at the end of the applicable year to convert the foreign currency to U.S. currency.

240. Can a corporation file one FBAR for all of its foreign financial interests and on behalf of its subsidiaries?

Yes. A corporation that owns, directly or indirectly, more than a 50 percent interest in one or more other entities is permitted to file a consolidated FBAR form on behalf of itself and such other entities provided that the listing of those subsidiaries is made part of the consolidated report. An authorized official of the parent corporation should sign such consolidated reports.

241. How long should FBARs be retained?

FBARs must be retained for a minimum of five years from the date of filing.

242. What are the consequences for failing to file an FBAR in a timely manner?

Failure to file an FBAR may result in both civil and/or criminal penalties. The civil penalties for failing to file an FBAR may be up to $10,000 for each instance of a violation, and either $100,000 or 50 percent of the balance of the account, whichever is greater, for instances of willful violations. Willful violations may also be subject to criminal penalties. In some instances, the IRS has the discretion to decrease or terminate penalties as it deems appropriate. In the event an individual or institution discovers that he/she or it has failed to file an FBAR, a delinquent FBAR should be submitted, and a statement attached explaining why the FBAR is being filed late. It is possible for cumulative FBAR penalties to exceed the balance in the foreign financial account.

Recent Tax Scandals

243. Why have FBARs been in the news so often?

Some high-profile tax scandals have highlighted the use of non-reported foreign accounts by U.S. taxpayers. Congressional testimony reported widespread use of accounts held in foreign financial facilities located in certain foreign jurisdictions for the purpose of violating U.S. law. Secret foreign bank accounts held at foreign financial institutions allegedly permitted proliferation of white-collar crimes, and were used by U.S. citizens and others to evade income taxes, illegally conceal assets, purchase gold, and avoid security laws and regulations. Such foreign bank accounts allegedly have been used to facilitate fraud schemes, serve as sources of questionable financing for certain stock and merger activity, and allegedly facilitate conspiracies to steal from the U.S. defense and foreign aid funds, as well as commit money laundering.

244. Given the likelihood that there are a substantial number of unreported foreign accounts, has the U.S. government taken any specific steps to encourage reporting?

The IRS still encourages voluntary disclosure and considers it a factor when determining whether to recommend criminal proceedings to the U.S. Department of Justice.

Report of International Transportation of Currency or Monetary Instruments

CMIR Basics

245. What is the Report of International Transportation of Currency or Monetary Instruments?

The Report of International Transportation of Currency or Monetary Instruments (CMIR) is required to be filed by:

- Each person who physically transports, mails or ships, or causes to be physically transported, mailed or shipped, currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time from the United States to any place outside of the United States or into the United States from any place outside of the United States
- Each person who receives U.S. currency or other monetary instrument(s) in an aggregate amount exceeding $10,000 at one time, which has been transported, mailed or shipped from any place outside of the United States

246. What is the benefit of the CMIR to law enforcement?

The CMIR is useful to law enforcement because it can be used to trace the international transportation of currency or monetary instruments.

247. What does the term "persons" mean for CMIR filing purposes?

Persons are one of the following: an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, a joint venture or other unincorporated organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities perceived as legal personalities.

248. Are financial institutions required to file CMIRs?

Yes. Financial institutions are included within the definition of "person" for CMIR purposes, although financial institutions may qualify for exceptions.

249. Are there exceptions from the CMIR requirement?

CMIRs are not required to be filed by the following:

- A Federal Reserve Bank
- A bank, a foreign bank, or a broker or dealer in securities with respect to currency or other monetary instruments mailed or shipped through the postal service or by common carrier
- A commercial bank or trust company organized under the laws of any state or of the United States with respect to overland shipments of currency or monetary instruments shipped to or received from an established customer maintaining a deposit relationship with the bank, in amounts that the bank may reasonably conclude do not exceed amounts commensurate with the customary conduct of the business, industry or profession of the customer concerned
- A person who is not a citizen or resident of the United States with respect to currency or other monetary instruments mailed or shipped from abroad to a bank or broker or dealer in securities through the postal service or by common carrier
- A common carrier of passengers with respect to currency or other monetary instruments in possession of its passengers
- A common carrier of goods in respect to shipments of currency or monetary instruments not declared to be such by the shipper
- A traveler's check issuer or its agent with respect to the transportation of traveler's checks prior to their delivery to selling agents for eventual sale to the public
- A person with a restrictively endorsed traveler's check that is in the collection and reconciliation process after the traveler's check has been negotiated
- A person engaged as a business in the transportation of currency, monetary instruments and other commercial papers with respect to the transportation of currency or other monetary instruments overland between established offices of bankers or brokers or dealers in securities and foreign persons

250. Are persons transporting or shipping prepaid access devices across the U.S. border in an aggregate amount of more than $10,000 required to file a CMIR?

Not currently. However, in October 2011, FinCEN proposed amending the definition of "monetary instruments" to include tangible prepaid access devices that would be subject to reporting on CMIRs; no final rule on this proposed change has yet been issued. The term "tangible prepaid access device" has been defined as the following:

- Any physical item that can be transported, mailed, or shipped into or out of the United States and the use of which is dedicated to obtaining access to prepaid funds or the value of funds by the possessor in any manner without regard to whom the prepaid access is issued.

This definition would include devices such as general-use prepaid cards, gift cards, store cards, payroll cards, government benefit cards, and any tangible device to the extent that they can provide access to prepaid funds or the value of funds by being readable by a device employed for that purpose by merchants (e.g., cell phones, key fobs, etc.). The definition does not extend to credit and debit cards.

Similar to the exclusion for a traveler's check issuer or its agent, a business or its agent offering prepaid devices prior to their delivery to a seller for sale to the public would not be subject to the CMIR filing requirement.

FinCEN has also proposed new cross-border recordkeeping requirements for many types of electronic funds transfers.

For additional guidance on prepaid access devices, please refer to the Prepaid Access, Stored-Value and E-Cash section.

251. What value would be reported on CMIRs as it relates to prepaid access devices?

The reportable balance would be the amount available through a prepaid access device at the time of the physical transportation, mail or shipment into or out of the United States.

252. Are financial institutions required to file Reports of International Transportation of Currency or Monetary Instruments (CMIRs) on shipments of bulk currency?

Yes. Any shipment of currency outside of the United States that is greater than $10,000 must be reported via FinCEN Form 105, Reports of International Transportation of Currency or Monetary Instruments (CMIR). For additional guidance on bulk currency shipments, please refer to the Bulk Shipments of Currency section.

253. Are financial institutions required to file CMIRs on shipments of currency via the postal service?

No. Currency shipped via the postal service or common carrier is exempt from CMIR reporting, according to 31 CFR 103.23 (Reports of International Transportation of Currency or Monetary Instruments) of the Bank Secrecy Act. However, currency shipped by other methods, including via air courier or the airlines, is not exempt. For additional guidance on bulk currency shipments, please refer to the Bulk Shipments of Currency section.

254. What are the consequences for failing to file CMIRs?

Civil and/or criminal penalties for failure to file timely forms or failure to include complete and correct information on CMIR forms can include fines up to $500,000, imprisonment up to 10 years and/or seizure of funds.

CMIR Filing

255. Where are CMIRs filed?

All CMIRs should be filed with the customs officer in charge at any port of entry or departure, or as otherwise specified by the Commissioner of Customs.

256. Are CMIRs required to be filed electronically?

No. Unlike many other BSA reports, CMIRs are not required to be filed electronically.

257. What is the time frame for filing CMIRs?

CMIRs must be filed within 15 days after receipt of the currency or monetary instruments. Travelers carrying currency or monetary instruments are required to file a report at time of entry to or departure from the United States. If unaccompanied by the person entering or departing the United States, CMIRs may be filed by mail with the Commissioner of Customs on or before the date of entry, departure, mailing or shipping of the currency or monetary instruments.

258. How long should CMIRs be retained?

CMIRs must be retained for a minimum of five years from the date of filing.

Recordkeeping Requirements

259. What are the key recordkeeping requirements of the BSA for depository institutions?

The BSA requires the retention of all BSA reports (e.g., SARs, CTRs, FBARs, CMIRs). Additionally, other required documentation must be retained, such as the following:

- Each check, draft or money order drawn on the bank or issued and payable by it, except those drawn for $100 or less, or drawn on certain accounts that are expected to have at least 100 checks per month drawn on them over the course of a year
- Each item in excess of $100, other than bank charges or periodic charges made per agreement with the customer, comprising a debit to the customer's deposit account unless exempted
- Each item, including checks, drafts or transfers of credit of more than $10,000 received directly and not through a domestic financial institution, by letter, cable or any other means from a bank, broker or dealer in foreign exchange outside of the United States
- A record of each remittance or transfer of funds or of currency, other monetary instruments, checks, investment securities or credit of more than $10,000 to a person, account or place outside of the United States
- Records prepared or received by a bank in the ordinary course of business needed to reconstruct a transaction account and to trace a check in excess of $100 deposited in the account through its domestic processing system or to supply a description of a deposited check in excess of $100
- A record containing the name, address and TIN, if available, of the purchaser of each certificate of deposit, as well as a description of the instrument, a note of the method of payment and the date of the transaction
- A record containing the name, address and TIN, if available, of any person presenting a certificate of deposit for payment and a description of the instrument and date of the transaction
- A record of the statement and purpose of each loan over $10,000, except if secured by real property
- Each piece of advice, request or instruction received regarding a transaction that results in the transfer of funds, currency, checks, investment securities, other monetary instruments or credit of more than $10,000 to a person or account outside of the United States
- Each piece of advice, request or instruction given to another financial institution or person located within or outside of the United States regarding a transaction intended to result in a transfer of funds, currency, checks, investment securities, other monetary instruments or credit of more than $10,000 to a person or account outside of the United States
- Each payment order that a financial institution accepts as an originator's, intermediary's or beneficiary's bank with respect to a funds transfer in the amount of $3,000 or more
- Each document granting signature authority over each deposit account
- Each statement, ledger card or other record of each deposit account showing each transaction involving the account
- Each document relating to a transaction of more than $10,000 remitted or transferred to a person or account outside of the United States
- Each check or draft in an amount in excess of $10,000 drawn on or issued by a foreign bank that the bank has paid or presented to a nonbank drawee for payment
- Each item relating to any transaction of more than $10,000 received on any one occasion directly, and not through a domestic financial institution, from a bank, broker or dealer in foreign exchange outside of the United States
- Each deposit slip or credit ticket reflecting a transaction in excess of $100 or the equivalent record for direct deposit or wire transfer deposit transactions that shall record the amount of currency involved

- Verifying information obtained about a customer at account opening, which must be retained for five years after the date the account is closed

The above applies to banks. The BSA outlines additional requirements for other types of financial institutions (e.g., currency dealers or exchangers, broker-dealers, casinos). For further guidance on the additional recordkeeping requirements for other types of financial institutions, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

Funds Transfer Recordkeeping Requirement and the Travel Rule

Funds Transfer Recordkeeping Requirement and the Travel Rule Basics

260. What is the Funds Transfer Recordkeeping Requirement?

The basic requirements of the Funds Transfer Recordkeeping Requirement vary depending on the role the financial institution plays in the funds transfer (e.g., originating institution, intermediary institution, beneficiary institution).

For each funds transfer of $3,000 or more, the originating institution shall obtain and retain the following information relating to the payment order:

- The name and address of the originator
- The amount of the payment order
- The execution date of the payment order
- Any payment instructions received from the originator with the payment order
- The identity of the beneficiary's bank
- As many of the following items as are received with the payment order:
    - The name of the beneficiary
    - The address of the beneficiary
    - The account number of the beneficiary
    - Any other specific identifier of the beneficiary

Nonbank financial institutions also must retain any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.

For each funds transfer of $3,000 or more that the financial institution accepts as an intermediary or beneficiary institution, the institution shall retain a record of the payment order (e.g., original record, microfilm).

261. Do the obligations of a financial institution differ for funds transfers involving noncustomers?

Yes. A financial institution must consider three factors when assessing its obligations. These factors include whether the financial institution is the sending/receiving institution, if the payment order/proceeds are not made/delivered in person, and whether the funds are sent or received by an agent of the originator/beneficiary. The requirements imposed on the financial institution vary from collecting information about the originator, beneficiary and agent (where applicable) and include name and address, type and number of identification reviewed, TIN, and copy or record of the method of payment. Additionally, the financial institution must verify identity under certain circumstances.

262. What is the Travel Rule?

The Travel Rule refers to the requirement for financial institutions that participate in funds transfers of $3,000 or more to pass along certain information about the funds transfer to the next financial institution involved in the funds transmittal.

The requirements of the Travel Rule vary depending on the role the financial institution plays in the funds transfer (e.g., originating institution, intermediary institution).

The originating financial institution must forward the following information to the next financial institution in the chain:

- The name of the originator
- The account number of the originator, if used
- The address of the originator
- The amount of the payment order
- The execution date of the payment order
- The identity of the recipient's financial institution
    - As many of the following items as are received with the payment order:
    - Name of the recipient
    - Address of the recipient
    - Account number of the recipient
    - Any other specific identifier of the recipient
- Either the name and address or the numerical identifier of the originator's financial institution

A financial institution serving as an intermediary must pass on the required information listed above to the next financial institution in the chain if received from the preceding financial institution. The intermediary, however, has no obligation to obtain information not provided by the preceding financial institution.

263. What is the difference between the Funds Transfer Recordkeeping Requirement and the Travel Rule?

The Funds Transfer Recordkeeping Requirement requires each financial institution involved in funds transfers to collect and retain certain information in connection with funds transfers of $3,000 or more.

At the same time, a companion rule, the Travel Rule, requires all financial institutions to include certain information in payment orders for funds transfers of $3,000 or more.

264. Who is required to comply with the Funds Transfer Recordkeeping Requirement and Travel Rule?

The rules apply to the following:

- Banks
- Broker-dealers
- Casinos and card clubs that meet specified thresholds (e.g., annual gaming revenue)
- Money transmitters in which they meet specified thresholds
- Telegraph companies
- Futures commission merchants (FCMs) and introducing brokers (IBs) in commodities
- Any entity subject to supervision by any state or federal bank supervisory authority

265. Do the requirements imposed on nonbank financial institutions (NBFIs) differ from the requirements imposed on depository institutions?

Yes. The requirements are very similar, although the terminology differs for NBFIs. Rather than using the terms "originator," "beneficiary" and "payment order," the terminology for NBFIs is "transmitter," "recipient" and "transmittal order," respectively. NBFIs also are required to retain any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.

266. What does the term "funds transfer" mean in terms of the Funds Transfer Recordkeeping Requirement and the Travel Rule?

A funds transfer is a series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order. The term includes any payment order issued by the originator's bank or an intermediary bank intended to carry out the originator's payment order. A funds transfer is completed by acceptance by the beneficiary's bank of a payment order for the benefit of the beneficiary of the originator's payment order. Funds transfers governed by the Electronic Fund Transfer Act of 1978, as well as any other funds transfers made through an automated clearing house (ACH), Automated Teller Machine (ATM) or a point-of-sale (POS) system, are excluded from this definition.

267. What types of transmittals of funds are not subject to these rules?

Funds transfers where both the originator and the beneficiary are the same person and the originator's bank and the beneficiary's bank are the same bank are excluded. Additionally, exceptions are provided from the recordkeeping requirements for funds transfers where the originator and beneficiary (or transmitter and recipient) are:

- A domestic bank
- A wholly owned domestic subsidiary of a bank chartered in the United States
- A domestic broker or dealer in securities or a wholly owned domestic subsidiary of a broker or dealer in securities
- An FCM or IB in commodities or a wholly owned domestic subsidiary of an FCM or IB in commodities
- U.S., state or local government
- A federal, state or local government agency or instrumentality

268. Are there instances in which recordkeeping requirements are required for funds transfers of less than $3,000?

Yes. A Geographic Targeting Order (GTO) gives the U.S. Treasury Department, and in some instances states, the authority to require a financial institution or a group of financial institutions in a geographic area to file additional reports or maintain additional records above and beyond the ordinary requirements for funds transfers. GTOs are used to collect information on individuals/entities suspected of conducting transactions under a certain threshold (e.g., under $3,000).

269. Do the Funds Transfer Recordkeeping Requirement and Travel Rule require any reporting to the government of any information?

No. However, if a transmittal of funds appears to be suspicious, then a Suspicious Activity Report (SAR) is required, if the financial institution is subject to the suspicious activity reporting requirement.

270. What are the benefits of the Funds Transfer Recordkeeping Requirement and Travel Rule to law enforcement?

The Funds Transfer Recordkeeping Requirement and Travel Rule provide an audit trail regarding individuals and entities sending and receiving funds through the funds transfer system, helping law enforcement agencies detect, investigate and prosecute money laundering and other financial crimes.

271. What other AML requirements are required for funds transfers?

Apart from sanction screening requirements, which are not AML requirements per se, financial institutions are also required to screen transactions, including funds transfers, for possible OFAC Sanctions violations. For additional guidance, please refer to the sections Office of Foreign Assets Control and International Government Sanctions Programs and Blocking and Rejecting Transactions.

In instances where potentially suspicious activity is detected, a financial institution may need to file a Suspicious Activity Report (SAR). For further guidance, please refer to the Suspicious Activity Reports section.

Additionally, FinCEN recently issued a proposed rule that would impose additional recordkeeping requirements for "cross-border electronic transmittals of funds" (CBETF). For further guidance, please refer to the Cross-Border Electronic Transmittal of Funds section.

For additional guidance on the AML risks of funds transfers, please refer to the sections: High-Risk Products, Services and Transactions and Funds Transfers.

272. Do the CFPB's remittance rules impose additional AML-related requirements on financial institutions?

No. The CFPB's remittance rules, which amend Regulation E, are intended to protect consumers who send money electronically to foreign countries by providing more information about the costs of remittances. The rules apply to most international remittances regardless of their purpose, including, but not limited to funds transfers and automated clearing house (ACH) transactions. Specifically, they would require the following:

- Disclosures including:
    - A prepayment disclosure (listing the exchange rate, fees and taxes, and the amount to be delivered abroad) at the time the person initiates; and
    - A receipt disclosure which must be provided to the sender once the payment has been made.
- A provision that consumers can cancel a transfer within 30 minutes (and sometimes more) of originating it;
- Requirements that companies must investigate problems consumers report about transfers and provide standards for error resolutions;
- Companies are made responsible for mistakes made by certain people who work for them; and
- Provisions relating to transfers pre-scheduled on a regular basis.

The rules are applicable to banks, thrifts, credit unions, money transmitters and broker-dealers that consistently execute 100 or more remittance transfers per calendar year and apply to remittance transfers that are more than $15, made by a consumer in the United States, and sent to a person or company in a foreign country. The rules are effective February 7, 2013, though at the time of the publication of this Guide there continues to be significant industry pressure to delay the implementation given the perceived burden on the industry, particularly smaller institutions. The CFPB has provided model forms as well as an International Funds Transfer Small Entity Compliance Guide; these and other information related to the rules can be found on the CFPB's website at http://www.consumerfinance.gov/regulations/final-remittance-rule-amendment-regulation-e.

Addresses and Abbreviations

273. What type of address may the originator or beneficiary provide?

The Funds Transfer Recordkeeping Requirement requires the financial institution to collect and maintain the originator's or beneficiary's street address. The Travel Rule allows the address of the originator or beneficiary to be the street address or a mailing address so long as the street address is available in the originating financial institution's customer information file and it is retrievable upon law enforcement's request.

It is recommended that both the street address and mailing address be included in screenings so that Office of Foreign Assets Control (OFAC) checks can be conducted properly.

274. If a customer arranges to have his or her mail held at the financial institution, can the customer use the financial institution's address as his or her address in the funds transfer transmittal?

No. The financial institution should use the customer's address in the funds transfer transmittal.

275. Does the use of abbreviated names and mailing addresses violate the Travel Rule?

The Travel Rule does not consider the use of abbreviated trade names reflecting different accounts of a corporation (e.g., XYZ Payroll Account) and assumed names (i.e., doing business as [DBA]) or the names of unincorporated divisions or departments of the business as violations. The Funds Transfer Recordkeeping Requirement does not consider the use of a mailing address, including a post office box, as a violation either.

276. Can a financial institution use coded customer names and addresses within the funds transmittals?

No. Financial institutions need to ensure they do not use coded customer names and addresses in funds transmittals. The true name and address of the customer must be forwarded to the next financial institution in the chain.

Verification of Identity

277. What requirements are imposed on financial institutions regarding verification of identity?

There is no verification of identity requirement for established customers. An established customer is a person with an account at a financial institution or a person for whom the financial institution has obtained or maintains on file the person's name, address and TIN. Verification is, however, required for noncustomers.

278. What types of documentation can the financial institution use to verify identity?

Where verification is required, the financial institution should verify a person's identity by examining a document (other than a bank signature card) that contains the person's name, address and, preferably, photograph. The documentation used to verify the identity should be the type normally acceptable by financial institutions as a means of identification when cashing checks for a person other than an established customer.

Verification of the identity of an individual who indicates that he or she is an alien or is not a resident of the United States may be made by passport, alien identification card, or other official document evidencing nationality or residence (e.g., a foreign driver's license with indication of home address).

279. Can a bank signature card be used to verify identity?

No. The Funds Transfer Recordkeeping Requirement explicitly prohibits use of a bank signature card for verifying identity.

Joint Party Transmittals and Aggregation

280. How should joint party transmittals of funds be treated?

When a transmittal of funds is sent to more than one recipient, the originator's financial institution may select one recipient as the person whose information must be passed. When a transmittal of funds is sent by more than one originator, the originator's financial institution should select the account holder who ordered the transmittal of funds (in the case of joint accounts) as the person whose information must be passed. In all other instances where more than one originator sends funds, the financial institution may choose one person whose information must be passed. However, records on all parties must be kept.

281. How should aggregated transmittals of funds be treated?

A financial institution becomes the originator when it aggregates separate originators from separate transmittals of funds. Similarly, a financial institution becomes the recipient when it combines separate recipients from separate payment orders. However, records on all parties must be kept.

282. If a corporation has one or several individuals who are authorized by the corporation to order funds transfers through the corporation's account, who is the originator in such a transfer?

The corporation, and not the individual(s) authorized to issue the order on behalf of the corporation, is the originator. Accordingly, the information must be retrievable by the name of the corporation, not by the name of the individual ordering the funds transfer.

283. Who is the originator in a transaction where a trustee initiates a funds transfer on behalf of the trust?

The trust is the originator of the funds transfer, and not the trustee initiating the funds transfer. The trustee is merely the person authorized to act on behalf of the trust, a separate legal entity, similar to authorized signers on a corporate account.

Retrievability

284. What are the retrievability requirements of the Funds Transfer Recordkeeping Requirement?

The information a financial institution must obtain and retain, as required, should be retrievable by the name of the originator or beneficiary. The information also should be retrievable by account number if the originator/beneficiary is an established customer of the financial institution and has an account used for funds transfers.

285. Are financial institutions required to maintain records in a specific format?

No. Financial institutions can decide on the format, as long as the financial institution can retrieve the information required in a reasonable period of time.

286. What is the time frame allotted for retrieving records?

There is no specific time frame prescribed with respect to the Funds Transfer Recordkeeping Requirement. FinCEN, however, has indicated that records should be accessible within a reasonable period, considering the quantity of records requested, the nature and age of the records, and the amount and type of information provided by the law enforcement agency making the request, as well as the financial institution's transaction volume and capacity to retrieve the records.

Financial institutions are, however, required to retrieve records relating to correspondent banking activity within 120 hours of a request made by a regulatory agency. For further guidance on the "120-Hour Rule," please refer to Section 319(b) Requirements – Bank Records.

Cross-Border Electronic Transmittal of Funds

287. Are any additional reporting requirements under consideration with regard to funds transfers?

Yes. In September 2010, FinCEN issued Notice of Proposed Rulemaking RIN 1506-AB01, "Cross-Border Electronic Transmittals of Funds." The proposed rule would require banks and money transmitters to report specified information on cross-border electronic transmittal of funds (CBETF), which are defined as "transmittal[s] of funds where either the transmittal order or the advice is communicated by electronic means and sent or received by either a first-in or last-out financial institution."

Banks would be required to report on all CBETFs; money transmitters would be limited to reporting on CBETFs greater than or equal to $1,000, or the equivalent in other currencies.

288. What are "first in" and "last out" financial institutions?

A first-in financial institution is "the first financial institution with respect to a transmittal of funds that receives a transmittal order or advice from a foreign financial institution." A last-out financial institution is "the last financial institution with respect to a transmittal of funds that sends a transmittal order or advice to a foreign financial institution."

289. What information does the proposal indicate would need to be reported on CBETFs?

As proposed, the following information would be required to be reported to FinCEN on CBETFs:

- Unique transaction identifier number
- Either the name and address or the unique identifier of the transmitter's financial institution
- Name and address of the transmitter
- The account number of the transmitter (if applicable)
- The amount and currency of the transmittal of funds
- The execution date of the transmittal of funds
- The identity of the recipient's financial institution

- The name and address of the recipient
- The account number of the recipient (if applicable)
- Any other specific identifiers of the recipient or transaction
- For transactions of $3,000 or more, reporting money transmitters shall also include the U.S. taxpayer identification number of the transmitter or recipient (as applicable) or, if none, the alien identification number or passport number and country of issuance

290. How would financial institutions submit the required information to FinCEN?

If a final rule is adopted, financial institutions would submit electronic copies of fund transmittal orders to FinCEN to fulfill reporting requirements.

291. When would reporting be required?

Reports would be required to be filed within five business days following the day the bank or money transmitter sent or received the transmittal order.

Additionally, all banks would be required to submit an annual report to FinCEN that provides the number of the account that was credited or debited to originate or receive a CBETF and the U.S. taxpayer identification number of the respective account holder.

292. Are there any exceptions to the proposed rule?

The following electronic transmittals would be exempt from the proposed rule:

- Cross-border electronic transmittals of funds where either the transmitter is a bank and the recipient is a foreign bank, or the transmitter is a foreign bank and the recipient is a bank and, in each case, there is no third-party customer to the transaction; or
- The transmittal order and advice of the transmittal order are communicated solely through systems proprietary to a bank.

293. What would the impact of the proposed rule be?

Estimates suggest that approximately 300 banks and 700 MSBs would be affected by the proposed rule and that the proposed reporting thresholds would result in some 500 to 700 million reports per year.

Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments

294. How are monetary instruments defined for the purpose of recordkeeping requirements for the purchases and sales of these instruments?

A monetary instrument is defined as follows:

- Bank check or draft
- Foreign draft
- Cashier's check
- Money order
- Traveler's check

295. Are prepaid access devices considered monetary instruments for the purpose of recordkeeping requirements for the purchases and sales of these instruments?

No. Prepaid access devices are not considered monetary instruments for the purposes of the recordkeeping requirements for the purchase and sale of monetary instruments. However, in October 2011, FinCEN proposed

amending the definition of "monetary instruments" to include tangible prepaid access devices that would be subject to reporting on Reports of International Transportation of Currency or Monetary Instruments (CMIRs). No final rule on this proposed change has yet been issued. For further guidance on prepaid access, please refer to the Prepaid Access, Stored-Value and E-Cash section. For further guidance on CMIRs, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

296. What documentation is required for purchases and sales of monetary instruments?

A financial institution that issues or sells for currency a monetary instrument (i.e., bank check or draft, foreign draft, cashier's check, money order, traveler's check) for amounts between $3,000 and $10,000 inclusive must first obtain the following information if the individual has a deposit account at the institution:

- The name of the purchaser
- The date of the purchase
- The type(s) of instrument(s) purchased
- The serial number(s) of each instrument(s) purchased
- The amount in dollars of each of the instrument(s) purchased

If the individual does not have a deposit account at the institution, in addition to the above, the following information must be obtained:

- Address of the purchaser
- SSN of the purchaser (or alien identification number if the purchaser is not a U.S. person)
- Date of birth (DOB) of the purchaser

297. What additional steps must the financial institution take to comply with the Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments?

In the case of deposit account holders, the financial institution also must verify that the individual is a deposit account holder (if verification of identity was previously conducted) or must verify the individual's identity. In the case of nondeposit account holders, the financial institution must verify the purchaser's name and address. Verification must be conducted in the following manner:

- Use of a signature card or other file or record at the financial institution, provided that the deposit account holder's name and address were verified previously and that information was recorded on the signature card or other file or record
- By examination of a document that is normally acceptable within the banking community as a means of identification when cashing checks

298. What is the value of the Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments rule to law enforcement?

By proactively requiring financial institutions to maintain complete records on the purchase and sale of monetary instruments for currency, law enforcement will have sufficient information available to investigate potentially suspicious transactions (e.g., identification of transaction counterparties) quickly.

299. Do the Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments apply to transactions in excess of $10,000?

No. If the transaction exceeds $10,000, Currency Transaction Report (CTR) filing requirements become applicable. For additional guidance on CTRs, please refer to the Currency Transaction Reports section.

300. Do sales of monetary instruments for currency need to be aggregated for the documentation requirements above?

The recordkeeping requirements are applicable for multiple sales of the same or different types of monetary instruments totaling $3,000 or more in one business day if the financial institution has knowledge that these sales have occurred.

301. If the purchaser of the monetary instrument is a customer of the financial institution, is the financial institution still obligated to collect the required information?

Yes. All purchases of monetary instruments for currency between $3,000 and $10,000 inclusive must be recorded, regardless of the purchaser's status as a customer of the institution. The only difference between the treatment of a customer and a noncustomer may be that the financial institution already has the required information on the customer and need only confirm its accuracy.

302. If the purchaser of the monetary instrument deposits the currency into his or her account prior to purchasing the instrument, is the financial institution still obligated to collect the required information?

Yes. The financial institution must still record the purchase of the monetary instrument for currency despite the fact that the customer deposits the currency into his or her account prior to the purchase. Depositing the currency into an account does create a paper trail; however, the purpose of the requirement is to document that currency was used to make the purchase.

303. How can a financial institution evidence its compliance with the Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments?

Though it is no longer required, financial institutions often maintain the required information in "Money Order Logs" or, more generally, "Logs of Negotiable Instruments." Maintaining electronic logs (e.g., spreadsheets, databases) as opposed to paper logs will assist with performing queries for internal investigations, 314(a) inquiries, or OFAC screenings.

304. How long should a financial institution maintain documentation supporting Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments?

Documentation must be retained for a minimum of five years. The required retention period may be longer than five years, depending on the state or self-regulatory organization (SRO).

305. What other recordkeeping and reporting requirements are required for monetary instruments?

Monetary instruments are also subject to the following recordkeeping and reporting requirements:

- **Form 8300:** Form 8300 should be completed and then submitted to the IRS if a person engaged in trade or business who, in the course of that trade or business, receives more than $10,000 in single or multiple related transactions in:
    - Cash, or
    - Covered monetary instruments that are either received in a "designated reporting transaction" or in a transaction in which the recipient knows the monetary instrument is being used to try to avoid the reporting of the transaction.

  For additional guidance, please refer to the Form 8300 section.

- **Report of International Transportation of Currency or Monetary Instruments (CMIR):** The CMIR is required to be filed by:
    - Each person who physically transports, mails or ships, or causes to be physically transported, mailed or shipped, currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time from the United States to any place outside of the United States or into the United States from any place outside of the United States; and
    - Each person who receives U.S. currency or other monetary instrument(s) in an aggregate amount exceeding $10,000 at one time, which has been transported, mailed or shipped from any place outside of the United States. For further guidance, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

Additionally, in instances where potentially suspicious activity is detected, a financial institution may need to file a Suspicious Activity Report (SAR). For further guidance, please refer to the Suspicious Activity Reports section.

For additional guidance on the AML risks of monetary instruments, please refer to the High-Risk Products, Services and Transactions and Monetary Instruments sections.

USA PATRIOT ACT

The sections that follow outline the USA PATRIOT Act AML Compliance Program for financial institutions, including Section 311 – Special Measures, Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks, Section 314 – Cooperative Efforts to Deter Money Laundering, Section 319 – Forfeiture of Funds in U.S. Interbank Accounts, and Section 325 – Concentration Accounts. The section also covers Section 326 – Verification of Identification, commonly referred to as the Customer Identification Program (CIP), Section 352 – AML Program and Section 505 – Miscellaneous National Security Authorities.

Overview of the USA PATRIOT Act

306. What is the USA PATRIOT Act?

The USA PATRIOT Act was signed into law by President George W. Bush on October 26, 2001, following the terrorist activity of September 11. The USA PATRIOT Act has 10 titles:

- Title I: Enhancing Domestic Security Against Terrorism
- Title II: Enhanced Surveillance Procedures
- Title III: International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001
- Title IV: Protecting the Border
- Title V: Removing Obstacles to Investigating Terrorism
- Title VI: Providing for Victims of Terrorism, Public Safety Officers and Their Families
- Title VII: Increased Information Sharing for Critical Infrastructure Protection
- Title VIII: Strengthening the Criminal Laws Against Terrorism
- Title IX: Improved Intelligence
- Title X: Miscellaneous

Title III, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, deals with money laundering and terrorist financing. Title III made significant changes to U.S. money laundering regulations, imposed enhanced requirements for AML programs, and significantly expanded the scope of coverage to nonbank financial institutions (NBFIs). It requires financial institutions to establish AML programs that include policies, procedures and controls, designation of a compliance officer, training and independent review. In addition, it requires certain financial institutions to have customer identification procedures for new accounts and enhanced due diligence (EDD) for correspondent and private banking accounts maintained by non-U.S. persons. Key provisions of the USA PATRIOT Act are detailed below.

307. To what types of institutions do the AML requirements of the USA PATRIOT Act apply?

The USA PATRIOT Act significantly expanded the type of “financial institution” subject to AML requirements. Many people assume that “financial institution” simply means “traditional” financial service company (e.g., banks, broker-dealers, insurance companies). However, the USA PATRIOT Act broadly defines “financial institutions” so that the definition includes, but is not necessarily limited to:

- Insured banks
- Commercial banks
- Trust companies
- Private banks
- Agency or branch of a foreign bank in the United States
- Credit unions
- Thrift and savings institutions
- Broker-dealers registered or required to register with the Securities and Exchange Commission (SEC)
- Securities/commodities broker-dealers
- Futures commission merchants (FCMs), introducing brokers (IBs), commodity pool operators (CPOs) and commodity trading advisers (CTAs) registered or required to register under the Commodity Exchange Act (CEA)
- State-licensed or Indian casinos with annual gaming revenue of more than $1 million
- Investment bankers
- Investment companies
- Currency exchanges
- Issuer or seller of traveler's checks, money orders or similar instruments
- Licensed sender of money or any other person who engages as a business in the transmission of funds, formally or informally
- Operators of credit card systems
- Insurance companies
- Dealers in precious metals, stones or jewels
- Pawnbrokers
- Loan or finance companies
- Travel agencies
- Telegraph companies
- Businesses engaged in vehicle sales, including automobile, airplane and boat sales
- Persons involved in real estate closings and settlements
- The U.S. Postal Service
- Agencies of the federal government or any state or local government carrying out a duty or power of a business described in the definition of a "financial institution"
- Any business or agency that engages in any activity that the Secretary of the Treasury determines, by regulation, to be an activity that is similar to, related to, or a substitute for any activity in which any of the above entities are authorized to engage
- Any other business, designated by the U.S. Secretary of the Treasury, with cash transactions that have a high degree of usefulness in criminal, tax or regulatory matters

It is important to understand, however, that not all provisions of the USA PATRIOT Act apply to all financial institutions. Some of the differences in application are highlighted in this publication.

For additional guidance relating to definitions of NBFIs (e.g., casinos, money services businesses [MSBs], broker-dealers), refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

308. Are foreign financial institutions subject to the requirements of the USA PATRIOT Act?

The requirements of the USA PATRIOT Act apply to the U.S. operations of foreign financial institutions in the same manner that they apply to domestic financial services companies. As a practical matter, however, non-U.S. offices of foreign financial institutions will find that they are directly and indirectly affected by USA PATRIOT Act requirements in their efforts to support the AML Compliance Programs of their U.S.-based operations.

309. What is the applicability of the USA PATRIOT Act to foreign subsidiaries and branches of U.S. financial institutions?

Foreign subsidiaries and branches of U.S. financial institutions must comply with some, but not all, U.S. AML laws and regulations. In addition, a foreign subsidiary or branch also must comply with the AML laws and regulations of the jurisdictions in which it operates. U.S. financial institutions with international operations, therefore, need to be aware of AML laws and regulations globally to ensure subsidiaries and branches operating outside of the United States are in compliance with host country AML regulations, as well as U.S. AML requirements.

310. Does the USA PATRIOT Act in any way impact non-U.S. financial institutions without a U.S. presence?

Even though the specific requirements of the USA PATRIOT Act are not applicable to foreign financial institutions that operate exclusively outside of the United States, the USA PATRIOT Act, nonetheless, has a significant impact on financial institutions across the globe.

Specifically, Sections 311, 312, 313, 314, 319, 326 and 352 of the USA PATRIOT Act can have significant effects on non-U.S. financial institutions. These sections are discussed in further detail below. In summary, these requirements could result in the following:

- Additional information requests about the financial institution itself and its customers if their transactions are processed through a U.S. financial institution
- Seizures of a financial institution's funds maintained in an account in the United States
- Sanctions against either the financial institution itself or the country from which it operates

These measures are far-reaching; global financial institutions must be aware of their potentially significant impact.

311. What are the key provisions of the USA PATRIOT Act?

The following is a summary of the key provisions of the USA PATRIOT Act:

- Section 311 – Special Measures for Jurisdictions, Financial Institutions or International Transactions of Primary Money Laundering Concern
    - Section 311 provides the U.S. Treasury Department broad regulatory authority to impose one or more of five Special Measures against foreign jurisdictions, foreign financial institutions, and transactions and accounts that involve such foreign jurisdictions or financial institutions, if it determines that such jurisdictions, financial institutions, transactions or accounts are of primary money laundering concern. For additional guidance, please refer to Section 311 – Special Measures section.
- Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts
    - Section 312 requires special due diligence for correspondent accounts and private banking accounts maintained for non-U.S. persons. Section 312 also creates EDD standards for correspondent accounts maintained for a foreign bank operating (a) under an offshore banking license, (b) under a license issued by a country that has been designated as being noncooperative with international AML principles or procedures by an intergovernmental group or organization with which the United States agrees, or (c) under a license issued by a country subject to a Special Measure order as authorized by Section 311. For additional guidance, please refer to Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts section.
- Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks
    - Section 313 prevents financial institutions from establishing, maintaining, administering or managing correspondent accounts in the United States for foreign shell banks (i.e., a foreign bank that does not have a physical presence in any country or jurisdiction). Additionally, this section requires financial institutions to take reasonable steps to ensure that any correspondent accounts provided to a foreign

respondent are not being used by that foreign respondent to provide banking services indirectly to a foreign shell bank. Foreign shell banks affiliated with the following type of institution are exempt from this prohibition: banks that maintain a physical presence and that are subject to banking authorities in their respective countries. For additional guidance, please refer to Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks and Private Banking Accounts sections.

- Section 314 – Cooperative Efforts to Deter Money Laundering
    - Sections 314(a) and 314(b) establish procedures that encourage information sharing between governmental authorities and financial institutions, and among financial institutions, respectively. Section 314(a) establishes a mechanism for law enforcement agencies to communicate the names of suspected money launderers and terrorists to financial institutions in return for securing the ability to locate accounts and transactions involving those suspects promptly. Similarly, Section 314(b) enables financial institutions to share information relating to suspected money launderers and/or terrorists among themselves. For additional guidance, please refer to Section 314 – Cooperative Efforts to Deter Money Laundering section.
- Section 319 – Forfeiture of Funds in U.S. Interbank Accounts
    - Section 319(a) provides for seizure by U.S. authorities of funds in U.S. interbank accounts. If funds are deposited into an account at a foreign bank, and that foreign bank has an interbank account in the United States with a U.S. bank, broker-dealer or branch or agency of that foreign bank, the funds are deemed to have been deposited in the U.S. interbank account and are potentially subject to seizure. There is no requirement that the funds deposited in the U.S. interbank account be traceable to the funds deposited in the foreign bank. Section 319(b) requires that financial institutions must reply to a request for information from a U.S. regulator relating to AML compliance within 120 hours of such a request. Upon receipt of a written request from a federal law enforcement officer for information required to be maintained under Section 319(b), that information must be provided within seven days. Section 319(b) also requires U.S. depository institutions and securities broker-dealers that have correspondent accounts in the United States for foreign respondents to maintain records identifying the owners of the foreign respondent, and to maintain the name and address of a person who resides in the United States and is authorized to accept service of legal process for records regarding the correspondent account. For additional guidance, please refer to Section 319 - Forfeiture of Funds in U.S. Interbank Accounts, Domestic Financial Institution Records ("120 Hour Rule") and Foreign Bank Certifications sections.
- Section 325 – Concentration Accounts at Financial Institutions
    - Section 325 authorizes the U.S. Secretary of the Treasury to issue regulations concerning the maintenance of concentration accounts by U.S. depository institutions, with the purpose of preventing an institution's customers from anonymously directing funds into or through such accounts. (While the U.S. Treasury Department is authorized to issue such regulations, it is not required to do so, and has not done so at this time.) For additional guidance, please refer to Section 325 – Concentration Accounts at Financial Institutions.
- Section 326 – Verification of Identification
    - Section 326 requires the U.S. Treasury Department, along with each federal functional regulator, to prescribe a Customer Identification Program (CIP) with minimum standards for (a) verifying the identity of any person opening an account, (b) maintaining records of the information used to verify the person's identity, and (c) determining whether the person appears on any list of known or suspected terrorists or terrorist organizations. The requirement to establish a CIP is applicable only to certain types of financial institutions, as explained in the section on CIP. For additional guidance, please refer to Section 326 – Verification of Identification section.
- Section 351 – Amendments Relating to Reporting of Suspicious Activities
    - Section 351 clarifies the terms of the Safe Harbor from civil liability for financial institutions filing Suspicious Activity Reports (SARs). This protection does not apply if an action against an institution is brought by a government entity nor when a SAR is filed maliciously. Additionally, a bank, and any director, officer, employee or agent of any bank, that makes a voluntary disclosure of any possible violation of law or regulation to a government agency with jurisdiction, including a disclosure made jointly with another institution involved in the same transaction, shall also be protected under the Safe Harbor provision. For additional guidance, please refer to the Safe Harbor section.

- Section 352 – Anti-Money Laundering Programs
    - Section 352 requires financial institutions to establish AML programs and grants the U.S. Secretary of the Treasury authority to set minimum standards for such programs. Current minimum standards for AML programs include:
    - Development of internal policies, procedures and controls
    - Designation of a compliance officer
    - An ongoing employee training program
    - Independent testing of AML programs

  For additional guidance, please refer to Section 352 – AML Program.

- Section 353 – Penalties for Violations of Geographic Targeting Orders and Certain Recordkeeping Requirements, and Lengthening Effective Period of Geographic Targeting Orders
    - Section 353 clarifies that penalties for violation of the BSA and its implementing regulations also apply to violations of Geographic Targeting Orders (GTOs) issued by the U.S. Treasury Department and to certain recordkeeping requirements relating to funds transfers. For additional guidance, please refer to the Funds Transfer Recordkeeping Requirement and the Travel Rule section.
- Section 355 – Authorization to Include Suspicions of Illegal Activity in Written Employment References
    - Section 355 permits, but does not require, an insured depository institution to include information about the possible involvement of a current or former institution-affiliated party in potentially unlawful activity in response to a request for an employment reference by a second insured depository institution. If, however, such disclosure is done maliciously, there is no shield from liability.
- Section 356 – Reporting of Suspicious Activities by Securities Brokers and Dealers; Investment Company Study
    - Section 356(a) directs the Secretary of the Treasury to publish regulations requiring broker-dealers to file SARs. For additional guidance, please refer to the Suspicious Activity Reports and Broker-Dealers sections.
- Section 359 – Reporting of Suspicious Activities by Underground Banking Systems
    - Section 359 amends the BSA definition of money transmitter to include underground banking systems or informal value transfer systems (IVTS) in the definition of financial institution and thus subject to AML laws and regulations. For additional guidance on underground banking systems, please refer to the Informal Value Transfers Systems section.
- Section 363 – Increase in Civil and Criminal Penalties for Money Laundering
    - Section 363 increases from $100,000 to $1 million the maximum civil and criminal penalties for a violation of provisions added to the BSA.
- Section 365 – Reports Relating to Coins and Currency Received in Nonfinancial Trade or Business
    - Section 365 requires institutions that receive more than $10,000 in coins or currency from a customer, in one transaction or two or more related transactions in the course of that person's nonfinancial trade or business, to file a report (Form 8300) with respect to such transaction with FinCEN, a division of the U.S. Treasury Department. Previously, nonfinancial institutions were required to report to the IRS; they now are required to report to both FinCEN and the IRS. For additional guidance, please refer to Form 8300 section.
- Section 373 – Illegal Money Transmitting Businesses
    - Section 373 prohibits the operation of an unlicensed money transmitter. For additional guidance, please refer to the Money Services Businesses section.
- Section 505 – Miscellaneous National Security Authorities
    - Section 505 expanded the use of national security letters (NSLs), allowing their use in scrutiny of U.S. residents, visitors and U.S. citizens who are not suspects in any criminal investigation. For additional guidance, please refer to the National Security Letters section.

USA PATRIOT Act – Analysis of Key Sections

Section 311 – Special Measures

312. What requirements does Section 311, Special Measures, impose on financial institutions?

Section 311 provides the U.S. Treasury Department broad authority to impose one or more of five Special Measures against foreign jurisdictions, foreign financial institutions, classes of international transactions or types of accounts, if it determines that such jurisdictions, financial institutions, transactions or accounts are of primary money laundering concern. These Special Measures require a range of responses, from information requirements to outright prohibitions. They are as follows:

- Additional recordkeeping and reporting of certain financial transactions
- The collection of information relating to beneficial ownership of accounts
- The collection of information relating to certain payable through accounts
- The collection of information relating to certain correspondent accounts
- The prohibition or imposition of conditions on opening or maintaining correspondent or payable through accounts

313. Who is required to comply with Special Measure orders?

Domestic financial institutions and domestic financial agencies and branches are required to comply with Special Measure orders, unless exempted by the order. Offices of foreign financial institutions operating in the United States are considered domestic financial institutions and, therefore, are required to comply with Special Measure orders.

314. Who imposes a Special Measure order, and what is the process?

The U.S. Treasury Department must follow a formal rulemaking process (a) before concluding that foreign jurisdictions, foreign financial institutions, classes of international transactions or types of accounts are of primary money laundering concern, and (b) when selecting the specific measures to be imposed against the foreign jurisdictions, foreign financial institutions, classes of international transactions or types of accounts.

FinCEN collects and disseminates information relating to Section 311 and serves as the main point of contact for inquiries.

315. What factors must the U.S. Treasury Department consider before making a Special Measure designation?

The Secretary is required to consult with appropriate federal agencies and consider the following specific factors:

- Whether similar action has been or is being taken by other nations or multilateral groups;
- Whether the imposition of any particular special measures would create a significant competitive disadvantage, including any undue cost or burden associated with compliance, for financial institutions organized or licensed in the United States;
- The extent to which the action or timing of the action would have a significant adverse system impact on the international payment, clearance and settlement system, or on legitimate business activities involving the jurisdiction; and
- The effect of the action on the United States national security and foreign policy.

Where concerns extend beyond money laundering and involve terrorist financing and weapons proliferation, the Secretary is required to consider the following additional factors:

- Evidence that organized criminal groups, international terrorists, or entities involved in the proliferation of weapons of mass destruction or missiles, have transacted business in the jurisdiction;

- The extent to which that jurisdiction or financial institutions operating in that jurisdiction offer bank secrecy or special regulatory advantages to nonresidents or nondomiciliaries of the jurisdiction;
- The substance and quality of administration of the bank supervisory and counter-money laundering laws of the jurisdiction;
- The relationship between the volume of financial transactions occurring in that jurisdiction and the size of the economy of the jurisdiction;
- The extent to which that jurisdiction is characterized as an offshore banking or secrecy haven by credible international organizations or multilateral groups;
- Whether the United States has a mutual legal assistance treaty with that jurisdiction, and the experience of United States law enforcement officials and regulatory officials in obtaining information about transactions originating in or routed through or to such jurisdiction; and
- The extent to which that jurisdiction is characterized by high levels of official or institutional corruption.

316. Are Special Measure designations permanent?

Special Measure orders requiring information gathering and/or recordkeeping (e.g., collection of information relating to beneficial ownership of accounts) may not remain in effect for more than 120 days unless imposed by a regulation. In addition, the U.S. Treasury Department may rescind Special Measure orders (both information gathering/recordkeeping and prohibitions) if it determines that circumstances supporting the designation as primary money laundering concern no longer exist. The U.S. Treasury Department has, in fact, rescinded at least two Special Measure orders.

317. How can a financial institution obtain the most current listing of Special Measure orders?

The U.S. Treasury Department's proposed and final Special Measure orders can be found at www.fincen.gov/reg_section311.html.

318. How can a financial institution screen its customer base for foreign jurisdictions or foreign financial institutions that are the subject of a Special Measure order?

Many financial institutions add subjects of Special Measure orders to their sanction interdiction software to facilitate the screening process for both customers and transactions. In addition, a financial institution can contact its correspondent account holders to inform them of Special Measure orders to prevent direct/indirect use of its correspondent accounts by Special Measure subjects. For additional guidance on interdiction software, please refer to the AML Technology section.

319. Should a financial institution terminate its correspondent relationship with an entity that is the subject of a proposed Special Measure order?

A financial institution is not obligated to terminate a correspondent relationship with an entity that is the subject of a proposed Special Measure; however, it may wish to conduct due diligence on the entity and determine if it wants to continue the relationship even before a final rule imposing the Special Measure is issued.

320. What should a financial institution do if a match to a subject of a Special Measure order is confirmed?

Financial institutions should consult the final order on the entity and follow the instructions exactly as written; requirements differ among final orders. A financial institution also may contact the FinCEN hotline with questions.

Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts

Overview

321. Which financial institutions must comply with Section 312, Special Due Diligence for Correspondent Accounts and Private Banking Accounts?

The following financial institutions must comply with Section 312:

- Banks (including U.S. branches and agencies of foreign banks)
- Securities broker-dealers
- FCMs and IBs in commodities
- Mutual funds
- Uninsured trust bank or trust fund that is federally regulated and subject to AML program requirements
- Certain other entities

322. What does the term "correspondent account" mean for Section 312 purposes?

The term "correspondent account" is defined broadly for banking organizations to include any account or formal relationship established by a financial institution to receive deposits from, make payments to or other disbursements on behalf of a foreign financial institution, or to handle other financial transactions related to the foreign financial institution.

In the case of securities broker-dealers, FCMs and IBs in commodities, and mutual funds, a correspondent account would include, but not be limited to, any account or formal relationship that permits the foreign financial institution to engage in regular services, including, but not limited to, those established to engage in trading or other transactions in securities and commodity futures or options, funds transfers or other types of financial transactions.

323. What is the difference between a correspondent bank and a respondent bank?

A "correspondent bank" (correspondent) is the financial institution providing the banking services. A "respondent bank" (respondent) is the financial institution utilizing these account services, whether foreign or domestic.

324. Are accounts with domestic financial institutions included in the USA PATRIOT Act's definition of a correspondent account?

No. The money laundering and terrorist financing risk associated with these relationships is not considered as high as those associated with foreign respondents because the domestic financial institutions are subject to the same regulatory regime. Financial institutions should, however, have appropriate risk-based policies, procedures and controls to manage the AML and terrorist financing risks involved in their domestic respondents.

325. What does the term "regular" mean for Section 312 purposes?

The term "regular" is not defined in the regulation; however, it suggests an arrangement for providing ongoing services and would generally exclude infrequent or occasional transactions. Some institutions use a standard of more than one transaction per quarter.

326. Do accounts maintained for foreign affiliates fall under the definition of correspondent accounts?

Yes. Accounts maintained by a financial institution's non-U.S. branches or offices fall under the definition of a correspondent account.

327. What types of services fall under the definition of correspondent banking services?

Correspondent banking services include, but are not limited to:

- Cash management services, including deposit accounts
- Check clearing
- Foreign exchange services
- International fund transfers
- Letters of credit (confirmed/advised)
- Syndicating or agenting loans
- Investment advisers
- Overnight investment accounts (sweep accounts)
- Payable through accounts (PTAs)
- Pouch activities
- Bulk cash activities

328. What does the term "payable through account" (PTA) mean for Section 312 purposes?

A PTA, also known as a "pass through" or "pass-by" account, is an account maintained for a respondent that permits the respondent's customers to engage, either directly or through a subaccount, in banking activities (e.g., check writing, making deposits) usually in the United States. For additional guidance, please refer to the Payable Through Accounts section.

329. What is the difference between PTAs and traditional correspondent banking?

In traditional correspondent banking, customers do not have the authority to transact through the respondent's account on their own. In order to send or receive funds through the respondent's account, the customer must send instructions to the respondent so that the respondent can transact on behalf of the customer. In other words, with PTAs, customers of the respondent have direct access to the account.

330. What are the heightened money laundering and terrorist financing risks of PTAs?

PTAs do provide legitimate business benefits, but the operational aspects of the accounts make them particularly vulnerable to abuse as a mechanism to launder money as multiple individuals can have signatory authority over a single correspondent account and, therefore, can conduct transactions anonymously. Often, PTA arrangements are with financial institutions and customers in less-regulated financial markets. Unless a financial institution is able to identify adequately and understand the transactions of the ultimate users of the respondent bank's account, there is a significant potential money laundering and terrorist financing risk.

331. When should financial institutions consider terminating PTAs?

Because they present a heightened risk of money laundering and terrorist financing, financial institutions that offer PTAs must have adequate resources and controls in place to manage the risks.

Financial institutions should consider terminating PTAs in situations including, but not limited to, the following:

- Adequate information about the ultimate users of the PTAs cannot be obtained
- Weak AML regulations and controls regarding customer identification and transaction monitoring exist in the jurisdiction of the foreign bank itself
- Ongoing suspicious and unusual activities occur in the PTA
- The financial institution is unable to conclude that PTAs are not being used for illicit purposes

332. How is the term "pouch activity" defined?

Pouch activity, also known as "pouch services" or "cash letters," entails the use of a courier to transport currency, monetary instruments, loan payments and other financial documents to a financial institution.

Pouches can be sent by another financial institution or by an individual and are commonly offered in conjunction with correspondent banking services. For additional guidance, please refer to the Pouch Activity section.

333. Is the term "pouch activity" limited to the transport of financial documents from a foreign country to a financial institution in the United States?

No. Pouch activity can be offered to domestic and foreign individuals and institutions. The risk is heightened for pouches received from countries with lax or deficient AML regimes.

334. What are bulk cash activities?

Bulk cash activities entail the use of common, independent of Postal Service carriers to transport large volumes of bank notes (U.S. or foreign) from sources inside or outside the United States to a bank in the United States. For further guidance, please refer to the section Bulk Shipments of Currency.

335. What is the purpose of correspondent banking?

Correspondent banking allows institutions to conduct business and provide services to their customers without the expense of a physical presence in a jurisdiction. It also allows institutions to expand their portfolio of products and services by offering the products and services of the correspondent to the respondent's customers.

336. What is the heightened money laundering and terrorist financing risk of correspondent accounts?

Correspondent banking relationships may expose the U.S. financial system to heightened money laundering and terrorist financing risk if they are established for foreign financial institutions located in jurisdictions with nonexistent or weak AML laws and regulations. Additionally, correspondent banking involves high-volume, international transactions involving multiple parties in which no one institution may have a direct relationship with all parties involved nor have a complete view of the entire transaction.

337. What guidance and information have been issued on correspondent banking?

Among the key guidance and information issued on correspondent banking are the following:

- **Correspondent Banking – Overview (Domestic and Foreign)** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 13: Correspondent Banking** (2012) by the Financial Action Task Force (FATF)
- **Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking** (2002) by The New York Clearing House Payments Co., LLC
- **Wolfsberg AML Principles for Correspondent Banking** (2012) by the Wolfsberg Group
- **Wolfsberg Frequently Asked Questions on Correspondent Banking** (2012) by the Wolfsberg Group
- **The Wolfsberg Group and the Clearing House Association: Cover Payments: Some Practical Questions Regarding the Implementation of the New Payment Messages** (2009) by the Wolfsberg Group
- **Correspondent Account KYC Toolkit: A Guide to Common Documentation Requirements** (2009) by the International Finance Corporation (IFC), the private sector arm of the World Bank Group
- **Application of Correspondent Account Rules to the Presentation of Negotiable Instruments Received by a Covered Financial Institution for Payment** (2008) by Financial Crimes Enforcement Network (FinCEN)
- **Application of the Correspondent Account Rule to Executing Dealers Operating in Over-the-Counter Foreign Exchange and Derivatives Markets Pursuant to Prime Brokerage Arrangements** (2007) by FinCEN
- **Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries** (2006) by FinCEN
- **Application of the Regulations regarding Special Due Diligence Programs for Certain Foreign Accounts to NSCC Fund/SERV Accounts** (2006) by FinCEN
- **Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-border Wire Transfers** (2008) by the Basel Committee on Banking Supervision of the Bank of International Settlements (BIS)
- U.S. Senate Hearing on the **Role of U.S. Correspondent Banking in International Money Laundering** (2001)
- Senate Permanent Subcommittee Hearing on "**U.S. Vulnerabilities to Money Laundering and Terrorist Financing: HSBC Case History**" (2012)

For additional guidance on correspondent banking, please refer to the following sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks, Section 319 – Forfeiture of Funds in U.S. Interbank Accounts, Foreign Bank Certifications, and Section 311 – Special Measures.

Due Diligence for Correspondent Accounts

338. What types of foreign respondents are subject to the correspondent account due diligence requirements outlined in Section 312?

Section 312 applies to correspondent accounts maintained at the following:

- Foreign banks
- Foreign branch(es) of a U.S. bank
- Businesses organized under a foreign law that, if located in the United States, would be a:
    - Securities broker-dealer
    - Futures commission merchant (FCM)
    - Introducing broker (IB) in commodities
    - Mutual fund
    - Money transmitter or dealer in foreign exchange

339. What are the general correspondent account due diligence requirements outlined in Section 312?

As part of its AML program, a domestic correspondent must establish a due diligence program that includes appropriate, specific, risk-based and, where necessary, enhanced policies, procedures and controls that are reasonably designed to detect and report known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered or managed in the United States for a foreign financial institution.

At minimum, the due diligence program must:

- Determine whether the account is subject to enhanced due diligence (EDD) under Section 312
- Assess the money laundering and terrorist financing risk posed, based on a consideration of relevant risk factors
- Apply risk-based policies, procedures and controls to each such respondent reasonably designed to detect and report known or suspected money laundering or terrorist financing activity. Controls should include a periodic review of the respondent's account activity to determine consistency with information obtained about the type, purpose and anticipated activity of the account

340. Can financial institutions rely upon a third party's due diligence for their correspondent banking relationships?

In instances where the parent company has effective control, financial institutions may be able to rely on due diligence conducted on the ultimate parent company in lieu of conducting individual assessments of each foreign branch, subsidiary or affiliate. However, financial institutions must consider unique factors of each branch, subsidiary or affiliate when determining if reliance is appropriate.

341. What steps should a financial institution take if it cannot perform the appropriate due diligence?

Section 312 states that a financial institution's due diligence program should include procedures to be followed in circumstances where due diligence cannot be performed. These procedures should detail the circumstances when the financial institution should file a Suspicious Activity Report (SAR), and when it should refuse to open the account, suspend transaction activity and close the account.

342. Does Section 312 provide guidance as to what relevant risk factors should be considered when assessing the money laundering and terrorist financing risks of foreign respondents?

Yes. Section 312 provides the following factors that should be considered:

- The nature of, and markets served by, the foreign respondent's business
- The type, purpose and anticipated activity of the foreign respondent's account
- The nature and duration of the relationship with the foreign respondent (and any of its affiliates)
- The AML and supervisory regime of the jurisdiction that issued the charter or license to the foreign respondent
- The AML and supervisory regime of the jurisdiction in which any company that is an owner of the foreign respondent is incorporated or chartered (if reasonably available)
- Information known or reasonably available about the foreign respondent's AML record

343. Are there any particular challenges to monitoring correspondent clearing activity?

One of the most difficult challenges to effective monitoring of correspondent clearing activity is determining the reasonableness of transactions conducted by customers of the respondent. This requires understanding the nature of the services provided by the respondent and the customer base of the respondent and determining what additional research or information is necessary for the adequate review of activity.

344. What are cover payments and how are they a challenge to monitoring correspondent clearing activity?

Cover payments are used in correspondent banking to facilitate international transactions. A cover payment involves two separate transactions: one credit transfer message that travels a direct route from the originating bank to the ultimate beneficiary's bank, and a second credit transfer that travels through a chain of correspondent banks to settle or "cover" the first credit transfer message.

Prior to changes made to the Society for Worldwide Interbank Financial Telecommunication (SWIFT) Payments Messaging system in 2009, a challenge to monitoring correspondent clearing activity stemmed from the industry's use of SWIFT MT202 transactions as cover payments.

MT202 transactions are intended for bank-to-bank transactions; however, they were occasionally used in lieu of the MT103 messages intended for use in a commercial transaction. In part, this occurred because the MT202s were more cost-effective. Regardless of the reason, however, the substitution of a MT202 for a MT103 in a commercial transaction masked the underlying parties to a transaction, thereby frustrating monitoring attempts.

To address this lack of transparency, SWIFT developed a variant of the MT202 payment message type, MT202 COV, which allows all information contained in certain fields (e.g., originator and beneficiary information) of the MT103 to be transmitted in the MT202 COV and is to be used for cover payments in lieu of MT202s.

345. What is SWIFT's role in the international payments system?

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is the infrastructure supporting both global correspondent banking and most domestic payment systems and Real-Time Gross Settlement (RTGS) networks involving over 9,000 financial institutions in more than 200 countries and territories.

346. What guidance has been issued on correspondent banking?

The following are examples of information and key guidance that have been issued on correspondent banking:

- **Correspondent Banking – Overview (Domestic and Foreign)** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 13: Correspondent Banking** (2012) by the Financial Action Task Force (FATF)
- **Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking** (2002) by The New York Clearing House Payments Co., LLC
- **Wolfsberg AML Principles for Correspondent Banking** (2012) by the Wolfsberg Group

- **Wolfsberg Frequently Asked Questions on Correspondent Banking** (2012) by the Wolfsberg Group
- **The Wolfsberg Group and the Clearing House Association: Cover Payments: Some Practical Questions Regarding the Implementation of the New Payment Messages** (2009) by the Wolfsberg Group
- **Correspondent Account KYC Toolkit: A Guide to Common Documentation Requirements** (2009) by the International Finance Corporation (IFC), the private sector arm of the World Bank Group
- **Application of Correspondent Account Rules to the Presentation of Negotiable Instruments Received by a Covered Financial Institution for Payment** (2008) by Financial Crimes Enforcement Network (FinCEN)
- **Application of the Correspondent Account Rule to Executing Dealers Operating in Over-the-Counter Foreign Exchange and Derivatives Markets Pursuant to Prime Brokerage Arrangements** (2007) by FinCEN
- **Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries** (2006) by FinCEN
- **Application of the Regulations regarding Special Due Diligence Programs for Certain Foreign Accounts to NSCC Fund/SERV Accounts** (2006) by FinCEN
- **Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-border Wire Transfers** (2008) by the Basel Committee on Banking Supervision of the Bank of International Settlements (BIS)
- **U.S. Senate Hearing on the Role of U.S. Correspondent Banking in International Money Laundering** (2001)

For additional guidance on correspondent banking, please refer to the following sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks, Section 319 – Forfeiture of Funds in U.S. Interbank Accounts, Foreign Bank Certifications, and Section 311 – Special Measures.

Enhanced Due Diligence for Correspondent Accounts

347. Which types of accounts are subject to the enhanced correspondent account due diligence requirements outlined in Section 312?

Section 312 applies to correspondent accounts maintained for the following foreign financial institutions:

- Foreign banks operating under an offshore banking license
- Foreign banks under a license issued by a country that has been designated as being noncooperative with international AML principles or procedures by an intergovernmental group or organization of which the United States is a member and with which designation the U.S. representative to the group or organization concurs
- Under a license issued by a country designated by the U.S. Treasury Department as warranting Special Measures due to money laundering concerns (as defined in Section 311)

348. What are the heightened money laundering and terrorist financing risks of financial institutions operating under an offshore banking license?

Financial institutions operating under offshore banking licenses are prohibited from conducting business with the residents of their licensing jurisdiction or in their local currency, but have the authority to transact business “offshore” with the citizens of other countries. Because they have no negative effect upon local citizens and are often lucrative profit centers for the licensing jurisdiction, local government regulators have less incentive to engage in appropriate oversight of offshore banking institutions.

349. Do all financial institutions operating under an offshore banking license pose the same risk?

No. Offshore banks affiliated with well-established onshore parent financial institutions may not pose as high a risk as unaffiliated offshore banks; however, affiliated status is no guarantee against anti-money laundering deficiencies. Financial institutions should consider conducting their own due diligence to understand the risks of affiliated offshore banks and not automatically assume their AML program is the same or as strong as the reputable affiliate.

350. What is the difference between a Class A and a Class B offshore banking license?

Simply put, Class A licenses allow an institution to provide services to customers within and outside of the jurisdiction granting the license, while Class B licenses restrict institutions to conducting only offshore banking activities.

351. What are the enhanced due diligence (EDD) requirements for correspondent accounts outlined in Section 312?

Applicable U.S. financial institutions must, at minimum:

- Conduct enhanced scrutiny to guard against money laundering and terrorist financing and to identify and report any suspicious transactions, including:
    - Obtaining and considering information relating to the respondent's AML Compliance Program
    - Monitoring transactions to, from or through the account
    - Obtaining information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable through account (PTA), and the sources and beneficial owner of funds or other assets in the PTA
- Determine whether the respondent for which the account is established or maintained in turn maintains correspondent accounts for other foreign institutions that use the account established or maintained by the U.S. financial institution, and take reasonable steps to obtain information relevant to assess and mitigate money laundering and terrorist financing risks associated with the respondent's correspondent accounts for other foreign financial institutions, including, as appropriate, the identity of such foreign institutions
- Determine, for any respondent whose shares are not publicly traded, the identity of each owner of the foreign institution and the nature of and extent of the ownership interest

Due Diligence for Private Banking Accounts

352. What are the due diligence requirements for private banking accounts outlined in Section 312?

Requirements include the establishment of a due diligence program that includes policies, procedures and controls that are reasonably designed to detect and report known or suspected money laundering activity conducted through or involving any private banking account established, maintained, administered or managed in the United States by the financial institution.

At minimum, the due diligence program must:

- Identify the nominal (i.e., named) and beneficial owners of a private banking account
- Determine if any of the nominal and beneficial owners of the private banking account are politically exposed persons (PEPs)
- Identify the private banking account's source of funds, purpose and expected use
- Review the private banking account activity to ensure it is consistent with the information obtained about the customer's source of funds, stated purpose and expected use of the account
- Report, as appropriate, known or suspected money laundering or suspicious activity conducted to, from or through the private banking account

353. What does the term "private banking account" mean for Section 312 purposes?

A private banking account is defined as an account (or combination of accounts) maintained at a financial institution that meets the following criteria:

- Requires a minimum aggregate deposit of funds or other assets of not less than $1 million
- Is established on behalf of or for the benefit of one or more non-U.S. persons who are direct or beneficial owners of the account

- Is assigned to, or is administered or managed by, in whole or in part, an officer, employee or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account

354. What are typical products/services offered to private banking customers?

Private banking services may include, but are not limited to:

- Cash management (e.g., checking accounts, bill-paying services, overnight sweeps, overdraft privileges)
- Asset management (e.g., trust advisory, investment management, custodial and brokerage services)
- Lending services
- Financial and estate planning
- Facilitation of offshore entities (e.g., private investment companies [PICs] and trusts)

355. What are private investment companies and their heightened money laundering and terrorist financing risks?

A private investment company (PIC) generally refers to a company formed by an individual(s) to own and manage his or her assets. Often established in offshore financial centers (OFCs) for tax reasons, PICs provide confidentiality and anonymity to the beneficial owners of the funds because the management of the PIC often rests with a third party not readily associated with the beneficial owner. It is because the ownership of a PIC is not transparent that PICs may pose heightened money laundering risk.

356. What are offshore financial centers?

OFCs are jurisdictions that have a relatively large number of financial institutions engaged primarily in business with nonresidents. OFCs are generally known for their favorable tax climate and bank secrecy laws. Some examples of OFCs include Bermuda, the British Virgin Islands, the Cayman Islands, Cyprus, the Isle of Man and Panama. Additional information, including assessments of OFCs, can be found on the International Monetary Fund's (IMF) website: www.imf.org.

357. Would an account be considered a private banking account if it satisfies the definition of a private banking account with the exception that the financial institution does not require a minimum balance of $1 million?

Financial institutions have taken varying stances regarding their interpretation of the definition of a private banking account. Some financial institutions have taken the position that if the financial institution does not require a minimum balance of $1 million to qualify for additional private banking services, then the financial institution does not have private banking accounts. Others classify any account(s) with more than $1 million in assets as a private banking account. A financial institution should clearly outline its definition of a private banking account within its policies and procedures. Regardless of a financial institution's definition, a risk-based approach should be used when selecting accounts for additional due diligence.

358. What does the term "beneficial owner" mean for Section 312 purposes?

For Section 312 purposes, the term "beneficial owner" means an individual who has a level of control over, or entitlement to, the funds or assets in the account. This control or entitlement allows the individual (directly or indirectly) to control, manage or direct the account.

FinCEN, the third European Union (EU) Money Laundering Directive and the 2007 United Kingdom (U.K.) Money Laundering Regulations provide additional guidance on who qualifies as a beneficial owner. Most recently, FinCEN published the advanced notice of proposed ruling (ANPR), Customer Due Diligence Requirements for Financial institutions that proposes a more detailed definition of "beneficial owner" and could require all financial institutions to collect and verify this information on their customers. For further guidance, please refer to the Beneficial Owners section.

359. If an individual is entitled to the funds in the account, but does not have any authority to control, manage or direct the account, would the individual be considered a "beneficial owner"?

No. The ability to fund the account or the entitlement to the funds in the account alone does not cause the individual to be a beneficial owner.

360. What is the heightened money laundering and terrorist financing risk of private banking accounts?

Private banking can be vulnerable to money laundering schemes for the following reasons:

- Strict privacy and confidentiality culture of private bankers
- Powerful clientele (e.g., politically exposed persons [PEPs])
- Use of trusts, PICs and other types of nominee companies
- Increased frequency of international transactions

361. Can a financial institution rely on the due diligence conducted by well-regulated foreign intermediaries that open private banking accounts on behalf of their clients?

No. Financial institutions cannot rely on foreign intermediaries to satisfy a financial institution's Section 312 obligations.

Enhanced Due Diligence for Private Banking Accounts

362. What are the enhanced due diligence (EDD) requirements for private banking accounts outlined in Section 312?

A private banking due diligence program should include reasonable steps to detect and report transactions that may involve the proceeds of foreign corruption. This is in addition to the other requirements for private banking accounts as detailed in the Due Diligence for Private Banking Accounts section.

363. What does the term "proceeds of foreign corruption" mean for purposes of Section 312?

"Proceeds of foreign corruption" are defined as assets or properties that are acquired by, through or on behalf of a senior foreign political figure through (a) misappropriation, theft or embezzlement of public funds, (b) the unlawful conversion of property of a foreign government, or (c) acts of bribery or extortion. Properties into which any such assets have been transformed or converted also are covered under this definition.

364. What guidance has been issued on private banking?

The following are examples of key guidance that has been issued on private banking:

- **Private Banking Due Diligence Program (Non-U.S. Persons)** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Wolfsberg Anti-Money Laundering Principles for Private Banking** (2012) by the Wolfsberg Group
- **Wolfsberg FAQs on Beneficial Ownership** (2012) by the Wolfsberg Group
- **Private Banking and Money Laundering: A Case Study of Opportunities and Vulnerabilities** (2001) by the U.S. Senate (Hearing)

Senior Foreign Political Figure

365. What does the term "politically exposed person" mean for Section 312 purposes?

A "politically exposed person" (PEP) is a senior foreign political figure. Section 312 defines the term "senior foreign political figure" to include a current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned commercial enterprise; a corporation, business or other entity formed by or for the benefit of any such individual; an immediate family member of such an individual; or any individual publicly known (or actually known by the financial institution) to be a close personal or professional associate of such an individual.

"Immediate family member" means an individual's spouse, parents, siblings, children and spouse's parents or siblings. "Senior official" or "senior executive" means an individual with substantial authority over policy, operations or the use of government-owned resources.

366. Is the definition of a PEP limited to individuals?

No. In the broadest sense, PEPs can be nonindividuals. For example, government entities or corporations that have the authority to award government contracts also could be considered PEPs.

367. Is the definition of a PEP limited to "foreign" senior officials?

Many financial institutions extend the definition of PEP to include domestic senior political figures, as well, though this is not required by Section 312.

368. Is the definition of a PEP limited to private banking customers?

No. Status as a PEP is not dependent on the types of products and services utilized by the PEP.

369. Do embassy and foreign consulate accounts fall within the definition of a PEP?

Certain individuals within an embassy or consulate may fall within the definition of a PEP (e.g., the ambassador or a high-ranking military officer). The average employee in an embassy or consulate is unlikely to reach PEP status. For further guidance on embassy accounts, please refer to the Foreign Embassy and Consulates section.

370. What is the heightened money laundering risk of PEPs?

Access to government funds may increase the potential for corruption and bribery.

371. Do all PEPs pose the same degree of risk?

No. Not all PEPs pose the same degree of risk. A financial institution may consider, for example, the country of domicile, level of office, negative history/media on the PEP and the degree of affiliation to the PEP (in the case of family members and close associates) when assessing the degree of risk.

372. What guidance has been issued with respect to PEPs and embassy banking?

The Financial Action Task Force (FATF), an intergovernmental policy-making body created to establish and promote international legislative and regulatory standards in the areas of money laundering and terrorist financing, defines PEPs as individuals who are or have been entrusted with prominent public functions in a foreign country (e.g., heads of state, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials). FATF also states that business relationships with family members or close associates of PEPs have similar reputational risks to PEPs themselves and, therefore, should be included in the definition of a PEP, as well.

FATF also advises that the definition of a PEP was not meant to include junior- or middle-ranking individuals in the categories mentioned above. FATF also suggests that domestic individuals who hold prominent public positions also should be subject to enhanced due diligence (EDD).

Additional guidance includes the following:

- **Politically Exposed Persons – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 12: Politically Exposed Persons** (2012) by the Financial Action Task Force (FATF)
- **Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption** (2008) by the FinCEN
- **Wolfsberg FAQs on Politically Exposed Persons** (2008) by the Wolfsberg Group
- **Guidance on Enhanced Scrutiny for Transactions That May Involve the Proceeds of Foreign Official Corruption** (2001) by the U.S. Treasury, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision, and the Department of State
- **Stolen Asset Recovery: Politically Exposed Persons, A Policy Paper on Strengthening Preventive Measures** (2010) by the World Bank
- **Stolen Asset Recovery: Guide on Non-Conviction Based (NCB) Asset Forfeiture** (2009) by the World Bank

For further guidance on PEPs, please refer to the sections Politically Exposed Persons and Foreign Embassy and Consulates.

Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks

373. Which financial institutions are required to comply with Section 313, Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks?

The following financial institutions must comply with Section 313:

- An insured bank
- A commercial bank or trust company
- A private banker
- An agency or branch of a foreign bank in the United States
- A credit union
- A savings association
- A corporation acting under section 25A of the Federal Reserve Act (12 U.S.C. 611 et seq.)
- A registered (or required to be registered) broker or dealer in securities with limited exceptions

374. What does the term "foreign shell bank" mean for Section 313 purposes?

The term "foreign shell bank" is a foreign bank without a physical presence in any country.

375. What does the term "physical presence" mean for Section 313 purposes?

Physical presence means a place of business that:

- Is maintained by a foreign bank
- Is located at a fixed address (other than solely an electronic address or a P.O. box) in a country in which the foreign bank is authorized to conduct banking activities, at which location the foreign bank:
    - Employs one or more individuals on a full-time basis
    - Maintains operating records related to its banking activities
    - Is subject to inspection by the banking authority that licensed the foreign bank to conduct banking activities

376. What are the reasons a financial institution would create a foreign shell bank?

There are a variety of reasons a financial institution would create a foreign shell bank, including their ease of formation and the ability to operate with anonymity.

377. What are the requirements imposed on financial institutions outlined in Section 313?

Financial institutions are prohibited from establishing, maintaining, administering or managing a correspondent account in the United States for, or on behalf of, a foreign shell bank.

378. Are there exceptions to the requirements outlined in Section 313?

Yes. A financial institution can maintain a correspondent account for a foreign shell bank that is a regulated affiliate of a bank with a physical presence.

379. What steps should a financial institution take to ensure that one or more of its correspondent relationships do not involve a foreign shell bank?

Beyond complying with Section 313, the financial institution should conduct due diligence on its correspondent relationships to (a) gain a better understanding of the respondent, and (b) develop an understanding of the respondent's customer base. In addition, the correspondent should perform transaction monitoring to identify, among other things, potential nested relationships.

380. What does the term "nested relationship" mean for Section 313 purposes?

Foreign banks may use correspondent accounts of other foreign banks rather than opening their own correspondent account with a U.S. financial institution to gain access to the U.S. financial system. These are nested relationships. A nested bank gains the advantages of a correspondent status often without being subject to the correspondent's customer acceptance standards and perhaps without the correspondent's awareness.

381. What should a correspondent do when a former respondent is nesting through a current respondent relationship?

When a correspondent closes an account due to the identification of suspicious activity, the respondent usually is added to a watch list in order to ensure the respondent does not open another account a few months later. Monitoring against this list would enable a correspondent to find nested relationships that were closed due to suspicious activity. Where a correspondent has terminated a relationship with a respondent and subsequently finds nesting, it may inform its respondent that it is not comfortable doing business with the nested respondent (if it can do so without tipping the respondent off to the fact it has filed a SAR) or it may decide to file a SAR(s) on the nested activity if it deems it suspicious.

382. What should a correspondent do when a foreign shell bank is nesting through a current respondent relationship?

In addition to the investigation and SAR filing procedures detailed above, the correspondent should close all accounts with the respondent within a commercially reasonable amount of time. Reopening of such accounts can occur only under special circumstances.

Section 314 – Cooperative Efforts to Deter Money Laundering

Section 314(a) – Cooperation among Financial Institutions, Regulatory Authorities and Law Enforcement Authorities

383. How does Section 314(a), Cooperation among Financial Institutions, Regulatory Authorities, and Law Enforcement Authorities, facilitate the sharing of information?

Section 314(a) of the USA PATRIOT Act establishes a mechanism for law enforcement agencies to communicate the names of persons engaged in or suspected to be engaged in terrorism and money laundering to financial institutions in return for securing the ability to locate accounts and transactions involving those suspects promptly. Currently, FinCEN can reach more than 44,000 points of contact in over 22,000 financial institutions.

384. Are financial institutions obligated to share information under Section 314(a)?

Any financial institutions required to establish an AML program under Section 352 may be obligated to comply with 314(a) information requests. Unlike Section 314(b), participation is not voluntary.

385. What are the protocols for issuing 314(a) requests prior to distribution to financial institutions?

Every 314(a) request is certified and vetted through the appropriate channels within each law enforcement agency to ensure that the information requested from financial institutions is related to a valid and significant money laundering/terrorist investigation. FinCEN also requires documentation showing the size or impact of the case, the

seriousness of the underlying criminal activity, the importance of the case to major agencies, and the exhaustion of traditional or alternative means of investigation prior to the submittal of requests to financial institutions by FinCEN.

386. What law enforcement agencies are able to participate in issuing 314(a) requests?

Since the inception of 314(a) information sharing, all federal domestic law enforcement agencies have been permitted to participate in providing requests to FinCEN to be submitted to the participating financial institutions. On February 10, 2010, FinCEN issued a final rule expanding participation privileges to foreign law enforcement agencies as well as domestic state and local agencies. Further, the final rule grants FinCEN the ability to initiate 314(a) inquiries on its own behalf, and on behalf of other areas of the U.S. Department of Treasury.

387. How often do financial institutions receive information requests under Section 314(a)?

Batched information requests are sent by FinCEN every two weeks. However, an ad hoc information request may be sent to a financial institution in an urgent situation.

388. How are 314(a) requests distributed to financial institutions?

In March 2005, FinCEN began distributing 314(a) subject lists through a secure website. Every two weeks, or more often if an emergency request is transmitted, the financial institution's designated point of contact can download the current and one preceding 314(a) subject list in various formats for searching. Financial institutions were previously able to receive the 314(a) subject lists via facsimile transmission; however, this option is no longer available. Institutions may no longer elect to receive 314(a) transmissions via fax, as FinCEN now requires that all participants obtain 314(a) subject lists through the secure website. FinCEN may still elect to send facsimile transmissions of the list; however, this may not be relied upon by financial institutions.

389. What information is included in 314(a) requests?

The requests contain subject and business names, addresses and as much identifying data as possible to assist the financial institutions with searching their records.

390. How does a financial institution change its point-of-contact information on FinCEN's distribution list for receiving 314(a) information requests?

A financial institution should contact its primary federal regulator or self-regulatory organization (SRO) to change its point of contact. Financial institutions also should provide information for Section 314(a) points of contact on the financial institutions' quarterly call or Thrift Financial Report (for financial institutions subject to supervision by one of the five federal banking regulators). Contact information can be found at www.fincen.gov.

391. Within what time frame are financial institutions required to complete their 314(a) searches?

Financial institutions are required to complete their searches and respond to FinCEN with any matches within two weeks of receiving the request.

392. What records are financial institutions required to search under 314(a)?

Financial institutions are required to search the following records if maintained in a searchable electronic format:

- Deposit account records
- Funds transfer records
- Records for the sale of monetary instruments
- Loan records
- Trust department account records
- Records of accounts to purchase, sell, lend, hold or maintain custody of securities
- Commodity futures, options or other derivatives
- Safe deposit box records

393. If a financial institution scans and saves checks onto its systems as images, should these also be searched?

No. Electronic media that is searchable (e.g., databases, delimited text files) should be included in 314(a) searches, but images and other electronic media that do not support search technology are excluded from the scope of 314(a) searches.

394. Should parties other than account holders be included in the search?

Yes. Parties other than account holders should be included in the search (e.g., authorized signers, guarantors).

395. Is a financial institution obligated to report a possible match with a noncustomer of the institution (e.g., beneficiary of a funds transfer originated by its own customer)?

Yes, any match should be reported. 314(a) searches apply not only to accounts, but also to transactions conducted at or through the financial institution; therefore, a transaction counterparty, who may be a noncustomer, could result in a possible match.

396. Are there records that financial institutions are not required to search for possible 314(a) matches?

Financial institutions are not required to search the following records unless the information is readily searchable (e.g., databases, delimited text files):

- Checks processed through an account to determine whether a named subject was a payee of a check
- Monetary instruments (e.g., cashier's checks, money orders, traveler's checks, drafts) issued by the institution to determine whether a named subject was a payee of such an instrument
- Signature cards to determine whether a named subject is a signatory to an account (unless such a search is the only method to confirm whether a named subject maintains an account, as described above)

397. For what periods are financial institutions required to search their records under Section 314(a)?

Unless otherwise noted in the 314(a) information request, financial institutions must search their records for the preceding 12 months for account parties (e.g., account holders, signers), and for the preceding six months for transactions.

398. Should financial institutions receiving information requests from FinCEN under Section 314(a) search their records on a continuing basis?

Unless otherwise noted on the information request, 314(a) requests require a one-time search only. Financial institutions do not need to continue to search their records in the future, unless specified on the information request.

399. What action should a financial institution take if it does not identify a match to a 314(a) request?

If the search does not yield any results, a financial institution should not reply to the 314(a) request. It should document the completion of the search and the results, and protect the confidentiality of the 314(a) list.

400. What action should a financial institution take if it identifies a potential match to a 314(a) request?

In the event of a possible match, a financial institution should conduct an investigation to the extent necessary to determine whether the information represents a true match, or is a false positive. In the event of a true match, the designated point of contact should notify FinCEN that it has a match via the website, as well as the individual's contact information to enable the requesting law enforcement agency to contact the institution to obtain further information regarding the match. It is to provide FinCEN with the name and account number of each individual, entity or organization for which a match was found, as well as any TIN, DOB or other similar identifying information provided by such person at the account opening or when the transaction(s) was conducted.

401. Is 314(a) information sharing an acceptable substitute for complying with a subpoena or National Security Letter?

No. Section 314(a) provides lead information only. It is not a substitute for a subpoena or other legal process. To obtain documents from a financial institution that has a reported match, a law enforcement agency must meet the legal standards that apply to the particular investigative tool it chose to use to obtain the documents.

402. What documentation should a financial institution maintain relating to its 314(a) searches?

Some financial institutions choose to maintain copies of the cover page of the request, with sign-off from appropriate personnel indicating the date the search was completed, and the results (i.e., positive, negative). For positive matches, many financial institutions also maintain the correspondence with FinCEN. Other financial institutions maintain the entire 314(a) request, including subjects searched. Regardless of the documentation maintained, a financial institution must maintain procedures to protect the security and confidentiality of 314(a) requests.

403. Should financial institutions automatically file a SAR on a positive 314(a) match?

No. FinCEN strongly discourages financial institutions from using the results of a 314(a) search as the sole factor in reaching a decision to do so unless the request specifically states otherwise. A 314(a) match may serve to initiate an investigation; however, the decision to file a Suspicious Activity Report (SAR) should be based on the institution's investigation of the activity involved.

404. Has FinCEN issued statistics relating to the usefulness of 314(a) requests?

Yes. FinCEN issued a 314(a) Fact Sheet in October 31, 2012 that outlined a number of statistics relating to 314(a) requests. To date, FinCEN has processed 1,784 requests for information, including:

- 396 requests (22 percent) pertaining to terrorism-related cases
- 1,388 cases (78 percent) related to money laundering
- 18,926 subjects of interest, with approximately 119,000 positive confirmations with accounts and/or transactions held at, or conducted through, financial institutions

The law enforcement requesters who provided FinCEN with feedback indicated that because of the 314(a) system, 47 percent of the confirmations contributed to arrests and 54 percent of the confirmations contributed to indictments.

405. Beyond Section 314(a), what other mechanisms are used by law enforcement to obtain information from financial institutions?

Other mechanisms used by law enforcement to obtain information from financial institutions include, but are not limited to, the following:

- **Subpoenas** – Law enforcement has the ability to request certain specific information by the use of subpoenas, which must comply with applicable laws, such as the Right to Financial Privacy Act.
- **National Security Letters (NSLs)** – Written investigative demands may be issued by the local FBI field office and other federal government authorities in counterintelligence and counterterrorism investigations to obtain telephone and electronic communications records from telephone companies and Internet service providers, information from credit bureaus and financial records from financial institutions. NSLs are highly confidential documents; as such, examiners will not review or sample specific NSLs. For further guidance on NSLs, please refer to Section 505 – Miscellaneous National Security Authorities.

Section 314(b) – Cooperation among Financial Institutions

406. How does Section 314(B), Cooperation among Financial Institutions, facilitate the sharing of information?

Section 314(b) enables financial institutions, or an association of financial institutions, to share information concerning suspected money laundering and terrorist activity with other financial institutions under a Safe Harbor from liability. To participate in information sharing with other financial institutions and financial institution associations, each participant must notify FinCEN of its intent to share information. Notification can be provided by completing a Financial Institution

Notification Form that can be found on FinCEN's website. If the notification form is not provided to FinCEN, the Safe Harbor protection is not available.

407. Which financial institutions may participate in Section 314(b) sharing?

The universe of financial institutions that may share information under 314(b) includes all financial institutions required to establish and maintain AML programs, unless FinCEN specifically determines that a particular category of financial institution should not be eligible to share information under this provision.

408. How is an "association of financial institutions" defined for the purpose of Section 314(b) sharing?

An "association of financial institutions" is defined as a group whose membership is comprised entirely of financial institutions as defined by the broad list of financial institutions listed in the USA PATRIOT Act.

409. Are financial institutions obligated to share information under Section 314(b)?

No. Unlike Section 314(a), financial institutions are not obligated to share information under Section 314(b).

410. For what period does the notification form submitted to FinCEN allow a financial institution to share information?

Once the notification is filed, the filing institution may share information for one year, beginning on the execution date of the notification form. A financial institution does not need to wait for confirmation from FinCEN to begin sharing information.

411. Do financial institutions have any obligations beyond submitting notification forms in order to share information?

Yes. Financial institutions sharing information under Section 314(b) must have procedures in place to protect the security and confidentiality of shared information and to ensure the information is used only for authorized purposes.

Financial institutions also should take reasonable steps to ensure that any financial institution with which it shares information has submitted the requisite form as well. This can be done by confirming that the other financial institution appears on a list that FinCEN provides to financial institutions that have filed a notice, or by confirming directly with the other financial institution that the requisite notice has been filed.

412. Does the notification form need to be renewed?

To continue to share information after the expiration of the one-year period, a financial institution must submit a new notification form.

413. What are the consequences of failing to submit this notification form but continuing to share information?

A financial institution that fails to notify FinCEN of its intent to share information with other institutions will not be protected under the Safe Harbor provision.

414. Can SARs be shared as part of Section 314(b) sharing?

No. Section 314(b) sharing does not allow financial institutions to disclose the filing of SARs. However, the underlying transactional and customer information may be shared.

415. Are there any restrictions on what information is permitted to be shared under 314(b)?

Yes. To benefit from the protection afforded by the Safe Harbor provision associated with 314(b), financial institutions must adhere to guidelines established by FinCEN that cover the purpose of information permitted to be shared and the content:

- The purpose for sharing under the 314(b) rule is to identify and report activities that the financial institutions "suspects may involve possible terrorist activity or money laundering"
- "Permissible information" is limited to that which the financial institution(s) (both parties) feel is relevant to an investigation of only money laundering or terrorist financing activities

As of June 26, 2009, FinCEN extended the breadth of permissible information covered under the Safe Harbor provision to include information related to certain specified unlawful activities (SUA) including, but not limited to, the following:

- Manufacturing, import, sale or distribution of a controlled substance
- Murder, kidnapping, robbery, extortion, destruction of property by means of explosive or fire, or a crime of violence
- Fraud, or any scheme or attempt to defraud, by or against a foreign bank
- Bribery of a public official, or the misappropriation, theft, or embezzlement of public funds by or for the benefit of a public official
- Smuggling or export control violations involving specified items outlined in the United States Munitions List and the Export Administration Regulations
- Trafficking in persons, selling or buying of children, sexual exploitation of children, or transporting, recruiting or harboring a person, including a child, for commercial sex acts

A comprehensive listing of unlawful activities covered under the 314(b) Safe Harbor provision is documented in 18 U.S.C. Section 1956 and 1957. Financial institutions should consult with counsel on how best to handle the sharing of information under the 314(b) provision.

416. Does the sharing of information as permitted in Section 314(b) obviate the need for a financial institution to file a SAR or notify law enforcement?

No. Section 314(b) sharing does not obviate the need to file a SAR or notify law enforcement, if warranted.

Section 319 - Forfeiture of Funds in U.S. Interbank Accounts

Section 319(a) Requirements – Forfeiture from U.S. Interbank Accounts

417. What are the implications of Section 319(a), Forfeiture from U.S. Interbank Accounts?

Section 319(a) addresses the circumstances in which funds can be seized from a U.S. interbank account. If a deposit with a financial institution outside of the United States is subject to forfeiture, and that foreign institution, in turn, deposits funds in the United States with a bank, broker-dealer, or branch or agency of a foreign bank, those funds are deemed to have been deposited in a U.S. interbank account and thus are subject to seizure under this rule. The funds do not have to be traceable to the funds originally deposited in the foreign financial institution to be subject to seizure.

418. Who has the authority to seize funds under Section 319(a)?

The U.S. Department of Justice (DOJ) has authority to seize funds under Section 319(a). Although the U.S. DOJ has used its authority to seize foreign bank funds in a number of interbank accounts at financial institutions in the United States, the seizure of funds in an interbank account is intended to be used as a last resort by law enforcement agencies.

419. What does the term “interbank account” mean for Section 319 purposes?

An interbank account is an account owned by a financial institution that is held with another financial institution for the primary purpose of facilitating customer transactions.

420. What can a financial institution do to mitigate the risk of seizure of funds in its interbank accounts?

Financial institutions should ensure they complete thorough due diligence procedures on their interbank accounts and understand the other financial institution’s customer base. However, funds subject to seizure do not need to be traceable to the original funds deposited at the foreign financial institution. Thus, although performing thorough due diligence reduces the risk of seizure, such risk cannot be eliminated altogether.

Section 319(b) Requirements – Bank Records

Domestic Financial Institution Records ("120-Hour Rule")

421. What authority does a U.S. regulatory agency have to request information about a domestic financial institution's accounts, transactions or customers?

Financial institutions must reply to an information request regarding one or more of its accounts from a U.S. regulatory agency relating to AML compliance within 120 hours of such a request.

422. If a financial institution receives a request for information covered under the 120-Hour Rule at 5 p.m. on Friday, when must the financial institution respond?

The financial institution must reply by 5 p.m. the following Wednesday, within 120 hours of the request. Weekends and holidays are included in the time frame for submissions.

Foreign Bank Records

423. Who has authority to request information from a foreign financial institution?

The U.S. Secretary of the Treasury or the Attorney General is authorized to subpoena records of a foreign bank relating to a U.S. correspondent account.

424. What will happen if a foreign bank does not comply with the information request?

If a foreign bank does not comply with or contest any such summons or subpoena within 10 calendar days of notification, U.S. depository institutions or broker-dealers that hold an account with the foreign bank are required to sever immediately their correspondent arrangements with the foreign bank.

425. Are financial institutions obligated to provide U.S. regulatory agencies and/or law enforcement agencies with records maintained outside of the United States?

If a transaction is conducted by or through a financial institution in the United States, records relating to that transaction can be requested by regulatory agencies and/or law enforcement agencies. The financial institution is obligated to provide those records.

Foreign Bank Certifications

426. What recordkeeping requirements does Section 319(b) impose on financial institutions?

A foreign respondent that maintains a correspondent account with any U.S. bank or U.S. broker-dealer in securities must certify the following in writing:

- Physical presence/regulated affiliated status
- Prohibition of indirect use of correspondent accounts by foreign shell banks
- Ownership status (for nonpublic institutions)

This "foreign bank certification" also must include the name and address of a person who resides in the United States and is authorized to accept service of legal process for records regarding the correspondent account.

Domestic correspondents are required to obtain a foreign bank certification from each foreign respondent.

427. Are there any exceptions from foreign bank certification requirements?

Foreign bank certifications are not required for nonbank financial institutions (including foreign broker-dealers), U.S. banks operating in the United States, or U.S. branches or subsidiaries of foreign banks.

428. Do certifications have to be obtained from each branch, agency and subsidiary of a foreign respondent?

Single certifications covering multiple branches and offices outside of the United States are permitted provided that the certification includes the names, addresses and regulating body(ies) of all branches or offices to be covered under the single certification (e.g., all the branches and offices outside of the United States that maintain a correspondent account with the U.S. depository institution or securities broker-dealer).

429. Has FinCEN provided an example of a foreign bank certification?

Yes. A template foreign bank certification form issued by the Treasury Department is available on FinCEN's website at www.fincen.gov.

430. What does the term "owner" mean?

The term "owner" is any person who directly or indirectly owns, controls or has the power to vote 10 percent or more. Members of the same family shall be considered to be one person.

431. Is ownership information required for all foreign respondents?

No. Ownership information is not required for foreign respondents that are publicly traded on an exchange or organized in the over-the-counter market that is regulated by a foreign securities authority as defined by the Securities Exchange Act of 1934 or that have filed an Annual Report of Foreign Banking Organizations form with the Federal Reserve.

432. If a foreign respondent posts its foreign bank certification form on the Internet, has it satisfied its 319(b) requirements?

Yes. Many financial institutions post foreign bank certifications on their websites to streamline the foreign bank certification process.

Additionally, the Wolfsberg Group, in partnership with a third-party vendor, has developed a subscription-based international due diligence repository that allows financial institutions to submit foreign bank certifications and other information about their institutions and their AML programs to a central repository. Additional information about this repository is available at www.wolfsberg-principles.com.

433. How often must a foreign respondent update its foreign bank certification?

Foreign bank certifications are required to be renewed every three years.

434. What is required of a foreign respondent if facts and circumstances (e.g., change in ownership) have changed since the last certification?

A foreign respondent must notify each domestic correspondent relationship, within 30 days, of changes to its:

- Physical presence/regulated affiliated status
- Indirect use of correspondent accounts by foreign shell banks
- Ownership status (for nonpublic institutions)

435. If a foreign respondent makes corrections/amendments to its original foreign bank certification, should the recertification date be three years from the original certification date or from the execution of an amended/corrected certification date?

The recertification date should be three years from the execution of an amended/corrected certification date.

436. What steps should a domestic correspondent take if the foreign respondent does not provide the requested foreign bank certification?

If certification or recertification has not been obtained from the foreign respondent within 90 days of a request, the domestic correspondent is required to close all correspondent accounts with the foreign respondent within a commercially reasonable time. At that time, the foreign respondent is prohibited from establishing new accounts or conducting any transactions with the domestic correspondent other than those necessary to close the account.

Failure to terminate a correspondent relationship can result in civil penalties of up to $10,000 per day until the relationship is terminated.

437. Can a domestic correspondent re-establish the correspondent account if the account was initially closed because the foreign respondent failed to provide a foreign bank certification?

Yes. Domestic correspondents may re-establish the account, or even open a new correspondent account, for the foreign respondent if the foreign respondent provides the required information.

438. What is the time frame for terminating a relationship with a foreign respondent when requested by regulators and/or governmental agencies?

A financial institution must terminate the relationship within 10 business days of the request.

439. What steps should a domestic correspondent take after receiving a foreign bank certification?

Domestic correspondents should have procedures in place to ensure the foreign bank certifications obtained are reviewed for reasonableness, completeness and consistency. This responsibility may be assigned to the correspondent bank group or to AML compliance personnel.

440. Does compliance with foreign bank certification requirements suggest the good standing of a financial institution's AML program?

No. Obtaining the certification will help domestic correspondents ensure they are complying with requirements concerning correspondent accounts with foreign respondents and can provide Safe Harbor for purposes of complying with such requirements. However, due diligence still must be conducted to understand the AML laws in the country of domicile and incorporation of the foreign respondent, as well as the foreign respondent's AML program.

441. Does the receipt of the foreign bank certification meet the due diligence requirements outlined in Section 312?

No. The foreign bank certification requirements outlined in Section 319(b) are, though related, distinct from the requirements outlined in Section 312.

442. How long should a domestic correspondent retain original foreign bank certifications?

The foreign bank certifications must be retained for a minimum of five years after the date that the domestic correspondent no longer maintains any correspondent accounts for the foreign respondent.

443. What is the time frame in which the domestic correspondents must respond to formal law enforcement requests regarding foreign bank certifications?

The domestic correspondent must provide a copy of the foreign bank certification within seven days upon written request from a federal law enforcement officer.

Section 325 – Concentration Accounts at Financial Institutions

444. How is the term "concentration account" defined for purposes of Section 325?

The USA PATRIOT Act introduces the possibility of future regulation relating to concentration accounts; however, it does not define this term. Within the industry, a concentration account is an account that a financial institution uses to aggregate funds from different customers' accounts. Concentration accounts are also known as collection, intraday, omnibus, settlement, special-use or sweep accounts.

445. What are financial institutions required to do with respect to concentration accounts?

As previously noted, regulations relating to concentration accounts have not been issued by the U.S. Treasury Department. However, financial institutions are advised to recognize and take appropriate actions to control the risks of these accounts.

Section 325 mandates that if regulations are issued, they should:

- Prohibit financial institutions from allowing customers to direct transactions through a concentration account.
- Prohibit financial institutions and their employees from informing customers of the existence of the institution's concentration accounts.
- Require financial institutions to establish written procedures governing documentation of transactions involving concentration accounts.
- In the absence of finalized regulations related to concentration accounts, financial institutions should:
    - Ensure they understand the reasons and the extent to which they use concentration accounts.
    - Establish controls over the opening, maintenance and reconcilement of concentration accounts.
    - Subject concentration accounts to AML monitoring.

446. What is the heightened money laundering risk of concentration accounts?

Concentration accounts involve the commingling of different customers' funds and also can involve the commingling of customer funds with a financial institution's funds in a way that conceals the identity of underlying parties to a transaction.

Section 326 – Verification of Identification

Overview

447. What are the requirements of Section 326 – Verification of Identification?

Section 326 requires each financial institution to maintain and develop a written Customer Identification Program (CIP). Specifically, financial institutions are required to:

- Collect the following information from new customers:
    - Name
    - Date of birth (DOB) for individuals
    - Address
    - Identification number
- Verify the identity of any person seeking to open an account
- Maintain records of the information used to verify a person's identity
- Consult lists of known or suspected terrorists or terrorist organizations to determine whether a person seeking to open an account appears on any such list

448. When must the financial institution obtain and verify the information?

Depository institutions must obtain the information prior to opening the account. Some exceptions may apply to obtaining the taxpayer identification number (TIN). Financial institutions must apply a risk-based approach in verifying the information within a reasonable time of account opening. For additional guidance on verification, please refer to the Verification section. For additional guidance on Customer Identification Programs (CIPs) for other types of financial institutions, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

449. Which financial institutions must comply with Section 326 – Verification of Identification?

The following financial institutions must comply with Section 326:

- Banks (including U.S. branches and agencies of foreign banks)
- Savings associations
- Credit unions
- Securities broker-dealers
- Mutual funds
- Futures commission merchants (FCMs) and introducing brokers (IBs) in commodities

450. Is Section 326 applicable to a financial institution's foreign subsidiaries?

No. Section 326 does not apply to any part of the financial institution located outside of the United States. Nevertheless, financial institutions should implement an effective AML program (including Section 326 requirements) throughout their operations, including in their foreign offices, except to the extent that requirements of the rule would conflict with local law.

Customer Defined

451. What does the term "customer" mean for purposes of Section 326?

A "customer" is any person who opens a new account or enters into another formal relationship after October 1, 2003. "Person" in this context includes individuals, corporations, partnerships, trusts or estates, joint stock companies, joint ventures or other incorporated organizations or groups.

452. Are there exemptions from the definition of "customer"?

The following are exempt from the definition of customer:

- A financial institution regulated by a federal functional regulator or a bank regulated by a state bank regulator
- A department or agency of the United States, a state or political subdivision of a state
- An entity that exercises governmental authority on behalf of the United States, a state or political subdivision of a state
- An entity (other than a bank) whose common stock is traded on the New York Stock Exchange (NYSE) or the American Stock Exchange (Amex/ASE) or whose common stock has been designated as a National Association of Securities Dealers Automated Quotations (NASDAQ) National Market Security listed on the NASDAQ Stock Market (except stock listed under NASDAQ Small-Cap Issues)
- A person who has an account with the financial institution that existed before October 1, 2003, if the financial institution has a reasonable belief that it knows the true identity of the person

453. Does exemption indicate that a financial institution need not conduct any due diligence on a customer?

No. A financial institution's KYC procedures should, on a risk-assessed basis, address all customers, even those exempt from a financial institution's CIP.

454. Is a person who has an existing relationship with an affiliate considered exempt from the definition of a "customer"?

No. The relationship must have existed with the financial institution itself, not an affiliate, to be excluded from the definition of "customer."

455. Is a person with a previous relationship with the financial institution considered exempt from the definition of a "customer"?

Only customers with existing relationships are exempt. For example, a customer who had a loan with a financial institution, repaid it, and subsequently obtained a new loan would be a new customer.

456. Is a person who becomes co-owner of an existing deposit account or new borrower who is substituted for an existing borrower through an assumption of a loan considered a "customer"?

Yes. What qualifies a person as a "customer" is the new establishment of a formal relationship between that particular customer and the financial institution, even though the account itself previously existed.

457. Do the requirements apply to loans that are renewed or certificates of deposit that are rolled over for customers with accounts existing before October 1, 2003?

Each time a loan is renewed or a certificate of deposit is rolled over, the financial institution establishes new formal banking relationships. Because the CIP rule excludes persons with existing relationships from the definition of "customer," assuming that the financial institution has a reasonable belief that it knows the true identity of the person, the institution need not perform its CIP when a loan is renewed or certificate of deposit is rolled over.

458. Who is the "customer" with respect to a commercial entity?

Financial institutions are required to verify the identity of the commercial entity, not the signers on the commercial accounts. However, based on the financial institution's risk assessment of new accounts opened by customers that are not individuals, the institution may need to conduct due diligence on the individuals with authority or control over such an account, including signatories, in order to verify the identity of the account holder.

459. Who is the "customer" for purposes of trust accounts?

The "customer" is the trust, not the beneficiary(ies) of the trust, whether or not the financial institution is the trustee for the trust. Similar to commercial accounts, based on the financial institution's risk assessment of new accounts opened by customers that are not individuals, the institution may want to conduct due diligence on the individuals with authority or control over such an account, including signatories, settlors, grantors, trustees or other persons with the authority to direct the trustee, in order to establish the true identity of the account holder.

460. Who is the "customer" when an account is opened by an individual who has power of attorney for the owner of an account?

When an account is opened by an individual who has power of attorney for a competent person, the "customer" is the owner of the account. In the situation where the owner of the account lacks legal capacity, the individual with power of attorney is the "customer." Similarly, if parents open accounts on behalf of their minor children, the parents are the "customers" of the financial institution, and not the children.

461. Who is the "customer" for purposes of escrow accounts?

If a financial institution establishes an account in the name of a third party, such as a real estate agent or an attorney who is acting as an escrow agent, then the financial institution's customer will be the escrow agent. If the financial institution is the escrow agent, then the person who establishes the account is the customer.

462. Who is the "customer" when there are joint account holders?

All joint account holders are deemed to be customers. This includes persons opening accounts for minors and unincorporated entities. It does not include beneficiaries, authorized users, authorized signers on business accounts or other financial institutions.

463. Does FinCEN's advance notice of rulemaking "Customer Due Diligence Requirements for Financial Institutions" amend Section 326 requirements?

FinCEN's ANPR "Customer Due Diligence Requirements for Financial Institutions" does not amend what financial institutions must collect pursuant to Section 326, but it does expand the parties for which they would be expected to collect information. Currently, covered financial institutions are required to obtain beneficial ownership in the following situations as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

The ANPR could categorically require all financial institutions subject to AML Program requirements to identify, and in some instances, verify the identity of beneficial ownership of all of its account holders. For further guidance, please refer to the Beneficial Owners section.

Account Defined

464. What does the term "account" mean for purposes of Section 326?

An "account" is a formal relationship in which financial transactions or services are provided. Examples of products and services where a formal relationship would normally exist include deposit accounts and extensions of credit; a safe deposit box or other safekeeping services; or cash management, custodian or trust services.

465. Are there exemptions from the definition of "account"?

An "account" does not include:

- Products or services for which a formal banking relationship is not established with a person (e.g., check cashing, wire transfers, sales of money orders)
- An account that the bank acquires (as a result of acquisitions, mergers, purchase of assets)
- Accounts opened for the purpose of participating in an employee benefit plan established by an employer under the Employment Retirement Income Security Act of 1974 (ERISA). In such cases, the plan administrator and not the plan participant has control over the account, thus personal identification from each participant is not required

Such circumstances would not require the institution to implement its CIP. However, this does not exempt an institution from recordkeeping and reporting requirements. The institution still must obtain the minimum information required for reporting in regards to CTRs, SARs and recordkeeping requirements (e.g., Purchase and Sale of Monetary Instruments, Funds Transfer Recordkeeping Rule, the Travel Rule).

Verification

466. Are financial institutions required to confirm every element of customer identification information used to establish the identity of their customers?

Financial institutions need not confirm every element of customer identifying information; rather, they must verify enough information to form a reasonable belief that they know the true identity of their customers. The CIP must include procedures for verifying the identity of customers and whether documentary methods, nondocumentary methods or a combination thereof will be used and must require additional verification for customers that are nonindividuals, based on the financial institution's risk assessment of the customer (e.g., verifying the identity of account signatories). It must also contain procedures for responding to circumstances in which the financial institution cannot form a reasonable belief that it knows the true identity of a customer.

467. What does the term "reasonable belief" mean for Section 326 purposes?

The regulation does not provide any guidance as to what constitutes a "reasonable belief."

Some financial institutions have created a list of information above and beyond the minimum requirements (e.g., salary/revenue, occupation/industry) that, if received, would provide a basis for a financial institution to decide it has reasonable belief that it knows the customer. Other financial institutions require the account officer to certify he or she

has reasonable belief that he or she knows the identity of the customer. Regardless of the financial institution's definition, the financial institution should clearly define the term within its CIP.

468. What are the obligations or requirements for financial institutions to update customer identification information for existing customers, i.e., customers that established their relationship with the financial institution prior to October 1, 2003?

Existing customers are exempt from the verification requirements on the condition that the financial institution has a reasonable belief that it knows the true identity of the customer. To a large extent, the acceptability of exempting existing customers from CIP requirements will depend on the strength of the financial institution's customer identification procedures prior to implementation of its CIP. Financial institutions that had strong customer identification procedures will have a better case for exempting customers.

469. What are some examples of documentary methods of verification?

Documentary verification may include physical proof of identity or incorporation, i.e., visual inspection of documents. Examples include, but are not limited to, an unexpired driver's license, passport, business license, certificate of good standing with the state, or documents showing the existence of the entity, such as articles of incorporation. These documents can be presented physically at the time of account opening, as well as virtually (e.g., opening an account with a financial institution online by providing a driver's license number in an electronic form).

470. What are some examples of nondocumentary methods of verification?

Nondocumentary verification may include positive, negative or logical verification of a customer's identity. Positive verification ensures that material information provided by customers matches information from third-party sources. Negative verification ensures that information provided is not linked to previous fraudulent activity. Logical verification ensures that the information is consistent (e.g., area code of the home number is within the ZIP code of the address provided by the customer).

Examples of nondocumentary verification include phone calls; receipted mail; third-party research (e.g., Internet or commercial databases); electronic credentials, such as digital certificates; and site visits. Site visits should be conducted using a risk-based approach and should not be limited to account opening, but also conducted periodically for high-risk relationships such as foreign correspondent banking relationships.

Regardless of the type of nondocumentary verification used, a financial institution must be able to form a reasonable belief that it knows the true identity of the customer.

471. What resources are currently available to financial institutions to assist in the verification process?

Various public record search engines and commercial databases allow financial institutions to conduct ID matches (e.g., determining that a customer's TIN is consistent with his or her DOB and place of issue) and to check for prior fraudulent activity.

472. Should a financial institution collect additional information on its customers beyond CIP?

Based on its risk assessment, a financial institution may require identifying information in addition to the items above for certain customers or product lines. For further guidance on customer due diligence and enhanced due diligence, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence section.

473. Can a financial institution open an account for a customer even if it cannot form a reasonable belief that it knows the customer's true identity?

Although a financial institution may allow a customer under certain circumstances to use an account while the financial institution attempts to verify the customer's identity, the financial institution's CIP procedures should identify the terms under which this will occur, when the financial institution should close an account after attempts to verify the customer's identity have failed and when the financial institution should file a SAR.

474. Should financial institutions conduct verification for individuals with authority or control over a business account (e.g., authorized signers, grantors)?

Based on its risk assessment, a financial institution may require identifying information for individuals with authority or control over a business account for certain customers or product lines.

475. Should subsidiaries of financial institutions implement a CIP?

The federal banking agencies take the position that implementation of a CIP by subsidiaries is appropriate as a matter of safety and soundness and protection from reputation risks.

476. What types of addresses can financial institutions accept as identifying information?

For an individual, Section 326 requires that a residential or business street address be obtained. If an individual does not have a residential or business street address, an Army Post Office (APO) box number, Fleet Post Office (FPO) box number or rural route number may be accepted. Alternatively, the residential or business street address of next of kin or of another individual may be accepted. For companies, a principal place of business, local office or other physical location must be obtained.

477. Can a financial institution accept a rural route number?

Yes. A rural route number is a description of the approximate area where the customer is located. These types of addresses are commonly used in rural areas and are acceptable for a customer who, living in a rural area, does not have a residential or business address.

478. What type of identification number can financial institutions accept?

A taxpayer identification number (TIN) should always be obtained for U.S. persons. For non-U.S. persons, one or more of the following should be obtained:

- TIN
- Passport number and country of issuance
- Alien identification card number
- Number and issuing country of any other unexpired government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard

The identification obtained must be government-issued and unexpired. Although Section 326 does not prescribe that the form of identification bear a photograph in all cases, many financial institutions make this a requirement.

479. What steps should a financial institution take if the customer has applied for, but has not yet received, a TIN?

The financial institution's CIP should include procedures for opening an account for a customer who has applied for, but has not yet received, a TIN. The financial institution's CIP must include procedures to confirm that the TIN application was filed before the customer opens the account. Additionally, the financial institution must take measures to ensure it has received the TIN in a reasonable amount of time.

480. Can a financial institution open an account for a U.S. person who does not have a TIN?

Though the financial institution does not need to have the TIN at account opening for new customers, the financial institution must receive the TIN in a reasonable amount of time. Financial institutions, however, are able to open additional accounts for existing customers without TINs if they have a reasonable belief that they know the identity of the customer. The financial institution should have procedures in place to track compliance with this requirement and close accounts, as appropriate.

481. Can financial institutions rely on other types of identification cards other than a passport?

The decision of whether to rely on other forms of identification (e.g., Matricula Consular IDs) must be made by the financial institution. Regardless of this decision, the financial institution must be able to form a reasonable belief that it knows the true identity of its customers.

Updating CIP for Existing Customers

482. What are the obligations of financial institutions to update CIP information for existing customers?

Financial institutions are exempt from performing CIP on existing clients so long as the institution has a "reasonable belief" that it knows the true identity of the customer. The regulation does not provide any guidance as to what constitutes "reasonable belief."

To a large extent, the acceptability of exempting existing customers from CIP requirements inevitably will depend on the strength of the financial institutions' customer identification procedures prior to implementation of its CIP. Financial institutions that had strong customer identification procedures will have a better case for exempting customers.

483. What are the obligations of financial institutions to update customer information beyond CIP for existing customers?

A customer's information should be updated if there are significant changes to the customer's transaction activity or the risk level to the customer's account. Financial institutions should consider a risk-based approach to updating customer information beyond CIP, such as nature of business/occupation and expected activity. For additional guidance on obtaining and updating customer information beyond CIP, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence section.

Record Retention

484. Should copies of identifying information be made and retained?

Section 326 does not require a financial institution to make copies of identifying information. However, Section 326 does require a financial institution to retain records of the method of identification and the identification number. For example, if an individual's passport was reviewed as identifying information, the financial institution should note the fact that the passport was seen, and should document and retain the passport number and issuing country. While it is not required that identification be copied and retained, financial institutions may choose to adopt this procedure as a leading practice, although they must also be mindful of the implications of maintaining copies of identification in light of fair lending and other anti-discrimination laws.

485. How long must original account opening information be maintained?

Section 326 requires that a financial institution retain the identifying information obtained at account opening for five years after the date the account is closed or, in the case of credit card accounts, five years after the account is closed or becomes dormant. The required retention period may be longer than five years, depending on the state or self-regulatory organization (SRO).

486. How does the record retention period apply to a customer who opens multiple accounts in a financial institution?

If several accounts are opened for a customer, all identifying information about a customer obtained under Section 326 must be retained for five years after the last account is closed or, in the case of credit card accounts, five years after the last account is closed or becomes dormant.

487. How does the record retention period apply to a situation where a financial institution sells a loan but retains the servicing rights to the loan?

When a loan is sold, the account is "closed" under the record retention provision, regardless of whether the financial institution retains the servicing rights to the loan. Thus, records of identifying information about a customer must be retained for five years after the date the loan is sold.

488. If the financial institution requires customers to provide more identifying information than the minimum required by Section 326 at account opening, is it required to keep this information for five years?

Yes. If the financial institution obtains other identifying information at account opening in addition to the minimum required, such as the customer's phone number, then this information must be retained for the same period as the required information.

List Matching

489. What requirements does Section 326 impose on financial institutions regarding list matching?

Financial institutions also are required to screen their customers against government sanctions lists to determine whether the individual/entity appears on any list of known or suspected terrorists or terrorist organizations. For additional guidance on government sanctions, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

490. Has FinCEN provided financial institutions with a comprehensive list of known or suspected terrorists or terrorist organizations to screen against as required in Section 326?

No. FinCEN has not provided one consolidated list of entities that should be included in the financial institutions' screening software. For additional guidance on government sanctions, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

Customer Notice

491. What notification requirements does Section 326 impose?

A financial institution is obligated to notify its customers that it is requesting information to verify identity. Many financial institutions have incorporated the notification language into their account opening documentation in order to ensure that the notice is properly delivered to both primary and joint account holders.

492. Should notifications be provided to all owners of a joint account?

Yes. Notice must be provided to all owners of a joint account. However, a financial institution may satisfy this requirement by directly providing the notice to any account holder of a joint account for delivery to the other owners of the account.

493. Must this notification to customers be provided in writing?

Section 326 does not require that the notification be in writing, but it must be provided in a manner reasonably designed to ensure that a customer is able to view the requirement or is given it before opening the account.

Third-Party Reliance

494. Can a financial institution rely upon a third party to conduct all or part of the financial institution's CIP?

Yes. A financial institution may rely on other federally regulated institutions to conduct all or part of the financial institution's Customer Identification Program (CIP). Such reliance is permitted only when:

- Such reliance is reasonable.
- The other financial institution is regulated by a federal functional regulator.
- The other financial institution is subject to a general Bank Secrecy Act (BSA) compliance program requirement.

- The other financial institution shares the customer with the financial institution.
- The two institutions enter into a reliance contract that contains certain provisions.

495. What obligations does Section 326 impose on third-party financial institutions conducting part or all of the financial institution's CIP?

The third-party financial institution must provide an annual certification that it has implemented its AML program and that it will perform (or its agent will perform) the specified requirements of the financial institution's CIP.

496. What guidance has been issued on third-party service providers (TPSP)?

The following are examples of guidance that has been issued on third-party service providers:

- **Third-Party Payment Processors – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 17: Reliance on Third Parties** (2012) by the Financial Action Task Force (FATF)
- **Retail Payment Systems** and **Wholesale Payment Systems Booklet** (2004) within the FFIEC Information Technology Examination Handbook by the FFIEC
- **Third-Party Senders and the ACH Network: An Implementation Guide** (2012) by The Electronic Payments Association (NACHA) (formerly National Automated Clearing House Association)
- **Bank Use of Foreign-Based Third-Party Service Providers** (2002) by the Office of the Comptroller of the Currency (OCC)
- **Risk Management Principles for Third-Party Relationships** (2001) by the OCC
- **Payment Processor Relationships** (2012) by the Federal Deposit Insurance Corporation (FDIC)
- **Guidance on Managing Third-Party Risk** (2008) by the FDIC

Section 352 – AML Program

Overview

497. What are key elements of an effective AML program as required by Section 352 of the USA PATRIOT Act?

At a minimum, Section 352 requires financial institutions to establish AML programs, including:

- Development of written internal policies, procedures and controls
- Designation of an AML compliance officer
- Ongoing AML employee-training program
- Independent testing of the AML program

498. Should the AML program be limited to the key elements above as required by Section 352 of the USA PATRIOT Act?

No. The AML program should be customized to the institution, cover all aspects of the business and address the following, at minimum:

- **Designated Compliance Officer** – For further guidance, please refer to the Designation of AML Compliance Officer and AML Compliance Organization section.
- **Risk Assessments** – For further guidance, please refer to the Business Line Risk Assessment, Customer Risk Assessment and OFAC Risk Assessment sections.

- **Customer Acceptance and Maintenance Program** – For further guidance, please refer to the Know Your Customer, Due Diligence and Enhanced Due Diligence, Section 326 – Verification of Identification, Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts and High Risk Customers sections.
- **Large Currency Monitoring and Currency Transaction Report Filing Program** – For further guidance, please refer to the Currency Transaction Reports section.
- **Monitoring, Investigating and Suspicious Activity Report Filing Program** – For further guidance, please refer to the Transaction Monitoring, Investigations and Red Flags and Suspicious Activity Report sections.
- **Sanctions Program** – For further guidance, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.
- **Information Sharing** – For further guidance, please refer to Section 314(a) – Cooperation among Financial Institutions, Regulatory Authorities and Law Enforcement Authorities, Section 314(b) Requirements – Cooperation among Financial Institutions and National Security Letters sections.
- **Recordkeeping and Retention Program** – For further guidance, please refer to the Funds Transfer Recordkeeping Requirement and the Travel Rule, Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments, Form 8300 and Report of Foreign Bank and Financial Accounts sections.
- **Independent Testing** – For further guidance, please refer to the Independent Testing section.
- **Training** – For further guidance, please refer to the AML Training section.
- **Management and Board Reporting** – For further guidance, please refer to the Designation of AML Compliance Officer and AML Compliance Organization section.

It is important to note that not all types of financial institutions are required to have each of the key components listed above. For additional guidance on the AML requirements of nonbank financial institutions, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

499. How often should the AML program be reviewed and approved?

The AML program should be updated on an ongoing basis to address changing risks facing the financial institution (e.g., new products and services, new target markets), as well as changing control structure throughout the organization (e.g., upgrades to or implementation of new AML monitoring systems, added roles and responsibilities of compliance staff). At minimum, however, the AML program should be approved by the board of directors and senior management on an annual basis or when material changes are made to the AML program.

500. How can a financial institution maintain a successful and effective AML program?

A key element of maintaining an effective AML program is to emphasize the importance of AML compliance across all business lines, as well as to demonstrate the importance of the AML program to customers. Building a compliance culture throughout the financial institution will lead to a stronger and more effective compliance program, as well as deter unwanted risks for the financial institution. Some common practices to encourage compliance throughout the financial institution include:

- Ensuring consistency between the practices of the institution and policies and procedures
- Embedding compliance requirements into business processes
- Ensuring timely communication between Compliance and senior management on compliance matters
- Establishing roundtables or group forums around compliance matters
- Conducting customized compliance training sessions for lines of business
- Requiring attestation to code of conduct as a condition of employment
- Communicating and enforcing specific and clear consequences for noncompliance
- Developing direct incentives for compliance tied to the compensation process
- Developing Key Performance Indicators (KPIs) for measuring the effectiveness of the compliance program

501. What are the most common gaps in the AML compliance efforts of financial institutions?

Often financial institutions do not recognize the breadth and applicability of the AML laws and regulations, and thus underestimate the resources and commitment required to achieve compliance with the regulations. This has commonly resulted in the following problems and issues:

- AML compliance officer (as well as other employees) lacks sufficient experience and/or knowledge regarding AML policies, procedures and tools
- Insufficient/inadequate resources dedicated to AML compliance
- Lack of specific and customized training of employees with critical functions (e.g., account opening, transaction processing, risk management)
- Failure to conduct adequate risk assessments (e.g., customer risk assessment, business line risk assessment, OFAC risk assessment)
- Failure to incorporate risk assessments into a transaction-monitoring process, customer acceptance standards, audits, testing or training
- Inadequate KYC (e.g., CIP, CDD and EDD procedures at or after account opening, including inadequate controls over required fields, inadequate methods of obtaining and/or maintaining current information, lack of reporting capabilities over missing information and lack of verification procedures)
- Poor documentation maintained for investigations that did not lead to SAR filings
- Poor follow-up on SAR actions (e.g., close, monitor)
- Lack of reporting of key SAR information to senior management/board of directors
- Inadequate tuning, validation and documentation of automated monitoring systems
- Overreliance on software to identify transactions for which CTRs and/or SARs must be filed without fully understanding how the software is designed and what information it does and does not capture
- Exclusion of certain products from transaction monitoring (e.g., loans, letters of credit, capital markets activities)
- Lack of timeliness when filing CTRs and SARs (e.g., reports are manually filed via certified mail, and the date postmarked is not noted)
- Lack of or inadequate independent testing of the AML Compliance Program
- Lack of or untimely corrective actions to prior examination or audit findings

In order to identify potential gaps in a financial institution's AML Compliance Program, regulatory enforcement actions for AML deficiencies against other (similar) financial institutions should be reviewed to identify the specific violations and related action steps. This enables financial institutions to recognize and correct any potential weaknesses of their own before their next regulatory examination.

Policies and Procedures

502. What is required under Section 352 of the USA PATRIOT Act with regard to policies and procedures?

A financial institution is required to have written AML policies and procedures as part of its AML program.

Written AML policies and procedures should incorporate the following:

- Definition of money laundering and terrorist financing
- Legislative and regulatory framework (federal, state and international, if applicable)
- Standards of knowledge
- AML-related roles and responsibilities (including reliance placed on any third parties)
- Principal products and service offerings and customer base

- AML risk assessment methodologies (i.e., business line risk assessment, customer risk assessment, OFAC risk assessment)
- Customer acceptance and maintenance standards (CIP/CDD/EDD/KYC)
- Examples of suspicious activities specific to the financial institution
- Investigation, reporting and recordkeeping requirements for suspicious activity
- AML training (e.g., type of training, frequency of training)
- Use of systems to support the compliance effort, especially maintenance, tuning and validation of automated transaction monitoring systems
- Internal testing, which includes details of the steps and frequency of testing for compliance with the policies and procedures and the requirements for communicating the results of the testing and following up on any deficiencies noted
- Independent testing of the AML program

503. Can one set of policies and procedures be applied uniformly throughout an institution?

The AML policy should be developed and adopted at the corporate level. Because financial institutions have many different departments and service offerings, a "one-size-fits-all" approach to procedures implementing the corporate policy generally would not be adequate. It is essential that procedures be customized to different departments and product areas to mitigate the money laundering and terrorist financing risk to that particular department and the specific product offering concerned.

504. Should an institution separate its policies from its procedures?

Since changes in AML policy require approval by senior management and/or the board of directors, many companies separate policies from procedures to allow for prompt modifications to procedures to provide clarification to policies or address new regulatory requirements.

505. Where should the AML policies and procedures be stored?

In many cases, the compliance department maintains the most recent versions of the AML policies and procedures for ease of updating. Some financial institutions, however, have a dedicated department that is responsible for maintaining all of the financial institution's policies and procedures in a central location. Wherever the policies and procedures are stored, the financial institution should have a mechanism in place to ensure that the most recent (and approved) policies and procedures are available for both reference and submission to the financial institution's regulators upon request.

In addition, many financial institutions post AML policies on an internal website so that all employees can reference the documentation.

506. How can a financial institution ensure all of its employees are familiar with its AML policies and procedures?

Many financial institutions include a review of AML policies and procedures during new-hire training and third-party introductions to the institution (depending upon an employee's/third party's roles and responsibilities within the institution). Additionally, the ongoing AML training of employees, required by Section 352, commonly addresses the AML policies and procedures.

Also, many compliance departments develop and distribute AML publications to staff. These publications reiterate roles and responsibilities outlined within AML policies, as well as requirements of AML laws and regulations applicable to the institution. They commonly are posted on the institution's internal website for future reference.

Designation of AML Compliance Officer and the AML Compliance Organization

507. What is required under Section 352 of the USA PATRIOT Act with regard to the AML compliance officer?

Section 352 requires the designation of an AML compliance officer by the board of directors.

508. What is the role of the AML compliance officer?

The AML compliance officer generally is responsible for developing and maintaining the AML Compliance Program, including policies and procedures; ensuring the timely and accurate filing of required reports; coordinating AML training (within the compliance department and with relevant employees); and acting as the liaison for AML-related matters with regulators. In addition, many AML compliance officers oversee the transaction monitoring function.

Beyond these general points, the role of the AML compliance officer will vary by institution depending on its size and the availability of resources. In some instances, the AML compliance officer is responsible for OFAC compliance; in larger institutions, an OFAC compliance officer is responsible for OFAC compliance. Accordingly, the role of the AML compliance officer should be documented clearly in a job description.

509. What is the role of the board of directors with respect to the AML program?

The board of directors is responsible for ensuring that adequate resources are provided to promote and support an effective AML program. In addition, the board of directors is responsible for designating the AML compliance officer, for approving AML policy and for periodically reviewing the status of the AML program, often through periodic reporting made by the AML compliance officer.

510. What is the role of senior management, with respect to the AML program?

Senior management, together with other members of the senior management team, is responsible for continually reinforcing the importance of compliance to all personnel of the financial institution. This is accomplished through creating an environment where compliance is of the highest priority through, for example, considering compliance in all employee evaluations and ensuring that the AML compliance department has the support and cooperation of all business units. Senior management also should ensure that the financial institution has adequate resources to effectively perform its AML compliance responsibilities and assure that such responsibilities are being carried out in accordance with approved policies and procedures.

511. Is the AML compliance officer for a financial institution required to receive the board of directors' approval to file a SAR?

No. The AML compliance officer should not seek approval from the board of directors or any business line for Suspicious Activity Report (SAR) filings. Though Compliance may involve the business to aid in its investigation of unusual or potentially suspicious activity, the department must make its own determination as to whether the activity identified warrants a SAR filing. In many instances, the AML compliance officer makes the final decision to file or not file a SAR. In some instances, a committee is established to review the case and decide to file or not file a SAR.

It is important to note, however, that the board of directors and senior management should be notified of SAR filings. Since regulations do not mandate a particular notification format, financial institutions have flexibility in structuring their format and may opt to provide summaries, tables of SARs filed for specific violation types, or other forms of notification as opposed to providing actual copies of SARs.

512. In addition to SAR-related information, what information should be included in periodic reports to senior management and/or the board of directors?

Management reporting will vary depending on the type of financial institution, the nature of the products and services it offers, and the clients it serves. The following are non-exhaustive examples of key risks and key performance indicators related to the AML Compliance Program that may be considered:

- **Suspicious Activity Reports (SARs) and significant investigations**
    - Number of SAR filings and associated volume of suspicious activity and deposit/lending balance of named subjects
    - Explanations for significant changes in volume of SAR filings
    - Volume of alerts, investigations
    - Alert-to-investigation ratio, investigation-to-SAR ratio
    - Summary of significant investigations (e.g., high volume of suspicious activity, uncovered weakness in monitoring program, investigations involving insiders, politically exposed persons [PEPs])
- **Currency Transaction Reports (CTRs)**
    - Overall volume of cash activity

    - Number of CTR filings and associated volume of cash activity
    - Explanations for significant changes in volume of cash activity/CTR filings
- **Office of Foreign Assets Control (OFAC) and other sanctions reporting**
    - Number of OFAC blocked/rejected report filings and associated volume of blocked/rejected activity and deposit/lending balance of named subjects
    - Results of OFAC risk assessment
- **Information sharing**
    - Number of confirmed 314(a) matches and associated deposit/lending balance of named subjects
    - Number of incoming/outgoing 314(b) requests and associated deposit/lending balance of named subjects
    - Number of National Security Letters (NSLs)
    - Number of subpoenas and other information requests
- **Training**
    - Number of exceptions (e.g., employees who have not completed or who have failed training)
    - Summary of significant updates to the training program
- **Monitoring**
    - Major changes to the automated systems being used to support the company's AML Compliance Program and rationale for the changes
- **Third-party reliance**
    - Periodic discussion of any third parties on which the company relies for any part of its AML or sanctions compliance programs and actions taken by the company to satisfy itself with third parties' compliance efforts
- **Risk assessments**
    - Results of executed AML risk assessments (e.g., business line, customer, OFAC), including inherent risk, ratings of controls/control environment, and residual risk
    - Explanations for significant changes in risk and control ratings
    - Summary of significant changes to risk assessment methodologies
    - Number of high-risk customers and associated deposit/lending balances
    - New products/services/transaction types and associated risks
    - New target markets (e.g., customer type, geography) and associated risks
- **Examination/independent testing/self-testing findings**
    - Summary of findings and status of corrective actions
- **Changes in laws, regulations or regulatory expectations**
    - Summary of new requirements and their impact on the company
- **"Current events"**
    - Details of recently reported money laundering/terrorist financing schemes, to the extent that the company may, because of its products/services and customers, be subject to risk and discussion of controls in place to mitigate such risks

The content, level of detail and frequency of reports should be tailored to the audience (e.g., business line management, compliance, risk management, senior management, board of directors).

513. Should Compliance be involved in the decision to offer new products?

Compliance should be aware of a financial institution's plans to offer new products and services and should work with relevant parties in the institution to ensure compliance risks are considered appropriately. The ultimate decision to

offer a new product or service, however, rests with the business; however, Compliance should be on record if it believes the product or service exposes the institution to undue or difficult to manage risks.

514. Should Compliance be involved in the decision to enter into customer relationships?

Many financial institutions have developed customer acceptance committees that meet on a regular basis to discuss high-risk prospects (e.g., those customers posing increased credit risk, AML risk, reputation risk) wishing to enter into a relationship with the financial institution. The committee should be composed of members from each business line and Compliance. While Compliance can provide its view on the risks associated with the prospect, the decision to enter into a customer relationship rests with the business.

515. Should Compliance be involved in the decision to exit a customer relationship?

As with customer acceptance committees, many financial institutions have developed committees that meet on a regular basis to discuss high-risk customers (e.g., those customers who have defaulted on a number of credit products, customers subject to SARs). The committee should be composed of members from each business line and Compliance. While Compliance can provide its view on the risks associated with the customer and regulators encourage Compliance to challenge the business, the ultimate decision to exit a customer relationship usually rests with the business.

AML Training

516. What is required under Section 352 of the USA PATRIOT Act with regard to training?

Section 352 requires an ongoing AML training program for relevant employees.

517. What are the key components of an AML training program?

An AML training program needs to be customized to an institution. For institutions with many different departments and products, it may even need to be customized further for each different department or product.

A basic AML training program should incorporate the following:

- Background on money laundering and terrorist financing
- Summary of the key AML laws and regulatory requirements (federal, state and international, if applicable)
- Requirements of the AML policies and procedures of the financial institution
- Summary of how the AML laws and regulatory requirements impact the financial institution
- Roles and responsibilities of the employees in attendance
- Suspicious activity red flags and case studies
- Consequences of noncompliance

518. What form does the training typically take?

The form of AML training depends on a financial institution's preference (e.g., cost, level of interaction). Financial institutions have several methods of delivering AML training:

- Computer-based training (CBT) (e.g., delivered through the intranet, Internet or downloaded/installed applications)
- Face-to-face training
- Outsourcing

For additional guidance on AML training software, please refer to the AML Technology section.

519. Should external training be included as part of a financial institution's AML training program?

Although not required, outside seminars and conferences may be appropriate for employees with overall responsibility for AML compliance efforts (e.g., AML compliance officer, internal audit director). Financial institutions can keep abreast of industry standards through their interactions with peer institutions.

520. How often should the AML training program be updated?

The AML training program should be reviewed and updated as necessary to reflect current developments in and changes to laws and regulations, money laundering and terrorist financing trends and developments, and internal policy. It also should be reviewed or updated based on areas of weakness as indicated by employee test scores (assuming quizzes are given as part of the training).

521. Should OFAC training be included as part of the AML training program?

OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. As a result, OFAC training is often included in the AML training program.

522. How can a financial institution measure the effectiveness of the training provided?

Some financial institutions choose to provide employees with a quiz at the end of the training session, as this often encourages employees to take the training seriously. It also provides the compliance department with an idea of employee understanding of AML requirements and isolates topics that need to be expanded to improve the overall AML training program.

523. Who should attend AML training?

Employees, permanent or temporary, who have direct or indirect contact with customers, open customer accounts, or process transactions or customer information should attend AML training.

In addition, employees in compliance, accounting and internal audit departments, as well as those personnel in management functions (including senior management and board members), should attend AML training.

524. Is it sufficient for the AML Compliance Officer to attend only internal training?

Regulators expect that AML Compliance Officers have broad knowledge of industry trends and peer practices. The best way to gain this perspective is to attend external training and networking events. Some recent regulatory enforcement actions, in fact, have mandated that the AML Compliance Officer attend external training.

525. Should nonemployees (e.g., vendors, agents) attend the AML training of an institution?

The vendor's roles and responsibilities should be taken into consideration when determining if nonemployees should be required to attend AML training.

526. How frequently should employees attend AML training?

While there is no formal requirement regarding the frequency of AML training, employees should attend AML refresher sessions on at least an annual basis. Financial institutions may also consider providing certain employees (such as those in account opening, transaction processing and compliance roles) with training on a more frequent basis (e.g., semiannually). New employees should receive training upon commencement of employment and prior to assuming their duties.

527. What records should be retained to evidence AML training of employees?

It is important that financial institutions retain records evidencing that their employees have attended AML training. Maintaining not only the attendance list, but also the agenda, training materials and employees' quiz scores (if applicable), will assist in assessing the overall quality of the AML training during the independent testing/audit of a financial institution's AML training program.

Independent Testing

528. What is required under Section 352 of the USA PATRIOT Act with regard to independent testing?

Section 352 requires a periodic independent testing of the AML program.

529. How does independent testing of the AML program differ from the AML compliance monitoring function?

The AML compliance department is responsible for developing and implementing an organization's overall AML Compliance Program, including AML compliance policies and procedures. Individual departments are required to adhere to those policies by developing their own procedures to comply with the organization's compliance policies. The compliance department may monitor business-unit adherence to policies and procedures in a number of ways, including reviewing business-unit self-assessments and conducting periodic reviews. Independent testing must be conducted by individuals independent of the compliance function and, in the same way as an internal audit, is intended to test compliance with legal and regulatory requirements and internal AML-related policies, procedures and controls. Regulators expect that independent tests will be risk-based.

530. What does the term "risk-based" mean for independent testing purposes?

For the purposes of independent testing, "risk-based" means that the scope and approach (e.g., determining sample selection methodology and sample sizes) are based on consideration of an organization's AML risk, as determined by its own risk assessment and/or a risk assessment performed by the independent reviewer. Put simply, in a risk-based examination, priority is given to areas of highest risk as well as areas that were previously criticized.

531. What should the independent testing incorporate?

The objective of the independent testing is to assess compliance with the institution's AML program, with particular focus on specific USA PATRIOT Act Section 352 requirements, including the development and maintenance of written policies, procedures and controls; the designation of an AML compliance officer; and the design and implementation of an AML training program. The policies and procedures must be tested to confirm that they contain procedures for meeting regulatory requirements and are updated in a timely manner to meet any newly developed regulatory requirements. A comprehensive independent test will include, at minimum, coverage of the following:

- Role of the board of directors and senior management
- The AML compliance organization
- AML risk assessment methodologies (e.g., business line risk assessment, customer risk assessment, OFAC risk assessment)
- Customer acceptance and maintenance standards (CIP, CDD, EDD)
- Monitoring and investigation, including adequate transaction testing
- Recordkeeping and reporting
- Training
- AML policies and procedures
- Management reporting
- A review of the results of previous independent reviews and regulatory examinations
- Use of third parties
- Use of technology (e.g., implementation, maintenance, tuning, validation, etc)

532. Should the OFAC program be included in the scope of the independent testing of the AML program?

OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on what should be considered with respect to independent testing of an OFAC program, refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

533. How often should the AML program be independently tested?

The frequency of the independent testing should be based upon the risk profile of the institution. Typically, AML programs are tested every 12 to 18 months.

534. Can AML program elements be tested separately, or does the entire program need to be tested at one time?

Elements of the AML program can be tested separately. A summary of the testing results should be prepared periodically to provide an overall assessment of the AML program.

535. If an institution manages its AML program at the corporate level, does there need to be a separate independent testing for each legal entity?

The requirement that an independent testing be conducted applies to each covered legal entity, so even though the AML program may be uniform across the organization, either a separate independent testing report should be prepared for each applicable legal entity or the entire report should be presented to the board of each legal entity.

536. What are some of the common criticisms of independent AML testing?

Regulatory criticisms of AML testing have included inexperienced or inadequately trained testers/auditors, insufficient or not appropriately risk-based coverage of the AML program, insufficient transaction testing, limited attention paid to the quality of training, limited understanding and inadequate testing of automated monitoring software, poor quality work papers, and inadequate follow-up on previously identified issues in prior audits or in regulatory examination reports.

537. What are the consequences of not having an effective independent testing program?

Developing and maintaining an effective independent testing program is required under the USA PATRIOT Act. Failure to maintain an effective testing program is a violation of the law and can lead to regulatory enforcement actions and civil money penalties.

538. Have financial institutions ever been penalized for not having performed an independent review, or for having a review conducted that was deemed to be inadequate?

Yes. The requirement to perform periodic independent testing is one of the four required components of an AML program. As such, not performing an independent review or not addressing cited deficiencies in the independent review provides the basis for an enforcement action. It is not uncommon for AML-related enforcement actions to cite multiple deficiencies related to independent testing.

539. How should the independent testing address senior management and board involvement and reporting?

Independent testing of senior management and board involvement and reporting should include testing to ensure that required reports (e.g., information on SARs) are provided to the board of directors. The testing should also evaluate whether management and the board of directors are sufficiently informed of the trends and issues related to AML compliance, internally and within the industry.

540. What should be considered with respect to independent testing of the compliance organization?

An assessment of the compliance organization must include verifying that the institution has a duly appointed AML compliance officer as required by Section 352 and making a determination that this individual has the experience, qualifications, and stature within the organization necessary to direct the AML program. However, the success of the AML compliance effort depends on much more than the performance of one individual. Other factors that impact the effectiveness of the compliance effort and should be considered include the resources (staff and tools) available for AML compliance; the autonomy of the AML compliance function; the level of access the AML compliance officer has to senior management, counsel, and the audit or compliance committee; how well roles and responsibilities with respect to AML compliance have been delineated throughout the institution; and the extent to which senior management and the board of directors are involved in the AML compliance effort.

541. How should the independent testing address the AML risk assessment methodologies?

The independent testing should include a reasonableness test of the risk assessment methodologies (e.g., a determination of whether risk assessment methodologies incorporate the right variables to identify the institution's high-risk accounts and customers; tests to determine whether risk ratings are applied consistently). Additionally, the independent tester should assess how the risk assessment process has an impact on other aspects of the institution's AML program, notably the account opening (CIP/CDD/EDD/KYC) process, transaction monitoring, compliance monitoring, audits and training. Effective and meaningful risk assessment processes will drive the documentation requirements for new customers, be used to establish priorities for monitoring, and assist AML compliance with focusing its resources on business lines and customers posing the highest risk in terms of money laundering and terrorist financing. For additional guidance on risk assessment methodologies, please refer to the Risk Assessments section.

542. What should the independent testing of monitoring and investigations include?

Independent testing of monitoring should include verifying that the institution has procedures for (a) keeping customer information current (such as requirements that customer profiles are updated on a periodic basis, customer visits/calls are documented for the file, and adequate follow-up occurs on any media or other third-party information about a customer), and (b) transaction and account monitoring. The independent testing also should consider the staffing of the monitoring and investigative functions, both in terms of whether there is an adequate number of people and if they have the experience and skills necessary to be effective. Tests also should be conducted to assess the timeliness and quality of the monitoring and investigative functions; this should include reviewing a sample of transactions/accounts (often both) to determine how potentially unusual or suspicious activities are identified, what prompts the decision to conduct an investigation, and how well-documented and timely the institution's decisions are to file or not file a Suspicious Activity Report (SAR). Additionally, the independent testing should consider reviewing a sample of investigations, as well as a sample of SARs filed to determine whether they have been prepared in accordance with the guidance provided by FinCEN. For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

543. Are there additional considerations that should be included for testing AML technology that is used to support AML suspicious activity monitoring processes?

The most common technology solutions used to support AML suspicious activity monitoring processes include suspicious transaction monitoring software and case management software, collectively referred to as the monitoring system. When conducting an independent test, these technology solutions should be tested not only for how end-users are utilizing the capabilities of the system, but the operating effectiveness of the system as well. Some institutions opt to include some of this testing as part of its overall independent test of the AML Compliance Program or separately, as part of an IT systems-specific review.

For testing to determine whether the monitoring system is adequately utilized by end-users to address the unique monitoring needs and transactional risks of a financial institution, the review should include, but not be limited to the following:

- **Coverage** – Does the system accommodate all of the products, services and transactions of the institution? If so, did end-users tailor the system to adequately monitor these products, services and transactions?
- **Risk-Based Approach** – Does the system allow for risk-rating (e.g., customers, transactions, alerts)? If so, did the end-users incorporate its risk assessment methodology and results into the design of monitoring rules and parameters?
- **Types of monitoring rules** – What types of monitoring rules and parameters for generating alerts does the system perform (e.g., artificial intelligence (AI), rules-based, profiling, outlier detection)? Did end-users implement meaningful rules and parameters to detect potentially suspicious activity? Are rules subject to periodic review and tuning?
- **Case management** – How does the system output alerts? Does the system have an adequate case management/audit trail functionality? If so, did end-users adequately document reviews of alerts and/or investigations within the system?

A review of the operating effectiveness of a monitoring system should include, but not be limited to the following:

- **Data integrity and continuity** – Does information being input into the system correspond to the information output by the system?

- **Data source and feeds** – Is the information needed for the system to operate correctly actually being captured by the system? This may include the linking and tying of multiple information platforms across the institution.
- **Data processing** – Does the system perform its intended functions at the appropriate times including as information is processed or on a cumulative periodic basis?
- **Model risk management** – Is there effective review and challenge of the system by knowledgeable personnel?
- **Security and change management** – Are there restrictions or monitoring tools in place to prohibit users from making modifications to the software's capabilities?
- **Information reporting** – Do the end-user reports generated by the system contain the appropriate information and accurately reflect the various types of occurrences which may take place within the system?
- **Business continuity** – Are technologies that support the compliance program considered in the institution's business continuity/disaster recovery planning?

For further guidance on technology solutions, please refer to the AML Technology section.

544. What should the independent testing of recordkeeping and reporting requirements include?

In addition to SAR filing requirements, financial institutions may be subject to the following AML-related recordkeeping and reporting requirements: CTRs, SARs, designation of exempt persons, CMIRs, FBARs, wire transfer recordkeeping, monetary instrument recordkeeping, foreign bank certifications, 314(a) notifications, 314(b) participation, the "120-hour rule," OFAC regulations, Special Measures and record retention requirements. The audit of recordkeeping and reporting should be designed to include testing of appropriate samples for each of the applicable requirements.

545. Determining whether AML training is taking place seems straightforward, but what else about the AML training program should be considered as part of the independent testing?

In addition to checking attendance to ensure all designated individuals have received training, it is important that the independent testing consider the quality of the AML training being provided. That means making a determination of whether the training is appropriately customized to the audience. A financial institution may offer generic AML training to introduce management and employees to AML concepts and issues, but individuals who play key roles in carrying out the institution's AML program (including, for example, individuals with customer contact and operations staff) should be provided with customized training that focuses on clearly explaining the responsibilities these individuals have in helping the institution combat money laundering and terrorist financing, and includes "red flags" appropriate to the areas in which the individuals work.

The audit also should consider the importance the financial institution places on AML training. In part, this may be gauged by whether the institution is diligent in ensuring that designated individuals attend training. Another factor to consider may be whether training is followed by testing and, also, what (if anything) happens to individuals who are unable to pass the test.

546. How should the independent testing address third-party reliance?

The Customer Identification Program (CIP) rules specifically allow financial institutions to rely on other regulated financial institutions to conduct elements of CIP. In this instance, the independent testing should verify that the third-party financial institution is subject to AML requirements and is regulated by a federal functional regulator, that the two institutions have entered into a contract delineating their respective responsibilities, and that the third-party financial institution certifies annually that it is complying with the requirements of the contract.

Financial institutions may rely on other financial institutions for other elements of their AML program (e.g., monitoring). In these instances, the independent testing also should assess how the third party was selected, verify the existence of detailed contractual arrangements, and determine how the relying financial institution satisfies itself that the third-party financial institution is meeting its contractual arrangements. Often, internal audit or SAS 70 reports may be available for review by the independent tester.

Financial institutions may rely on nonfinancial institution third parties, as well. Real estate brokers or automobile dealers, for example, may act as de facto agents of a bank; in these instances, the independent testing should include steps to determine how the financial institution conducts due diligence of its business associates and how it communicates its expectation for AML compliance to these associates.

547. Who should perform the independent testing of an institution's AML program?

The independent testing of an institution's AML program must be performed by individuals who are not responsible for the execution or monitoring of the institution's AML program.

An institution's internal audit department can perform the testing, individuals not involved in AML compliance or AML-related operations can perform the testing, or the institution can engage an outside party to perform such testing. In every case, the individuals performing the independent review must be qualified to execute the testing.

548. What experience and qualifications are necessary for conducting independent tests of AML programs?

In addition to basic auditing skills, independent testers must have knowledge of the applicable legal and regulatory requirements. They also must have a good understanding of the financial institution's customer base and the products and services it offers so they can identify the risks involved. Increasingly, as financial institutions continue to implement automated software for AML and OFAC monitoring, independent testers need technology skills, quantitative skills and a strong grasp of how AML software works.

549. When should the independent testing of the AML program be performed?

The independent testing of the AML program should be done in accordance with the financial institution's applicable Section 352 requirements and regulatory expectations.

Additionally, an independent test of an AML program should be conducted as part of the overall due diligence prior to acquiring new financial institutions to mitigate the risk of inheriting regulatory problems.

550. How should financial institutions evidence the performance of independent testing?

Upon completion of the independent testing, a written report should be issued to summarize the findings of the testing, including an explicit statement about the AML program's adequacy and effectiveness. Any recommendations arising from the testing also should be documented, and management should provide a written comment as to how and when it will address those recommendations.

The written report should be provided to senior management and/or the board of directors, the compliance department and the internal audit department, as well as any other relevant individuals or departments.

Work papers and other supporting documentation also should be maintained.

Section 505 – Miscellaneous National Security Authorities

551. What is a National Security Letter?

National Security Letters (NSLs) are written, investigative demands that may be issued by the local Federal Bureau of Investigation (FBI) office and other federal governmental authorities in counterintelligence and counterterrorism investigations to obtain the following:

- Telephone and electronic communications records from telephone companies and Internet service providers
- Information from credit bureaus
- Financial records from financial institutions

The authority to issue NSLs was expanded under Section 505 of the USA PATRIOT Act, which allows the use of NSLs to scrutinize U.S. residents, visitors or U.S. citizens who are not suspects in any ordinary criminal investigation. NSLs under Section 505 require no probable cause and are not subject to judicial oversight. However, under Section 505, NSLs cannot be issued for ordinary criminal activity, and may only be issued upon the assertion that information would be relevant to an ongoing terrorism investigation. As a result, many institutions question whether an NSL is indicative of terrorist activity requiring a SAR filing.

NSLs are highly confidential. Financial institutions, their officers, employees and agents are precluded from disclosing to any person that a government authority or the FBI has sought or obtained access to records. Financial institutions that receive NSLs must take appropriate measures to ensure the confidentiality of the letters.

552. Should an institution automatically file a SAR upon receipt of an NSL?

No. A financial institution should not automatically file a SAR upon receipt of an NSL. The decision to file a SAR should be based on the institution's own investigation into the activity of the party(ies) that/who is the subject of the NSL. If a financial institution files a SAR after receiving an NSL, the SAR should not contain any reference to the receipt or existence of the NSL. The SAR should reference only those facts and activities that support a finding of unusual or suspicious transactions identified by the financial institution.

Questions regarding NSLs should be directed to the financial institution's local FBI field office. Contact information for the FBI field offices can be found at www.fbi.gov.

OFFICE OF FOREIGN ASSETS CONTROL AND INTERNATIONAL GOVERNMENT SANCTIONS PROGRAMS

OFAC Basics

553. What is the role of the Office of Foreign Assets Control (OFAC)?

The purpose of OFAC is to promulgate, administer and enforce economic and trade sanctions against certain individuals, entities and foreign government agencies and countries whose interests are considered to be at odds with U.S. policy. Sanctions programs target, for example, terrorists and terrorist nations, drug traffickers and those engaged in the proliferation of weapons of mass destruction.

Overviews and details of each of the programs can be found on OFAC's website at www.treas.gov/ofac.

554. When was OFAC established?

OFAC was formally created in 1950, when President Harry S. Truman declared a national emergency following China's entry into the Korean War and blocked all Chinese and North Korean assets subject to U.S. jurisdiction.

555. How do OFAC regulations fit into AML compliance?

OFAC regulations are not part of AML compliance per se, but since the OFAC Sanctions lists include alleged money launderers and terrorists, institutions often consider the OFAC program to be a subset of their overall AML program.

556. Who is required to comply with OFAC Sanctions?

Contrary to a widely held belief that OFAC regulations are only applicable to financial institutions, OFAC requirements apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world; all persons and entities within the United States; and all U.S.-incorporated entities and their foreign branches. Requirements of certain OFAC programs also apply to subsidiaries of U.S. companies and to foreign persons in possession of goods of U.S. origin.

All individuals and entities subject to compliance are commonly referred to as "U.S. persons."

557. Should a foreign financial institution with no U.S. presence consider incorporating OFAC into a sanctions program?

Many international payments are settled in U.S. dollars using a U.S. dollar clearing account held at a U.S. institution that is required to comply with OFAC regulations. A foreign financial institution faces credit risk and reputation damage if it sends or receives funds to or from an OFAC-sanctioned individual, entity or country, since these funds likely will be blocked by the U.S. institution asked to clear the funds.

558. How does OFAC define the term "prohibited transactions"?

OFAC defines the term "prohibited transactions" as trades or financial transactions and other dealings in which "U.S. persons" may not engage unless previous authorization was granted by OFAC or was expressly exempted by statute.

559. Is there a dollar threshold applicable to prohibited transactions?

No. There is no defined minimum or maximum amount subject to OFAC regulations.

560. Does OFAC prescribe specific requirements for compliance programs?

No. Unlike AML laws and regulations, OFAC does not dictate specific components of compliance programs. An effective OFAC compliance program should include the following:

- Developing internal controls for OFAC compliance, including screenings of customers and transactions, as appropriate, against the following lists collectively referred to as "Sanctions listings":
    - OFAC Specially Designated Nationals (SDN) and Blocked Persons List
    - Country and List-Based Sanctions
    - Non-SDN Palestinian Council (NS-PLC) list
- Blocking/rejecting transactions
- Reporting blocked or rejected transactions
- Designating an individual to be responsible for OFAC compliance
- Developing and implementing written OFAC policies and procedures
- Conducting an OFAC risk assessment
- Conducting comprehensive and ongoing training
- Designing and maintaining effective monitoring, including timely updates to the OFAC filter
- Periodic, independent testing of the program's effectiveness (there is no single compliance program suitable for every institution)

561. Does OFAC offer any guidance on its expectations for specific industries?

OFAC has promulgated specific guidance for the following industries/businesses:

- Financial community (e.g., banks)
- Securities industry
- Money services businesses (MSBs)
- Exporters and importers
- Insurance industry
- Nongovernmental organizations (NGOs)/Nonprofits
- Credit reporting businesses
- Corporate registration businesses

562. Should other lists beyond the SDN, country and list-based sanctions and the NS-PLC list be incorporated into an OFAC compliance program?

Financial institutions should incorporate the List of Foreign Financial Institutions Subject to Part 561 (the Part 561 List) that includes entities which have violated Iranian Financial Sanctions Regulations (IFSR). U.S. financial institutions are prohibited from opening or maintaining a correspondent or payable-through account for any foreign financial institutions on the Part 561 List. Foreign-owned financial institutions and/or domestic financial institutions that operate internationally will likely also want to incorporate lists from other jurisdictions in which they are domiciled or do business.

There are several sanctions lists maintained by other countries that can be considered for inclusion. Additionally, U.S. government agencies, such as the U.S. Bureau of Industry and Security (BIS), the Department of Commerce, the Department of Labor and the State Department, have independent prohibitions on transactions with certain individuals or entities beyond those included in OFAC Sanctions listings. For further guidance, please refer to Other U.S. and International Government Sanctions Programs section.

563. What enforcement authority does OFAC have?

OFAC can impose penalties against any organization or entity that conducts or facilitates transactions with those associated with individuals/entities on the OFAC Sanctions listings.

564. Who is responsible for examining financial institutions for compliance with OFAC Sanctions?

For regulated financial institutions, an institution's primary regulator is responsible for examining OFAC compliance. Other types of organizations may not be subject to regular OFAC examinations by a regulatory body, but are nonetheless at risk for sanction by OFAC for noncompliance.

565. What is an OFAC risk assessment?

An OFAC risk assessment is a systematic method of qualifying and quantifying OFAC risks to ensure an OFAC compliance program mitigates potential risks identified. For additional guidance on OFAC risk assessments, please refer to the Risk Assessments section.

566. What is a reasonable time for compliance with updates to the OFAC Sanctions listings?

OFAC can update Sanctions listings at any time and expects compliance as soon as a name is added to the Sanctions listings. An institution must weigh its risk and determine the appropriate time frame for ensuring that updates are processed. Some institutions process updates the same day, while others, in accordance with their risk profile, may process updates within a week or a few weeks from the time Sanctions listings are updated. Documentation of updates should be maintained by the responsible department.

567. How can an institution stay up-to-date on the changes to the OFAC Sanctions listings?

OFAC offers real-time e-mail notifications of any changes to a sanctions program or the Specially Designated Nationals and Blocked Persons (SDN) list. Many vendors also provide automatic notifications and updates as part of their interdiction software package.

568. Does the Dodd-Frank Act include any Sanction requirements?

The Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA) does not include Sanction requirements per se, but it does require that a company publicly disclose if it uses conflict minerals that originated in the Democratic Republic of the Congo or adjoining countries (collectively, the covered countries) that are "necessary to the functionality or production" of a product manufactured or contracted to be manufactured by the company. The purchase of these so-called conflict minerals allegedly benefits armed rebels in these countries and the required disclosure is expected to put pressure on companies to disassociate with the covered countries.

The SEC rule implementing this provision of the Dodd-Frank Act requires both domestic and foreign issuers that file with the SEC to publicly disclose their use of conflict minerals on a new form, Form SD, which must be filed by May 31, 2014 and annually on May 31 thereafter. In order to file this disclosure, a company will need to exercise due diligence to determine whether any of the minerals used by the company originated in the covered countries. The regulation does provide for a two-year transition (four years for smaller companies) period in which a company may consider its products "DRC conflict undeterminable" if it is unable to determine the source of minerals used. "False or misleading statement" in the form will subject a company to liability under Section 18 of the Securities Exchange Act.

569. How will the new obligations of the "Customer Due Diligence Requirements for Financial Institutions" rule, if enacted, impact OFAC and sanctions programs?

Currently, covered financial institutions are required to obtain beneficial ownership in the following situations as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

The ANPR could categorically require all financial institutions subject to AML Program requirements to identify, and in some instances, verify the identity of beneficial ownership of all of their account holders. The ANPR would also impact the OFAC and sanctions program of financial institutions, as beneficial owners would be subject to screening against required Sanctions listings to the extent that financial institutions are not screening beneficial owners today.

For further guidance on the proposed rule, please refer to the Beneficial Ownership section. For further guidance on due diligence requirements for private banking and correspondent banking customers, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Private Banking and Correspondent Banking.

570. What resources has OFAC provided to the public?

Among the resources provided by OFAC are the following:

- **Sanctions Programs**
  - **Specially Designated Nationals List –** OFAC publishes the current SDN list and archives the changes made to the SDN list on its website.
  - **Country- and Regime-Based Programs –** OFAC publishes current country- and regime-based lists, including, but not limited to, the following:
    - Balkans-related Sanctions (BALKANS)
    - Belarus Sanctions (BELARUS)
    - Burma Sanctions (BURMA)
    - Côte d'Ivoire (Ivory Coast)-related Sanctions (COTED)
    - Counter Narcotics Trafficking Sanctions ([SDNT], [SDNTK])
    - Counter Terrorism Sanctions ([SDGT], [FTO], [SDT])
    - Cuba Sanctions (CUBA)
    - Democratic Republic of the Congo-related Sanctions (DRCONGO)
    - Iran Sanctions ([IRAN], [IRGC], [IFSR], [IRAN-HR],[BPI-IRAN-HR],[HRIT])
    - Iraq-related Sanctions ([IRAQ], [IRAQ2])
    - Former Liberian Regime of Charles Taylor Sanctions (LIBERIA)
    - Lebanon-related Sanctions (LEBANON)
    - Nonproliferation Sanctions (NPWMD)
    - North Korea Sanctions (DPRK)
    - Somalia Sanctions (SOMALIA)
    - Sudan Sanctions ([SUDAN], [DARFUR])
    - Syria Sanctions (SYRIA)
    - Zimbabwe Sanctions (ZIMBABWE)
  - **Non-SDN Palestinian Legislative Council (PLC) List –** OFAC publishes the current PLC list and archives the changes made to the PLC list on its website.
  - **List of Foreign Financial Institutions Subject to Part 561** (the Part 561 List) – OFAC publishes the current Part 561 List on its website, which includes entities who have violated Iranian Financial Sanctions Regulations (IFSR).
- **Overview of Sanctions Programs** – OFAC has published separate overview documents for the List-Based Sanctions (e.g., Anti-Terrorism, Nonproliferation, Narcotics Trafficking) and the Country Sanctions Programs (e.g., Cuba, Iran, North Korea, Sudan, Syria, Zimbabwe).
- **OFAC Information by Industry Groups** – OFAC compiles guidance by industry groups (e.g., financial sector, money services businesses [MSBs], insurance industry, exporting and importing). These sections include items such as links to the relevant sections of the compiled FAQs, articles and industry brochures.
- **Frequently Asked Questions (FAQs)** – OFAC's own FAQ list, regarding frequently asked questions it has received and answers to those questions on topics such as the SDN list, licensing, technology from multiple industries (e.g., financial institutions, insurance, importers/exporters) and country sanctions programs.

- **OFAC Risk Matrix** – A matrix that assists institutions with rating (low, medium, high) areas of their own OFAC programs to ensure effective risk management. They have been produced for different sectors (e.g., financial institutions, charitable organizations, securities sector).
- **Guidance on OFAC Licensing Policy** – Guidance on OFAC licensing, including "Guidance on the Release of Limited Amounts of Blocked Funds for Payment of Legal Fees and Costs Incurred in Challenging the Blocking of U.S. Persons in Administrative or Civil Proceedings" and "Guidance on Entities Owned by Persons Whose Property and Interests in Property Are Blocked."
- **OFAC Recent Actions** – OFAC maintains a list of current actions that it has made, such as updates to the SDN list or sanctions programs, and notifications of the release of certain reports.
- **Civil Penalties Actions and Enforcement Information** – An archive of the published civil penalties, enforcement actions and settlements taken against entities dating back to 2003.
- **Economic Sanctions Enforcement Guidelines** – Enforcement guidance for persons subject to the requirements of U.S. sanctions statutes, executive orders and regulations.
- **Memorandum of Understanding (MOU) between OFAC and the Federal Reserve, FDIC, NCUA and OCC** – An MOU that explains the relationship between OFAC and the banking regulators.
- **Interpretive Rulings on OFAC Policy** – An archive of published rulings and interpretations to clarify OFAC policy.
- **Terrorist Assets Report (TAR)** – An annual report submitted to Congress concerning the nature and extent of assets held in the United States by terrorist-supporting countries and organizations.

All guidance is available on OFAC's website: www.ustreas.gov/offices/enforcement/ofac.

Specially Designated Nationals and Blocked Persons List

571. What is the Specially Designated Nationals and Blocked Persons list?

As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, the governments of targeted countries. The Specially Designated Nationals and Blocked Persons (SDN) list also identifies individuals, groups and entities, such as terrorists and narcotics traffickers, designated under programs that are not country-specific. Their assets are blocked and U.S. persons generally are prohibited from dealing with them.

Although this list allows U.S. persons to know they are prohibited from dealing with persons or entities on the list, it is not comprehensive, as it does not include, for example, the names of all individuals in Cuba (who are subject to blocking, except under limited exceptions).

572. What information is provided on the SDN list?

The SDN list provides the following information, if known:

- Name(s) (including variations in spelling)
- Alias(es)
- Address(es)
- Website address(es)
- E-mail address(es)
- Nationality(ies)
- Citizenship(s)
- Place of birth(s) (POB)
- Date of birth(s) (DOB)

- Information provided on identification(s)/documentation (e.g., cédula number, passport number, expiration date, date of issuance, country of issuance, business registration number)
- Title(s)/position(s) (e.g., former Minister of Higher Education and Research, Republican Guard Secretary)
- Customer type (i.e., individual; if not stated, assumed as business/entity type)
- Reason(s) for inclusion on SDN list (e.g., SDNT, SDGT, SDNTK, Liberia, Iraq)

The reasons individuals/entities are added to the SDN list are as follows:

- Specially Designated Terrorists (SDT)
- Specially Designated Global Terrorists (SDGT)
- Foreign Terrorist Organizations (FTO)
- Specially Designated Narcotics Traffickers (SDNT)
- Specially Designated Narcotics Traffickers – Kingpins (SDNTK)
- Nonproliferation of Weapons of Mass Destruction (NPWMD)

This information can be used to assist in investigating potential matches with the SDN and other list-based sanctions programs.

573. Are all SDN designees foreign?

No. SDN designees consist of many nationalities, including U.S. individuals and entities, although most are foreign.

574. How frequently are the OFAC Sanctions listings updated?

Prior to September 11, 2001, updates to the Sanctions listings were relatively sporadic. The infrequent additions lulled many institutions, particularly smaller ones, into thinking that compliance responsibilities were easily manageable and did not require automated tools. In the current environment, however, names are added and removed to the Sanctions listings with greater frequency. As soon as a name is added to the Sanctions listings, OFAC expects compliance.

575. How can institutions ensure they are using the most current SDN List to screen customers and transactions?

Institutions can register with OFAC to receive a notification, via e-mail, whenever the SDN list has been updated. Additionally, many technology service providers are providing automated notifications to their users when updated lists have been incorporated into the interdiction software. When notifications are received, institutions should test their interdiction software to ensure the updated SDN list is being used to screen customers and transactions.

576. Can an individual/entity be listed on multiple sanctions programs?

Yes. An individual/entity can appear on multiple sanctions programs.

577. What is the process for adding a name to the SDN list?

The process of adding a name to the SDN list involves evidence being vetted through several agencies prior to OFAC's final designation on the SDN list. This information is labeled classified. In some cases, the designations are made through executive orders directly from the U.S. president.

578. If an SDN or list-based sanctions program designee dies, is that individual removed from the list?

No. Even though the individual is deceased, his or her assets remain blocked until OFAC sees fit to unblock them. For example, if an SDN designee dies, the individual's assets should not be released to beneficiaries until further guidance is received from OFAC.

579. What does a positive "hit" mean?

A positive "hit" is defined as a confirmed true match to the OFAC Sanctions listings.

580. What action must institutions take if a positive "hit" is identified on the SDN list?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the Investigating Potential Matches and Reporting Requirements sections.

Country- and Regime-Based Sanctions Programs

581. What are the Country- and Regime-Based Sanctions Programs administered by OFAC?

OFAC administers a number of U.S. economic sanctions, ranging from comprehensive bans against conducting activity with all individuals/entities from a specified country (e.g., there is a broad ban on Cuban transactions with only limited exceptions) or jurisdiction to limited regime-based bans that prohibit transactions/trade with a particular individual/entity/regime or activity (e.g., diamond-related activity).

For a list of country- and regime-based sanctions, refer to OFAC's website: www.treas.gov/offices/enforcement/ofac.

Non-Specially Designated Nationals Palestinian Council List

582. What is the Non-SDN Palestinian Council list?

OFAC published the Non-Specially Designated Nationals Palestinian Council (NS-PLC) list in April 2006.The NS-PLC list is composed of members of the Palestinian Legislative Council who were elected on the party slate of Hamas or other designated foreign terrorist organizations.

583. Is the NS-PLC list part of the SDN list?

No. The NS-PLC list is separate from the SDN list, and the individuals included on the NS-PLC list are not necessarily listed on the SDN list.

584. Who is required to screen customers/transactions against the NS-PLC list?

As with the SDN and country- and regime-based sanctions programs, these requirements apply to U.S. persons. "U.S. persons" is defined as U.S. citizens and permanent resident aliens, regardless of where they are located in the world; all persons and entities within the United States; and all U.S.-incorporated entities and their foreign branches.

585. What action must institutions take if a positive "hit" is identified for the NS-PLC list?

The U.S. Department of the Treasury has authorized U.S. financial institutions to reject transactions with individuals on the NS-PLC list who are not included on the SDN list. A Rejected Transaction report must be filed with OFAC within 10 business days.

In the case where an NS-PLC designee is also an SDN designee, transactions must be blocked. For additional guidance, please refer to the Investigating Potential Matches and Reporting Requirements sections.

U-Turn Payments

586. What is an Iranian "U-Turn payment"?

For many years, OFAC, under the Iranian Sanctions Regulations, has prohibited U.S. financial institutions from directly sending funds to Iran, but allowed U-Turn payments. A "U-Turn payment" is a payment originating at a non-U.S. bank going through a U.S. bank destined for a payment to another non-U.S. bank, provided the payments do not directly credit or debit an Iranian account (e.g., an account of a person/business in Iran or of the Government of Iran). The originator, beneficiary, originating bank or beneficiary bank could all be Iranian as long as there are third-country banks on both sides of the transaction.

587. What is the purpose of a U-Turn payment?

A U-Turn payment is designed to allow international financial institutions, in the wake of heavy economic sanctions against Iran, to still clear payments through their U.S. correspondent accounts under limited circumstances.

588. Are U-Turn payments allowed?

No. As of November 10, 2008, U-Turn payments are no longer allowed.

Iranian Sanctions Overview

Overview

589. What are the major U.S. government sanctions programs affecting Iran?

The U.S. government has imposed numerous sanctions on Iran including those mandated by the following statutes and executive orders which are listed in chronological order:

- International Emergency Economic Powers Act (IEEPA) (1977)
- Executive Order 12170 – Blocking Iranian Government Property (1979)
- Executive Order 12205 – Prohibiting Certain Transactions With Iran (1980)
- Executive Order 12211 – Prohibiting Certain Transactions With Iran (1981)
- Executive Order 12276 – Direction Relating to Establishment of Escrow Accounts (1981)
- Executive Order 12277 – Direction To Transfer Iranian Government Assets (1981)
- Executive Order 12278 – Direction To Transfer Iranian Government Assets Overseas (1981)
- Executive Order 12279 – Direction To Transfer Iranian Government Assets Held By Domestic Banks (1981)
- Executive Order 12280 – Direction To Transfer Iranian Government Financial Assets Held By Non-Banking Institutions (1981)
- Executive Order 12281 – Direction To Transfer Certain Iranian Government Assets (1981)
- Executive Order 12282 – Revocation of Prohibitions Against Transactions Involving Iran (1981)
- Executive Order 12283 – Non-Prosecution of Claims of Hostages and for Actions at the United States Embassy and Elsewhere (1981)
- Executive Order 12284 – Restrictions on the Transfer of Property of the Former Shah of Iran (1981)
- Executive Order 12294 – Suspension of Litigation Against Iran (1981)
- Section 505 of the International Security and Development Cooperation Act of 1985 (ISDCA)
- Executive Order 12613 – Prohibiting Imports from Iran (1987)
- Executive Order 12735 – Chemical and Biological Weapons Proliferation (1990)
- Executive Order 12851 – Administration of Proliferation of Sanctions, Middle East Arms Control, and Related Congressional Reporting Responsibilities (1993)
- Executive Order 12938 – Proliferation of Weapons of Mass Destruction (1994)
- Executive Order 12947 – Prohibiting Transactions with Terrorists Who Threaten to Disrupt the Middle East Process (1995)
- Executive Order 12957 – Prohibiting Certain Transactions with Respect to the Development of Iranian Petroleum Resources (1995)
- Executive Order 12959 – Prohibiting Certain Transactions with Respect to Iran (1995)

- Iran-Libya Sanctions Act (1995)
- Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA)
- Iran Sanctions Act of 1996 (ISA)
- Executive Order 13059 – Prohibiting Certain Transactions with Respect to Iran (1997)
- Executive Order 13099 - Prohibiting Transactions with Terrorists Who Threaten to Disrupt the Middle East Process (1998)
- Trade Sanctions Reform and Export Enhancement Act of 2000 (TSRA)
- Executive Order 13224 – Blocking Property and Prohibiting Transactions with Persons Who Commit, Threat to Commit, or Support Terrorism (2001)
- Executive Order 13382 - Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters (2005)
- Executive Order 13553 - Blocking Property of Certain Persons With Respect to Serious Human Rights Abuses By The Government of Iran and Taking Certain Other Actions (2010)
- The Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA)
- Executive Order 13574 – Authorizing the Implementation of Certain Sanctions Set Forth in the Iran Sanctions Act of 1996 (2011)
- Executive Order 13590 – Authorizing the Imposition of Certain Sanctions with Respect to the Provision of Goods, Services, Technology or Support for Iran's Energy and Petrochemical Sectors (2011)
- Executive Order 13599 – Blocking Property of the Government of Iran and Iranian Financial Institutions (2012)
- Executive Order 13606 – Blocking the Property and Suspending Entry Into the United States of Certain Persons With Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology (2012) (GHRAVITY E.O.)
- Executive Order 13608 – Prohibiting Certain Transactions with and Suspending Entry into the United States of Foreign Sanctions Evaders with Respect to Iran and Syria (2012)
- Executive Order 13622 – Authorizing Additional Sanctions with Respect to Iran (2012)
- Executive Order 13628 - Authorizing the Implementation of Certain Sanctions Set Forth in the Iran Threat Reduction and Syria Human Rights Act of 2012 and Additional Sanctions with Respect to Iran (2012)
- Section 1245 of the National Defense Authorization Act for Fiscal Year 2012 (NDAA)
- H.R. 1905 – Iran Threat Reduction and Syria Human Rights Act of 2012 (ITRSHRA)

Following are the regulations that implement Iranian sanctions:

- **31 CFR Part 535 – Iranian Assets Control Regulations** – Regulations that governed the 1979 seizure of $12 billion in Iranian Government bank deposits and securities held by overseas branches of U.S. banks. The asset freeze was later expanded to a full trade embargo which remained into effect until 1981. Part 535 has since been substantially modified in scope by subsequent laws and regulations.
- **31 CFR Part 560 - Iranian Transaction and Sanctions Regulations (ITSR)** – General Iran sanctions program administered by the Office of Foreign Assets Control (OFAC) along with unexpired provisions of Part 535.
- **31 CFR Part 561 – Iranian Financial Sanctions Regulations (IFSR)** – Implementing regulations of Sections 104(c) and 104(d) of CISADA.
- **31 CFR Part 562 – Iranian Human Rights Abuses Sanctions Regulations** – Implementing regulations of laws addressing human rights violations by Iran (e.g., ITRSHRA, Executive Order 13553)
- **31 CFR Part 1060 – Comprehensive Iran Sanctions, Accountability, and Divestment Reporting Requirements** – FinCEN regulation implementing Section 104(e) of CISADA.

Additionally, the U.S. Treasury Department issued a notice of proposed rulemaking on November 28, 2011 designating Iran as a jurisdiction of primary money laundering concern pursuant to Section 311 – Special Measures.

Major provisions of CISADA, NDAA, ITRSHRA and select executive orders are summarized below.

590. What are the major U.S. government sanctions programs affecting Syria?

The U.S. government has imposed sanctions on Iran including those mandated by the following statutes and executive orders which are listed in chronological order:

- Section 5 of the United Nations Participation Act (UNPA) (1945)
- International Emergency Economic Powers Act (IEEPA) (1977)
- Executive Order 13224 – Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism (2001)
- Executive Order 13315 – Blocking Property of the Former Iraqi Regime, Its Senior Officials and Their Family Members, and Taking Certain Other Actions (2003)
- Executive Order 13382 – Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters (2005)
- Executive Order 13338 – Blocking Property of Certain Persons and Prohibiting the Export of Certain Goods to Syria (2004)
- Executive Order 13399 - Blocking Property of Additional Persons in Connection With the National Emergency With Respect to Syria (2006)
- Executive Order 13441 - Blocking Property of Persons Undermining the Sovereignty of Lebanon or Its Democratic Processes and Institutions (2007)
- Executive Order 13460 - Blocking Property of Additional Persons in Connection With the National Emergency With Respect to Syria (2008)
- Executive Order 13338 - Blocking Property of Certain Persons and Prohibiting the Export of Certain Goods to Syria (2004)
- Syria Accountability Act and Lebanese Sovereignty Restoration Act (SAA) of 2004
- Executive Order 13572 --Blocking Property of Certain Persons with Respect to Human Rights Abuses in Syria (2011)
- Executive Order 13573 - Blocking Property Of Senior Officials Of The Government Of Syria (2011)
- Executive Order 13582 - Blocking Property of the Government of Syria and Prohibiting Certain Transactions with Respect to Syria (2011)
- Executive Order 13606 – Blocking the Property and Suspending Entry Into the United States of Certain Persons With Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology (2012) (GHRAVITY E.O.)
- Executive Order 13608 - Prohibiting Certain Transactions With and Suspending Entry Into the United States of Foreign Sanctions Evaders With Respect to Iran and Syria (2012)
- Iran Threat Reduction and Syria Human Rights Act in 20112 (ITRSHA)

Syrian sanctions are implemented under 31 CFR Parts 542 - Syrian Sanctions Regulations.

Additionally, on March 9, 2006, the U.S. Treasury Department designated the Commercial Bank of Syria, including its subsidiaries, Syrian Lebanese Commercial Bank, as financial institutions primary money laundering concern pursuant to Section 311 – Special Measures of the USA PATRIOT Act.

591. Who is responsible for administering Iranian and Syrian sanctions and regulations?

The Department of the Treasury (OFAC) has primary responsibility for implementing the economic sanctions contained in the ITSR,

The State Department is the agency primarily responsible for implementing the provisions of CISADA and ITRSHA, including the designation of entities in the energy, shipping and transportation sectors.

The Bureau of Industry and Security (BIS) within the Department of Commerce administers regulations pertaining to the export of goods and technology to Iran under the Export Administration Regulations, which are authorized by IEEPA.

OFAC has issued a few general licenses authorizing certain categories of transactions, and may issue specific licenses on a case-by-case basis. For further guidance, please refer to the Licensing section within the Office of Foreign Assets Control.

592. Where can one find a list of designated entities?

Designations are maintained in the appendices of applicable Iranian regulations, on lists administered by OFAC, or both. Examples of Iranian sanction designations and lists include, but are not limited to the following:

- Specially Designated Nationals (SDN) List
    - Persons designated under Executive Order 13606 (GHRAVITY E.O.) appear on the SDN list bearing the **Human Rights Information Technology [HRIT]** tag.
    - Persons designated under E.O. 13599 appear on the SDN List bearing the [IRAN] tag.
    - **Iran's Islamic Revolutionary Guard Corps (IRGC),** its agents and affiliates designated under Section 104(d) of CISADA, IEEPA and IFSR appear on the SDN list bearing the [IRGC] tag.
- **List of Foreign Financial Institutions Subject to Part 561 (the Part 561 List)** – Foreign financial institutions Entities that are deemed to have violated Iranian Financial Sanctions Regulations (IFSR) under CISADA and NDAA.

593. Are there exemptions from the Iranian sanctions regulations?

Yes. There are certain categories of products and services such as food, medicine and medical devices that are exempt from Iranian sanctions and regulations. OFAC and BIS can issue general licenses authorizing the performance of certain categories of transactions, as well as specific licenses, on a case-by-case basis, that would otherwise be prohibited under Iranian sanctions and regulations. For further guidance, please refer to Licensing section within OFAC.

The U.S. President also has the authority to waive the imposition of sanctions.

594. Are existing contracts and licenses still valid after the issuance of subsequent Iranian and Syrian sanctions?

Generally, existing contracts that cover prohibited activities or involve designated individuals or entities will no longer be legitimate, unless a valid license has been issued. Persons who have been issued licenses involving persons designated under Iranian and Syrian sanctions should check with the issuing agency regarding the ongoing validity of their licenses.

595. What types of actions are required upon identifying a designated entity or prohibited transaction?

Each sanction program outlines specific actions that must be taken upon identifying a designated entity or prohibited transaction. These actions include, but are not limited to the following:

- Blocking assets;
- Rejecting transactions;
- Reporting of blocked and rejected transactions; or
- Prohibiting the opening or maintenance of correspondent accounts and payable-through accounts.
- Taking appropriate actions to not provide a prohibited service or transaction (in addition to blocking assets as required).

For further guidance, blocking, rejecting and reporting transactions, please refer to the sections: Blocking and Rejecting Transactions and Reporting Requirements within OFAC. Details of recent Iranian sanctions laws and regulations are detailed further below.

596. Have any entities been penalized for violations of Iranian sanctions?

Yes. On May 24, 2011, the U.S. Department of State sanctioned seven companies for violations under the Iran Sanctions Act (ISA) of 1996, as amended by the CISADA, for activities in support of Iran's energy section, specifically for refined-petroleum related activities. These companies were

- Petrochemical Commercial Company International (PCCI) (Jersey/Iran);
- Royal Oyster Group (UAE);
- Speedy Ship aka Sepahan Oil Company (UAE/Iran);
- Tanker Pacific (Singapore);
- Ofer Brothers Group (Israel);
- Associated Shipbroking (Monaco); and
- Petróleos de Venezuela (PDVSA) (Venezuela).

On July 31, 2012, the U.S. Department of Treasury imposed sanctions under CISADA against the Bank of Kunlun in China and the Elaf Islamic Bank in Iraq. Specifically, these two banks violated Section 561.201 of IFSR, which implemented Section 104 of CISADA, which prohibits or imposes strict conditions with respect to correspondent accounts or payable-through accounts of certain foreign financial institutions that engage in activities that support the efforts of the Government of Iran or the IRGC and its agents or affiliates. Both banks and their aliases were added to the List of Foreign Financial Institutions Subject to Part 561 (the Part 561 List).

Comprehensive Iran Sanctions, Accountability and Divestment Act (CISADA) in 2010 and the Iran Threat Reduction and Syria Human Rights Act in 2012

597. What additional sanctions did the United States impose on Iran due to the passage of the Comprehensive Iran Sanctions, Accountability and Divestment Act (CISADA) in 2010 and the Iran Threat Reduction and Syria Human Rights Act in 2012?

CISADA and ITRSHA imposed new economic penalties designed to put additional pressures on Iran to end its nuclear weapons program. The law includes:

- Expanded scope of persons and the type of activities that may be subject to sanctions to include:
    - Investment (over certain threshold amounts) in Iran's development of petroleum resources;
    - Sales of goods, services or technology (over certain threshold amounts) that support Iran's ability to produce refined petroleum
    - Exporting Iran's refined petroleum products (over certain threshold amounts)
    - Participation in joint ventures with the Government of Iran to develop petroleum resources outside Iran
    - Insuring vessels used to transport Iranian crude oil
    - Participation in joint ventures with the Government of Iran related to uranium mining, production or transportation
- Expanded type of sanctions that may be imposed to include:
    - Denial of foreign exchange transactions subject to U.S. jurisdiction that involve sanctioned entities
    - Prohibition on transfers of credit or payments between, by, through or to financial institutions subject to U.S. jurisdiction and that involve any interest of sanctioned entities
    - Prohibition on transactions (e.g., acquiring, holding, withholding, using, transferring, withdrawing, transporting, importing or exporting) or exercising rights, powers, etc. with respect to property subject to U.S. jurisdiction in which a sanctioned entity has an interest
    - Ban on investment in equity or debt of a sanctioned person
    - Exclusion of corporate officers from the United States
    - Sanctions on principal executive officers of sanctioned company
- New restrictions for financial institutions barring U.S. banks from engaging in financial transactions with foreign banks doing business in Iran or facilitating Iran's nuclear program or support for terrorism

- Mandatory investigations into possible sanctionable conduct upon the receipt of “creditable evidence” subject to certain waiver provisions
- Requiring new regulations to prohibit or impose strict conditions on the holding of a correspondent or payable through account in the United States by foreign financial institutions engaged in specified activities, such as activities that facilitate the efforts of the Government of Iran to acquire or develop weapons of mass destruction or delivery for such records or to provide support for organizations designated as foreign terrorist organizations or support for acts of international terrorism; for facilitating efforts by Iranian financial institutions to carry out such activities
- Requirement for Treasury to promulgate regulations to prohibit any entity owned or controlled by a U.S. financial institution from knowingly transacting with or benefitting such a foreign financial institution or covered individual
- Authorization/safe harbor for state and local governments to more easily divest themselves of or prohibit any investments of public funds in companies that engage in certain business with Iran
- Certification by U.S. government contractors that neither they, nor any entity they own or control, engage in any activity subject to Iran sanctions
- Codification of long-standing U.S. Executive Orders prohibiting U.S. persons, wherever located, from doing business with the Government of Iran and any entities it owns or controls

598. Since most commerce between the United States and Iran is already prohibited under existing sanction programs, what more is really gained by CISADA and ITRSHA?

By targeting foreign firms that do business with Iran and restricting or denying them access, directly or indirectly, to the U.S. financial system, CISADA and ITRSHA seek to bring pressure on these foreign firms to cease their business operations with Iran.

599. Are CISADA and ITRSHA unilateral actions on the part of the United States?

Yes, the specific sanctions in these statutes that authorize the imposition of sanctions on foreign are unique to the United States. However, US policy towards Iran is broadly aligned with other countries as reflected in United Nations Security Council Resolutions. Canada, Australia and the European Union have all adopted their own sanctions on Iran, which include prohibiting exports of certain goods and technology, prohibiting transactions, blocking assets of Iranian financial institutions and other designated entities, and prohibiting the transport of Iranian oil.

600. How will CISADA and ITRSHA affect foreign companies?

CISADA requires that sanctions be imposed on foreign persons who:

- Knowingly invest more than $20 million (including by increments of at least $5 million within 12 months) in Iran’s development of petroleum resources;
- Sell, lease or provide goods, services, technology, information or support worth at least $1 million (or, during a 12-month period, have an aggregate value of $5 million or more) that could directly and significantly facilitate the maintenance or expansion of Iran’s domestic production of refined petroleum products;
- Selling or providing Iran with refined petroleum products with a fair market value of $1 million or ($5 million during a 12-month period); or
- Providing goods or services that could directly and significantly contribute to the enhancement of Iran’s ability to import refined petroleum products, including insuring, reinsuring, financing or brokering such transactions with a fair market value of $1 million (or, during a 12-month period, have an aggregate value of $5 million or more)

CISADA prescribes additional sanctions on persons who aid Iran’s development of nuclear capabilities, and on U.S. financial institutions that engage in financial transactions with foreign banks doing business with Iran’s Islamic Revolutionary Guard Corps (IRGC) or sanctioned Iranian banks, or facilitate Iran’s illicit nuclear program or its support for terrorism.

Further, ITRSHA requires that sanctions be imposed on persons who:

- Knowingly participate in a joint venture with respect to the development of petroleum resources outside Iran if the Government of Iran is a substantial partner or investor or Iran could receive through a direct operational role in the joint venture technological knowledge that could directly and significantly contribute to the enhancement of Iran ability to develop petroleum resources in Iran.

- Knowingly sells, leases, or provides Iran goods, services or technology with a fair market value of $1 million (or $5 million during a 12-month period) that support or could directly and significantly contribute to the maintenance or expansion of Iran's domestic production of petrochemical products.
- Owns, operates, controls or insures a vessel that was used to transport crude oil from Iran or such a person who knows that the vessel is being operated to conceal the transport of Iran origin crude oil or refined petroleum or to conceal the ownership, operation or control of the vessel by the Government of Iran, the National Iranian Oil Corporation (NIOC), the Islamic Republic of Iran Shipping Line (IRISL) or any other designated Iranian entity
- Exports, transfers or facilitates the transshipment by others of goods, services, technology or other items that would contribute materially to Iran's ability to acquire or develop chemical, biological or nuclear weapons
- Participates in a joint venture with the Government or Iran or any Iranian entity involving any activity relating to the mining, production or transportation of uranium

601. How does CISADA define "person"?

CISADA defines "person" as a natural person, business enterprise, government entity operating as a business enterprise, financial institution, insurer, underwriter, guarantor or any other business organization. This definition also includes parent companies and affiliates of sanctioned persons.

602. CISADA requires the imposition of sanctions when a person "knowingly" invests or takes certain other actions. What does "knowingly" mean in this context?

"Knowingly" in this context means actual knowledge or constructive knowledge (i.e., the person should have known).

603. What sanctions will be imposed on foreign companies that violate the CISADA and ITRSHA sanctions?

CISADA provided that nine possible sanctions may be imposed for violating of the sanctions:

- Prohibition within U.S. jurisdiction of foreign-exchange transactions in which a sanctioned person has any interest
- Prohibition within U.S. jurisdiction of payments and other transactions that involve any interest of a sanctioned person
- The blocking of the property (freezing of the assets) within U.S. jurisdiction of a sanctioned person
- Denial of U.S. Export-Import Bank loans or credit facilities for U.S. exports to the sanctioned person
- Denial of licenses for the U.S. export of military or militarily useful technology
- Denial of U.S. bank loans exceeding $10 million in one year
- If the sanctioned person is a financial institution, a prohibition on its service as a primary dealer in U.S. government bonds and/or a prohibition on its serving as a repository for U.S. government funds
- Prohibition on U.S. government procurement from the sanctioned person
- Restriction on imports into the United States from the sanctioned person

In addition, ITRSHA added three new sanctions to the list:

- Ban on investment in equity or debt of a sanctioned person
- Exclusion of corporate officers from the United States
- Sanctions on principal executive officers of sanctioned company

CISADA required that at least three of the above sanctions be imposed when there is a finding that a person has violated sanctions provision set forth in CISADA. ITRSHA strengthened the provision to require the imposition of at least five of the above sanctions. The U.S. president, however, does have the authority to waive the imposition of sanctions in certain circumstances.

604. What sanctions will be imposed on persons who violate the provisions of CISADA related to the transfer of nuclear technology?

CISADA prohibits the issuance of export licenses to the country having primary jurisdiction over the person engaging in the sanctionable activity. The U.S. president may waive the sanctions with a certification to Congress that the relevant country did not know of the sanctionable activity or is taking steps to prevent it and to penalize the offender.

605. Whom is targeted by the United States within Syria with the passage ITRSHA?

ITRSHA imposed sanctions against Syria with respect to persons who:

- Are responsible for or complicit in human rights abuses committed against citizens of Syria or their family members;
- Transfer goods or technologies to Syria that are likely to be used to commit human rights abuses; and
- Engage in censorship or other forms of repression in Syria.

Impact on Financial Institutions

606. What is the impact of CISADA on U.S. financial institutions?

CISADA requires the U.S. Treasury Department to issue regulations restricting or prohibiting the opening or maintenance of correspondent or payable through accounts by a foreign financial institution that:

- Facilitates the efforts of the Government of Iran, the Islamic Revolutionary Guard Corps (IRGC) or any of its agents or affiliates to acquire weapons of mass destruction or provide support to foreign terrorist organizations
- Facilitates the activities of persons subject to financial sanctions under the UN Security Council Iranian resolution
- Engages in money laundering related to the above activities
- Facilitates significant transaction(s) or provides financial services to the IRGC or any of its agents or affiliates or to financial institutions subject to U.S. blocking requirements

CISADA also requires U.S. financial institutions that maintain correspondent or payable through accounts in the United States for a foreign financial institution to do one or more of the following:

- Audit activities of the foreign financial institutions for which such accounts are made for indication that they are engaging in any prohibited activity;
- Report any such activity identified to the Department of the Treasury;
- Establish due diligence procedures, policies and controls that are reasonably designed to detect whether foreign financial institutions knowingly engage in prohibited activities; and
- Certify, to the best of their knowledge, that the foreign financial institutions with which they are maintaining accounts are not engaging in such activities.

For additional guidance on correspondent banking customers and payable through accounts, please refer to sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Customers, Correspondent Banking and Payable Through Accounts.

607. How does CISADA define “financial institution” and “U.S. financial institution”?

The definition of “financial institution” is broad and includes any entity engaged in the business of accepting deposits; making, granting, transferring, holding or brokering loans or credits; purchasing or selling foreign exchange, securities, commodity futures or options; or procuring purchasers and sellers thereof, as principal or agent. It includes but is not limited to:

- Depository institutions
- Banks
- Savings banks
- Money services businesses (MSB)

- Trust companies
- Securities brokers and dealers
- Commodity futures and options brokers and dealers
- Forward contract and foreign exchange merchants
- Securities and commodities exchanges
- Clearing corporations
- Investment companies
- Employee benefit plans
- Holding companies, affiliates or subsidiaries of any of the foregoing

For purposes of the definition of "U.S. financial institution," the term also includes those branches, offices and agencies of a foreign financial institution located in the United States, but not such institution's foreign branches, offices or agencies.

608. How does CISADA define "foreign financial institution"?

CISADA defines "foreign financial institution" to include foreign depository institutions, banks, savings banks, money service businesses, trust companies, securities brokers and dealers, commodities exchanges, clearing corporations, investment companies, employee benefit plans, and holding companies, affiliates, or subsidiaries of any of these entities.

609. Does CISADA apply to persons or entities who own, directly or indirectly, the aforementioned financial institutions?

Yes, to the extent that a person whose property is blocked owns, directly or indirectly, 50 percent or greater interest in property of another entity, the property and interests in the property of that entity will also be blocked regardless of whether that entity is itself included in Appendix A. What will determine whether financial transactions are "significant"?

A number of factors will influence the determination of whether a transaction is significant, including but not limited to:

- The size of the transaction(s)
- The number and frequency of the transaction(s)
- The type and complexity of the transaction(s)
- The extent of management involvement in the transaction(s)
- The proximity of the parties to the transaction(s) with a blocked person appearing on the Specially Designated Nationals (SDN) List
- The effect of the transaction(s) on Iran's ability to obtain weapons of mass destruction or commit acts of international terrorism
- Any effort to conceal the transaction(s)

610. How does CISADA treat pre-existing financial contracts?

There is no general exemption for payments arising out of pre-existing contracts. Whether such payments are "significant" will be examined on a case-by-case basis.

611. How does CISADA define "financial services"?

As provided in the Iranian Financial Sanctions Regulations, 31 C.F.R. Part 561, CISADA' s definition of "financial services" includes loans, transfers, accounts, insurance, investments, securities, guarantees, foreign exchange, letters of credit, and commodity futures or options.

612. Has the U.S. Treasury Department issued implementing regulations related to the prohibitions on U.S. financial institutions related to CISADA?

The Treasury Department has issued the following implementing regulations related to CISADA:

- **Iranian Financial Sanctions Regulations (31 CFR Part 561):** On August 16, 2010, the Treasury Department issued regulations to implement Sections 104(c) and 104(d), dealing specifically with the identification of foreign financial institutions for which U.S. financial institutions would be restricted/prohibited from opening or maintaining accounts. The regulations were effective when issued.
- **Comprehensive Iran Sanctions, Accountability, and Divestment Reporting Requirements (31 CFR Part 1060):** On April 27, 2011, the Treasury Department proposed regulations to implement Section 104(e) of CISADA which require would require that U.S. financial institutions report certain information to FinCEN on specified foreign banks for which the U.S. financial institution maintains a correspondent account. The regulations became effective October 5, 2011.
- **Iranian Transactions and Sanctions Regulations (31 CF.**R. Part 560) ("ITSR"): On October 22, 2012, the Treasury Department issued regulations to incorporate CISADA provisions as well as the provisions of Executive Order 13599 (blocking the property of the Government of Iran and Iranian Financial Institutions) and certain provisions of the Section 1245 of the National Defense Authorization Act for Fiscal Year 2012. These final regulations replace the Iranian Transactions Regulations in effect prior to that date.

Other CISADA requirements are expected to be subject to additional rulemaking.

613. What are the major provisions of Iranian Financial Sanctions Regulations implementing Sections 104(c) and 104(d) of CISADA?

Iranian Financial Sanctions Regulations (IFSR) provide that the Treasury may prohibit or impose strict conditions on the opening or maintenance in the United States of a correspondent account or a payable-through account for a foreign financial institution that the Treasury finds knowingly (or should have known):

- Facilitated the efforts of the Government of Iran, including Iran's Islamic Revolutionary Guard Corps (IRGC) or any of its agents or affiliates, to acquire or develop weapons of mass destruction or delivery systems for such weapons or to provide support for organizations deemed to be foreign terrorist organizations;
- Facilitated the activities of a person or entity subject to UN financial sanctions related to Iran;
- Engaged in money laundering to carry out such activity;
- Facilitated efforts by the Central Bank of Iran or any other Iranian financial institution to carry out such activity;
- Facilitated a significant transaction(s) or provided significant financial services for the IRGC or any of its agents or affiliates whose property is blocked under U.S. Iranian sanction.

The Treasury may force the closing of such correspondent account or payable through account (or other banking relationship) or impose certain conditions, such as:

- Prohibiting any provision of trade finance through the correspondent account or payable through account;
- Restricting the transactions that may be processed through such accounts to certain types (e.g., prohibit all transactions except personal remittances);
- Placing monetary limits on the transactions that may be processed; or
- Requiring preapproval from the U.S. financial institution for all transactions to be processed through such account.

Any person owned or controlled by a U.S. financial institution is prohibited from knowingly engaging in any transaction with or benefiting the IRGC or any of its agents or affiliates whose property is blocked.

U.S. financial institutions may not open or maintain correspondent or payable through accounts for those identified institutions and may only conduct such transactions as are necessary to close an account or transfer funds to the account of a foreign financial institution outside of the United States.

The regulations also make clear that a U.S. financial institution is not authorized to unblock or otherwise deal in property blocked under any other part in the process of closing a correspondent or payable through account for such a foreign financial institution. Findings, orders and regulations will be published in Appendix A to Part 560 of IFSR.

614. Where can a list of Iranian-linked financial institutions be found?

The ITSR issued on October 22, 2012 deleted Appendix A to Part 560 which listed financial institutions determined to be owned or controlled by the Government of Iran. The persons that were listed in Appendix A are now listed on OFAC's List of Specially Designated Nationals and Blocked Persons and their property and interests in property are blocked pursuant to Executive Order 13599 and ITSR Section 560.211

To obtain a current list, please refer to OFAC's website http://www.treasury.gov/resource-center/sanctions/Programs/Documents/irgc_ifsr.pdf.

615. Has the U.S. Treasury Department added any foreign financial institutions to Appendix A?

On September 7, 2010, the Treasury Department added the first foreign financial institution, Europäisch-Iranische Handelsbank (EIH), to Appendix A. EIH was added because of its alleged dealings with sanctioned Iranian banks in furtherance of Iran's activities related to the proliferation of weapons of mass destruction.

As of September 24, 2012, there were 25 financial institutions with IFSR tags, indicating 24 allegedly Iranian-linked financial institutions designated under IEEPA

U.S. financial institutions are encouraged to monitor the Treasury Department's website for information on additions to Appendix A.

616. Are the Islamic Revolutionary Guard Corps (IRGC), its agents and affiliates included on the SDN list?

Yes. The IRGC, its agents and affiliates appear on the SDN list bearing the [IRGC] tag.

As of September 24, 2012, there were 43 individuals and entities with IRGC tags. To obtain a current list, please refer to OFAC's website http://www.treasury.gov/resource-center/sanctions/Programs/Documents/irgc_ifsr.pdf.

617. Where can a list of foreign financial institutions that have violated IFSR be found?

The List of Foreign Financial Institutions Subject to Part 561 (the Part 561 List) includes entities that have violated Iranian Financial Sanctions Regulations (IFSR). U.S. financial institutions are prohibited from opening or maintaining a correspondent or payable-through account for any foreign financial institutions on the Part 561 List. The Part 561 List is available on OFAC's website at http://www.treasury.gov/ofac/downloads/561list.pdf.

618. Are entities on the Part 561 List included on the SDN list?

No. Entities on the Part 561 List are not included on the SDN list.

619. Have any foreign financial institutions violated IFSR?

Yes. On July 31, 2012, the U.S. Department of Treasury imposed sanctions under CISADA against the Bank of Kunlun Co. Ltd. in China and the Elaf Islamic Bank in Iraq. Specifically, these two banks were deemed to have violated Section 561.201 of IFSR, the implementing regulation of CISADA, which prohibits or imposes strict conditions with respect to correspondent accounts or payable-through accounts of certain foreign financial institutions that engage in activities that support the efforts of the Government of Iran or the IRGC and its agents or affiliates.

As of July 31, 2012, the following entities were included on the Part 561 List:

- Bank of Kunlun Co. Ltd.
- Elaf Islamic Bank
- Karamay City Commercial Bank Co. Ltd.
- Karamay Urban Credit Cooperatives

The last two entities were listed as aliases or former names for the Bank of Kunlun Co. Ltd.

620. What are the major provisions of Treasury's Comprehensive Iran Sanctions, Accountability, and Divestment Reporting Requirements (31 CFR Part 1060) implementing Section 104(e) of CISADA?

Comprehensive Iran Sanctions, Accountability, and Divestment Reporting Requirements (31 CFR Part 1060) requires U.S. financial institutions, including U.S. branches and agencies of foreign banks, to report, upon request from FinCEN, certain information about specified foreign banks for which the U.S. bank maintains a correspondent account. This information includes:

- Whether the foreign bank maintains a correspondent account for an Iranian-linked financial institution designated under the International Emergency Economic Powers Act (IEEPA)
- Whether the foreign bank has processed one or more transfers of funds within the preceding 90 calendar days related to an Iranian-linked financial institution designated under IEEPA, other than through a correspondent account: or
- Whether the foreign bank has processed one or more transfers of funds within the preceding 90 calendar days related to Iran's Islamic Revolutionary Guard Corps (IRGC) or any of its agents or affiliates designated under IEEPA.

In addition, a U.S. bank would have to request notification of the above from any foreign bank specified by FinCEN if an account is established within one year of the response to the request above for any Iranian-linked financial institution designated under IEEPA. The U.S. bank would be required to request notification within 30 days of establishing the account would be obligated to report this information to FinCEN within 10 days of receipt of the notification. FinCEN may also request, in certain instances, that a U.S. bank confirm that it does not maintain an account for a specified foreign bank, with a response due to FinCEN within 45 days of receipt of FinCEN's request for this information.

The regulation adds additional reporting requirements – Know Your Customer's Customers – for U.S. banks that are based on a newly imposed "duty to inquire" about the identification of a correspondent bank's customers and the originators, beneficiaries and purposes of transactions handled by a correspondent bank, regardless of whether there is a connection to the U.S. bank through the use of services or processing of transactions.

621. Are U.S. financial institutions required to review and independently verify responses from its foreign bank customers prior to submitting to the Treasury Department?

No. U.S. financial institutions are not required to review responses prior to submission to the Treasury Department. U.S. financial institutions are only required to respond to a written inquiry within 45 days of receipt, even if the response is a "non-response". However, if through the normal course of monitoring, a U.S. financial institution detects activity inconsistent with that provided by the foreign bank, it is obligated to submit this information to the Treasury Department.

622. What are the protocols for issuing Section 104(e) requests prior to distribution to financial institutions?

All Section 104(e) requests will be written and sent directly to banks that FinCEN, based on all available information, believes maintain correspondent accounts for the specified foreign bank(s).

623. Is there a minimum threshold for reporting transfers of funds processed within the preceding 90 calendar days related to an Iranian-linked financial institution designated under IEEPA?

No. The regulations do not establish a minimum threshold for a foreign bank to report on transfers of funds processed within the preceding 90 calendar days related to an Iranian-linked financial institution designated under IEEPA.

624. What guidance has the Treasury Department provided with regard to how U.S. financial institutions should query its foreign bank customers upon receipt of a written request under Section 104(e)?

FinCEN has created a model certification form that can be used by U.S. financial institutions to query its foreign bank customers. The model certification outlines the following:

- The purpose of the request

- Information that a foreign bank is requested to report to the U.S. financial institution
- Links to lists of relevant designated entities and individuals on which a foreign bank is requested to report

625. Are all types of U.S. financial institutions required to comply with Section 104(e)?

No. Section 104(e) applies to domestic ”banks,” including commercial banks or trust companies, private banks, savings and loan associations, national banks, thrift institutions, credit unions, and U.S. branches and agencies of foreign banks.

626. Are U.S. financial institutions required to take any action such as filing a SAR upon receipt of a written request under Section 104(e) regarding one of its foreign correspondent banking relationships?

U.S. financial institutions are not required to take any specific actions based on the information received in response to queries of the specified foreign banks, but the U.S. Treasury may, under CISADA, restrict or prohibit dealings with select foreign banks.

A financial institution should not automatically file a Suspicious Activity Report (SAR) upon receipt of a Notice from FinCEN. The decision to file a SAR should be based on the institution’s own investigation into the activity of the party(ies) that/who is the subject of the Notice.

627. Can U.S. financial institutions share information within a Section 104(e) request internally or externally?

A U.S. financial institution’s ability to share information within a Section 104(e) request will be determined by the requirement for confidentiality explicitly stated in each request by FinCEN.

628. Where directed by Treasury, what is the time frame for complying with an order to close a correspondent or payable through account?

Where the Treasury orders such a correspondent or payable through account to be closed, the U.S. financial institution holding such account may process limited transactions that are needed to close the accounts within 10 days of such designation.

629. What steps do U.S. financial institutions need to take to ensure compliance with the requirements of CISADA and ITRSHA?

Given the significant consequences of noncompliance, it is recommended that U.S. financial institutions, even prior to the issuance of additional regulations, review their portfolios of correspondent and payable though accounts for any potential problem foreign financial institutions, and begin developing due diligence and monitoring procedures designed to help ensure ongoing compliance.

630. When does the time period for record retention begin with written requests under Section 104(e)?

The record retention period begins on the date the Section 104(e) request from FinCEN is issued. Consistent with other AML laws and regulations, supporting documentation must be retained for five years.

631. What supporting documentation should be retained for recordkeeping purposes?

FinCEN advised that the all correspondence between the U.S. financial institution and FinCEN or between the U.S. financial institution and the foreign bank, regarding a request for information under Section 104(e) should be retained for recordkeeping purposes.

632. How does ITRSHRA affect foreign subsidiaries of U.S. parent companies?

Section 218 of ITRSHRA prohibits an entity owned or controlled by a U.S. person (or U.S. entity) and established or maintained outside the U.S. from knowingly engaging in any transaction directly or indirectly with the Government of Iran or any person subject to the jurisdiction of the Government of Iran that would be prohibited by a regulation or one of the several Orders that have been issued pursuant to the International Emergency Economic Powers Act (IEEPA) if the transaction were engaged in by a U.S. person or in the U.S. Such Orders implemented a broad ban on transactions, trade in goods and services, and investment involving Iran, Iranian-linked financial institutions, and the Iranian Government. It subjects non-U.S. entities owned or controlled by U.S. entities to Iranian sanctions. Entities

include “partnerships, associations, trusts, joint ventures, corporations and other organizations.” The term “own or control” with respect to the entity means:

- To hold more than 50 percent of the equity interest by vote or value in the entity;
- To hold a majority of seats on the board of directors of the entity; or
- To otherwise control the actions, policies or personnel decisions of the entity.

Attempts to evade or avoid ITRSHRA are also prohibited.

633. Is there a safe harbor provision for U.S. parents to avoid penalties for violations committed by its foreign subsidiaries?

Yes. Section 218 of ITRSHRA provides that civil penalties will not apply where the U.S. parent divests or terminates business with the foreign subsidiary by February 6, 2013.

634. How does ITRSHRA amend the reporting obligations of publicly traded companies?

Section 219 amends the Securities Exchange Act of 1934 to require publicly traded companies engaging in certain types of Iran-related business to publicly disclose such business to the U.S. Securities and Exchange Commission (SEC) through their mandatory annual or quarterly reports. This requirement is effective for reports required by the SEC after February 6, 2013. Covered companies must disclose whether the company or any of its affiliate knowingly engage in a number of specified activities, including but not limited to transactions involving any blocked property specified under Orders 13224 or 13382, which block property and prohibit transactions with:

- Persons who commit, threaten to commit, or support terrorism or related to blocking of property of weapons of mass destruction proliferators and their supporters; or
- The Government of Iran, without the specific authorization of a Federal department or agency, Thus, issuers in the U.S. would be required to report on the activities of their own affiliates or additionally face violations of the SEC rules.

635. What determinations were made about the National Iranian Oil Company (NIOC) and the National Iranian Tanker Company (NITC) pursuant to Section 312 of the ITRSHRA?

Section 312 of the ITRSHRA required the Secretary of the Treasury to determine whether NIOC or NITC were agents or affiliates of Iran’s Islamic Revolutionary Guard Corps (IRGC). On September 24, 2012, the Treasury Department made such a determination with regard to Although NIOC was already subject to previous sanctions, the determination can expose entities engaging in prohibited activities with NIOC to CISADA sanctions.

636. What provisions of ITRSHRA are implemented by Executive Order 13628?

On October 9, 2012, the President issued Executive Order 13628 – Authorizing the Implementation of Certain Sanctions Set Forth in the Iran Threat Reduction and Syria Human Rights Act of 2012 and Additional Sanctions with Respect to Iran. Specifically, E.O. 13628 implemented the following provisions of ITRSHRA:

- Section 204: Expansion of sanctions available under the Iran Sanctions Act of 1996 (ISA);
- Section 218: Liability of parent companies for violations of sanctions by foreign subsidiaries;
- Section 402: Imposition of sanctions with respect to the transfer of goods or technologies to Iran that are likely to be used to commit human rights abuses; and
- Section 403: Imposition of sanctions with respect to persons who engage in censorship or other related activities against citizens of Iran

E.O. 13628 also addresses several other issues, including providing penalties to be imposed on persons who improve Iranian petroleum refinement capacities, sell refined petroleum products to Iran, or provide certain enhancements to Iran’s ability to import petroleum products where the value of the activity is over specified thresholds.

637. What penalties may be imposed on a U.S. financial institution for violations of CISADA?

U.S. financial institutions that knowingly violate CISADA related to opening and maintenance of correspondent and payable through accounts may be subject to a civil penalty of $250,000 or twice the value of the transactions that violated the sanctions and criminal penalties of up to $1 million and 20 years in prison for individuals violating the

sanctions. Violations of the due diligence, monitoring and reporting requirements of CISADA could also be subject to the penalties prescribed by the USA PATRIOT Act.

National Defense Authorization Act for Fiscal Year 2012

638. What is the National Defense Authorization Act for Fiscal Year 2012 (NDAA)?

The National Defense Authorization Act for Fiscal Year 2012 (NDAA) is a federal law authorizing appropriations for the U.S. Department of Defense (DOD) including military activities, military construction and defense activities of the Department of Energy (DOE).

639. What additional sanctions did the United States impose on Iran due to the passage of the NDAA?

Section 1245 of the Fiscal Year 2012 NDAA imposes the following sanctions with respect to Iran:

- Designation of financial sector of Iran as primary money laundering concern under Section 311 – Special Measures, including the Central Bank of Iran (CBI);
- Blocking and prohibiting all transactions in all property and interests in property of Iranian-linked financial institutions, including the CBI, if such property are in the United States, come within the United States, or come within the possession or control of a U.S. person;
- Imposition of sanctions with respect to Iranian-linked financial institutions, including the CBI, that prohibits or imposes strict conditions on the opening and maintaining of a correspondent account or payable-through account for entities designated by the United States who knowingly conducted or facilitated any significant financial transaction with Iranian-linked financial institutions, including the CBI.

640. What is the goal of Section 1245 of the NDAA?

The goal of Section 1245 of the NDAA is to reduce Iranian oil revenues and discourage transactions with the Central Bank of Iran (CBI) by imposing sanctions on foreign financial institutions that knowingly conduct or facilitate certain significant financial transactions with the CBI.

641. How are “petroleum products” defined for the purposes of Section 1245 of the NDAA?

The U.S. Energy Information Administration’s (EIA) standard definition of “petroleum products” includes “unfinished oils, liquefied petroleum gases, pentanes plus, aviation gasoline, motor gasoline, naphtha-type jet fuel, kerosene-type jet fuel, kerosene, distillate fuel oil, residual fuel oil, petrochemical feedstock, special naphthas, lubricants, waxes, petroleum coke, asphalt, road oil, still gas, and miscellaneous products obtained from the processing of crude oil (including lease condensate), natural gas, and other hydrocarbon compounds.”

The EIA’s definition of petroleum products do not include non-petroleum fuels, including, but not limited to the following:

- Natural gas
- Liquefied natural gas
- Biofuels
- Methanol

642. What activities can trigger sanctions on a foreign financial institution under the NDAA?

Sanctions may be imposed on financial institutions that knowingly conduct or facilitate significant financial transaction with the Central Bank of Iran (CBI) or designated Iranian financial institutions, except for transactions involving the sale of food, medicine and medical devices. The President may also impose sanctions on the Central Bank of Iran. Further, foreign financial institutions can face sanctions under the NDAA if they knowingly conduct or facilitate significant financial transactions for the purchase of Iranian petroleum or petroleum products with a U.S.-designated Iranian financial institution or the CBI.

643. How does the NDAA define the terms “significant” and “knowingly”?

Treasury anticipates modeling the definition of “significant” for NDAA purposes on the IFSR. The IFSR, which implements section 104 of CISADA, identifies factors to be used in determining what is significant (as it relates to transactions) in 31 C.F.R. Section 561.404, which allows the Secretary of the Treasury to consider the totality of the facts and circumstances, while providing a list of 7 broad factors that can play a role in the determination, including:

- The size, number and frequency of the transaction(s);
- The nature of the transaction(s);
- The level and awareness of management and whether the transaction(s) are part of a pattern of conduct;
- The nexus between the transactions and a blocked person appearing on the Specially Designated Nationals (SDN) List;
- The impact of the transaction(s) on statutory objectives;
- Whether the transactions involve deceptive practices; and
- Such other factors the Secretary deems relevant on a case by case basis.

“Knowingly” is defined in the IFSR with respect to conduct, a circumstance, or a result, to mean that an entity or individual had actual knowledge, or should have known, about the conduct, the circumstance or the result.

OFAC has indicated it anticipates the use of a broad definition of “financial transaction” that encompasses “any transfer of value involving a financial institution.” The term “transaction” includes, but is not limited to: (i) the holding of nostro, vostro, or loro accounts for or with the CBI or designated banks, such as Bank Melli Iran and/or Bank Saderat Iran, including any of their branches or subsidiaries worldwide (“Listed Parties); (ii) the provision of trade finance and/or letter of credit services for or with Listed Parties; (iii) the provision of guarantees or similar instruments for or with Listed Parties; (iv) the provision of investment products or instruments for Listed Parties and/or the participation with Listed Parties in investments; (v) the receipt or origination of wire transfers on behalf of or involving Listed Parties; (vi) the acceptance of commercial paper (retail and wholesale) drawn on Listed Parties, and the clearance of such paper (including, but not limited to check and similar drafts); (vii) the receipt of or origination of ACH or ATM transactions with Listed Parties; and/or (viii) any other transactions for or on behalf of, directly or indirectly, Listed Parties and/or with Listed Parties service as correspondents, respondents, or beneficiaries. That would include transactions where the Listed Parties do not appear on the face of the transaction but where the transaction is undertaken with knowledge of the involvement of a Listed Party based on a relationship that exists through a third party such as a money exchange or trading house.

644. Does the NDAA amend CISADA’s provision that prohibits or imposes strict conditions on opening and maintaining correspondent accounts or payable-through accounts for designated entities?

No. The NDAA does not amend Section 104(c) of CISADA.

645. How do the NDAA and Executive Order 13599 and the blocking of all Iranian financial institutions affect the financial sanctions in terms of CISADA? Do CISADA sanctions apply to financial transactions with any Iranian financial institution?

CISADA applies to transactions only with Iranian financial institutions designated in connection with Iran’s WMD or terrorism activities and are identified on the SDN List with the [IFSR] tag.

On February 5, 2012, the President issued Executive Order 13599 – Blocking Property of the Government of Iran and Iranian Financial Institutions to amend the 31 CFR Part 560: Iranian Transaction Regulations (ITR) to include the provisions within Section 1245 of the NDAA.E.O. 13599 blocks all property and interests in property of the Government of Iran, including the Central Bank of Iran (CBI) and all Iranian financial institutions , E.O. 13599 is not grounded in the authorities that relate to counterterrorism or counter-proliferation and accordingly do not implicate CISADA.

Previously, financial institutions were obligated to reject these transactions.

Blocked entities under E.O. 13599 appear on OFAC’s Specially Designated National (SDN) List bearing the [IRAN] tag.

646. How does Executive Order 13622 impact the NDAA and ISA?

On July 30, 2012, the President signed Executive Order 13622 – Authorizing Additional Sanctions with Respect to Iran (E.O. 13622). E.O. 13622 provides additional sanctions authorities to the Secretary of the Treasury and the Secretary of State, building on prior authorities outlined in the NDAA and ISA. The goal of E.O. 13622 is to impose new sanctions against the Iranian energy and petrochemical sectors.

E.O. 13622 imposes financial sanctions on foreign financial institutions found to have knowingly conducted or facilitated any significant financial transaction with the National Iranian Oil Company (NIOC) or Naftiran Intertrade Company (NICO) (except for sales of refined petroleum products to NIOC or NICO that are below the dollar threshold that could trigger sanctions under ISA).

E.O. 13622 also provides additional authority to impose sanctions on foreign financial institutions found to have knowingly conducted or facilitated significant transactions for the purchase or acquisition of petroleum or petroleum products from Iran through any channel, with the aim of deterring Iran or any other country or institution from establishing workaround payment mechanisms for the purchase of Iranian oil to circumvent the NDAA oil sanctions. The existing exception rules under the NDAA will apply to these new sanctions; accordingly, countries determined by the Secretary of State to have significantly reduced their purchases of Iranian crude oil will be excepted from this new measure.

E.O. 13622 further gives the Secretary of the Treasury the authority to block the property and interests in property on any person determined to have materially assisted, sponsored, or provided financial, material or technological support for, or goods or services in support of NIOC, NICO or CBI or the purchase or acquisition of U.S. bank notes or precious metals by the Government of Iran.

It also provides new powers to the Secretary of State (in consultation with the Secretary of the Treasury and other cabinet members) to impose a range of sanctions on individuals or entities determined to knowingly engage in significant transactions for the purchase or acquisition of petroleum, petroleum products or petrochemical products from Iran. Entities or individuals that have been found to meet such criteria are to be subject to the same sanctions that may be imposed under the ISA. .

All property and interests in property of NIOC and NICO subject to U.S. jurisdiction are already blocked pursuant to E.O. 13599.

647. Which special measures were authorized against Iran?

In November 2011, FinCEN issued a notice of proposed rulemaking proposing the imposition of a special measures against the Islamic Republic of Iran, including the Central Bank of Iran, as a jurisdiction of primary money laundering concern under Section 311 of the PATRIOT Act. The proposed rule would prohibit covered financial institutions from establishing, maintaining, administering or managing correspondent accounts for or on behalf of an Iranian banking institution.

FinCEN indicated in the proposal that prior regulations that have designated jurisdictions of primary money laundering concern under Section 311have not included the jurisdiction's central bank within the scope of the regulation. Section 1245 of the National Defense Authorization Act for Fiscal Year 2012 (NDAA) designated the Iranian financial sector as a jurisdiction of primary money laundering concern, effectively mirroring FinCEN's determination in its proposed rulemaking.

648. Which special measures were authorized against Syrian financial institutions?

On March 9, 2006, the U.S. Treasury Department designated the Commercial Bank of Syria, including its subsidiaries, Syrian Lebanese Commercial Bank, as financial institutions primary money laundering concern pursuant to Section 311 – Special Measures of the USA PATRIOT Act.

649. What are the penalties for violations of sanctions imposed by Section 1245 of the NDAA?

Any person who violates, attempts to violate, conspires to violate or causes a violation of the NDAA could be subject to civil penalties in an amount not to exceed the greater of $250,000 or an amount that is twice the amount of the transaction that is the basis of the violation with respect to which the penalty is imposed. Criminal penalties can include fines up to $1,000,000, imprisonment up to 20 years or both.

Executive Orders and Other Sanctions

650. What other recent measures have been imposed in connection with Syria?

In addition to other broad sanctions imposed against Syria, three recent Executive Orders have been issued involving Syria.

On May 18, 2011 Executive Order 13573 was issued, entitled “Blocking Property of Senior Officials of the Government of Syria, which imposed blocking on certain persons and agencies of the Government of Syria.

On August 17, 2011, Executive Order 13582 “Blocking Property of the Government of Syria and Prohibiting Certain Transactions with Respect to Syria” was issued. The Order imposes broad prohibitions on investments with Syria, most exportation and importation, sales or supply from the U.S. or by a U.S. person wherever located into Syria, of any services to Syria, as well as other actions. It also provided that all property and interests in property that are in the U.S., that hereafter come within the U.S., or that are or hereafter come within the possession or control of any U.S. person, including any overseas branch, of the Government of Syria are blocked and may not be transferred, paid, exported, withdrawn or otherwise dealt in. Additionally, all property any interests in property are also blocked for any person the Secretary of the Treasury determines has materially assisted, sponsored, or provided financial, material or technological support for, or goods or services in support of, any person whose property and interest in property are blocked pursuant to the order or are owned, controlled by or have acted or purposed to act for or on behalf of, directly or indirectly, any person whose property and interests are blocked pursuant to this order.

On May 1, 2012, Executive Order 13608 was issued, which, among other things, authorized the Department of the Treasury to impose broad sanctions on anyone who has violated or attempt to violate certain orders concerning property and interests in property of any person subject to U.S. sanctions concerning Syria or Iran, or who has facilitated deceptive transactions for or on behalf of any person subject to U.S. sanctions concerning Syria or Iran.

651. How does Executive Order 13606 (GHRAVITY E.O.) impact the obligations of financial institutions?

On April 22, 2012, the President signed “Executive Order 13606 Blocking the Property and Suspending Entry into the United States of Certain Persons with Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology” (the “GHRAVITY E.O”).

The GHRAVITY E.O. requires U.S. persons to block all property and interests in property of persons designated by the Secretary of the Treasury, in consultation with or at the recommendation of the Secretary of State who:

- Have operated, or directed the operation of, information and communications technology that facilitates computer or network disruption, monitoring, or tracking that could assist in or enable serious human rights abuses by or on behalf of the Government of Iran or the Government of Syria; or
- Have sold, leased, or otherwise provided, directly or indirectly, goods, services, or technology to Iran or Syria likely to be used to facilitate such activities.
- Have materially assisted, sponsored, or provided financial, material or technological support for, or goods or services to or in support of, the activities described above or any person whose property and interests in property are blocked pursuant to this order; or
- To be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to that order.

Entities that are 50 percent or more owned by persons blocked by the GHRAVITY E.O are also blocked, regardless of whether such entities appear on the Annex or OFAC’s SDN List.

652. Where can a list of persons designated under GHRAVITIY E.O. be found?

Designated entities under GHRAVITY E.O. appear on the SDN list bearing the [HRIT] tag.

653. How is “information and communications technology” defined for the purposes of GHRAVITY E.O.?

"Information and communications technology" is defined as “any hardware, software, or other product or service primarily intended to fulfill or enable the function of information processing and communication by electronic means, including transmission and display, including via the Internet.”

654. How does Executive Order 13608 on Prohibiting Certain Transactions With and Suspending Entry in the U.S. of Foreign Sanctions Evaders with Respect to Iran and Syria impact the obligations of financial institutions?

On May 1, 2012, the President signed "Executive Order 13608 – Prohibiting Certain Transactions with and Suspending Entry into the United States of Foreign Sanctions Evaders with Respect to Iran and Syria" (E.O. 13068). E.O. 13608 strengthened Treasury's ability to impose sanctions on foreign persons determined to have violated, attempted to violate, conspired to violate or caused a violation of sanctions on Iran or Syria.

E.O. 13608 also gives the Treasury the authority to impose sanctions on foreign persons who have facilitated deceptive transactions for or on behalf o f persons subject to the U.S. sanctions. E.O. 13608 empowers the Secretary of the Treasury, in consultation with the Secretary of State, to impose on a foreign person certain measures upon determining that the foreign person:

(1) has violated, attempted to violate, conspired to violate, or caused a violation of any license, order, regulation, or prohibition contained in, or issued pursuant to certain Executive Orders related to national emergencies, or to the extent such conduct relates to property and interest in property of any person subject to the U.S. sanctions concerning Iran or Syria, or certain national emergencies, as defined in specific Executive Orders. With respect to any covered foreign person, the Secretary of the Treasury may prohibit, to the extent in or related to either (i) any goods, services or technology in or intended for the U.S., or (ii) any goods services or technology provided by or to the U.S. persons, wherever located, all transactions or dealings, whether direct or indirect, involving such persons, including, but not limited to the following activities:

- Exporting;
- Re-exporting;
- Importing;
- Selling;
- Purchasing;
- Transporting;
- Swapping;
- Brokering;
- Approving;
- Financing;
- Facilitating; or
- Guaranteeing.

These prohibitions apply, except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this Order, and notwithstanding any contract entered into or any license or permit granted prior to the date of this order.

Transactions by U.S. persons or within the U.S. involving persons sanctioned under this order are prohibited, effectively cutting the listed persons off of from the U.S. marketplace and financial system. By cutting off access to the U.S. marketplace and financial system to such sanction evaders, the Order provides the Treasury with the power to prevent and deter such behavior and to hold such persons accountable and to convince them to change their behavior. Publicly identifying such persons also allows U.S. persons to avoid unwittingly engaging in transactions with identified foreign persons that may expose U.S. persons to the risk of sanction violations.

If an individual or entity is made subject to the sanctions under this Order, U.S. persons generally may no longer provide or procure from such individual or entity any goods, services or technology. Practically speaking, it means that the sanctioned individual or entity will be cut off from the U.S. commercial and financial systems.

Financial institutions must:

- Reject any wire transfer involving a listed person; and

- Restrict use of accounts owned by a listed person, so that they cannot be operated without an authorization from OFAC. However, the account is not blocked. In general, a financial institution is prohibited from providing to or procuring from such a sanctioned individual or entity any goods, services or technology.

655. How is the term "deceptive transaction" defined for the purposes of E.O. 13608?

A deceptive transaction is defined as "any transaction where the identity of any person subject to the United States sanctions concerning Iran or Syria is withheld or obscured from other participants in the transaction or any relevant regulatory authorities.

Foreign persons have facilitated deceptive transactions will be listed under E.O. 13608 and subject to sanctions. Although this transactions are not subject to blocking under this specific Order (although note, if they are otherwise subject to blocking under another program, then blocking is required), A U.S. person may not provide or procure goods or services, including financial services, or technology to or from a listed person without authorization from OFAC, unless the transaction is otherwise exempt from regulation under the International Emergency Economic Powers Act (e.g., certain travel-related transactions). Wire transfers involving the assets of a listed person under this Order must be rejected. A U.S. person is prohibited from dealing with an Order 13608-listed person even where the dealing does not involve Iran or Syria (as well as where it does involve either country).

656. How is the E.O. 13608 list different from the Denied Persons List maintained by BIS?

The Denied Persons List (DPL) is a list of individuals and entities that have been denied export privileges for violating or presenting an imminent risk of violating the Export Administration Regulations (EAR). E.O. 13608 complements the Denied Persons List (DPL) by addressing two types of sanctions violations outside of the scope of the EAR:

- The prohibition of the provision of services, goods and technology and the prohibition of transactions to or from identified or listed persons, and
- The Treasury may prohibit transactions or dealings involving goods and technology not subject to EAR.

However, unlike the Commerce's authority, Treasury's authority under this Order may be implemented only with respect to foreign individuals or entities.

657. What if a transaction is already underway?

If a transaction is underway at the time of the listing, a U.S. person must cease dealing with the listed person and the U.S. person is prohibited from engage in transactions or dealings in or related to any goods, services or technology to or from the listed person, unless the transaction is exempt under the International Emergency Economic Powers Act, or until such time that OFAC authorizes the transaction pursuant to the Order. If the transaction involves a wire transfer, the U.S. financial institution must reject it and file a rejection report with OFAC within 10 days. Also, A U.S. person my not use a listed person to facilitate personal remittances to or from Iran or Syria without specific authorization from OFAC.

Screening Customers and Transactions

658. What parties, activities and transactions are subject to OFAC Sanctions?

Activities, including all trade or financial transactions, regardless of the amount, and all account relationships, regardless of type, are subject to OFAC Sanctions. This includes but is not limited to:

- **Account types**: deposits, loans, trusts, safety deposit boxes
- **Transaction types**: wire transfers, ACH transfers, letters of credit, currency exchanges, deposited/cashed checks, purchases of monetary instruments, loan payments, security trades, retail purchases
- **Individuals/entities**: account holders, authorized signers, guarantors, collateral owners, beneficiaries, nominee shareholders, noncustomers, employees, vendors

As a practical matter, however, institutions must decide, based on their assessment of OFAC risk, which parties, activities and transactions will be screened against the OFAC Sanctions listings, as well as how often, since 100 percent screening is not a viable option for most institutions.

659. When should customers be screened against the OFAC Sanctions listings?

Customers should be screened under several circumstances. Examples include, but are not limited to, before account opening (although some institutions screen at the end of the day and choose to take the risk), upon changes to the existing information (e.g., amendments to beneficiaries, signers, change of address), entire existing customer population periodically (frequency based on OFAC risk assessment) and upon distribution of funds (e.g., incoming/outgoing wire transfers, payees on monetary instruments).

660. Is a financial institution in violation of OFAC regulations if it establishes an account for an SDN designee?

Opening an account for an SDN designee is considered the provision of a prohibited service and is subject to sanctions. Accordingly, if a financial institution does not conduct OFAC screening before the opening of an account, it is taking a risk and thus the financial institution should implement controls on the account to ensure transactions are not conducted until the customer has been screened against Sanctions listings to ensure that, if required, any funds obtained by the financial institution are appropriately blocked.

661. How often should an institution's existing customer base be checked against the continuously updated Sanctions listings?

The existing customer base should, ideally, be checked against the OFAC Sanctions listings at each update. If this is not possible, the frequency of OFAC screens should be based on the institution's risk profile, recognizing that as soon as a name is added to the Sanctions listings, OFAC expects compliance. If the institution fails to identify and block/reject a transaction/trade conducted by an individual or entity on the Sanctions listings, consequences can include enforcement actions and negative publicity.

662. Should the names of account parties (e.g., beneficiaries) who are not account holders be included in the OFAC screening process?

Yes. Account parties who are not account holders (e.g., beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories and powers of attorney) should be screened for possible matches. However, the extent to which an institution can include these account parties will depend on the institution's risk profile, CIP, KYC programs and available technology.

Since account beneficiaries have a "property interest" in products, financial institutions should screen account beneficiaries upon account opening, while updating account information, when performing periodic screening and upon disbursing funds. Beneficiaries include, but are not limited to, trustees, children, spouses, nonspouses, entities and powers of attorney.

663. How does OFAC define the term "property"?

"Property" is defined by OFAC as "anything of value." Examples of property include, but are not limited to: money, checks, drafts, debts, obligations, notes, warehouse receipts, bills of sale, evidences of title, negotiable instruments, trade acceptance, contracts, and anything else real, personal or mixed, tangible or intangible, "or interest or interests therein, present, future, or contingent."

664. How does OFAC define the term "interest"?

"Interest" is broadly defined by OFAC as "any interest whatsoever, direct or indirect."

665. Since many financial institutions perform OFAC screens post-account opening, are they in violation if the next-day verification results in a positive "hit"?

If an institution is aware that a potential customer is on the Sanctions listings, it is prohibited from opening the account.

If the account is already open, the important thing is not to allow any transactions to be conducted. If an initial deposit was made in the account of a positive match to the Sanctions listings, the institution is obligated to freeze/reject the assets.

666. Do OFAC regulations apply only to accounts of and transactions by those customers that transact business through the institution?

No. OFAC regulations apply to all financial transactions performed or attempted by a financial institution, and this would include, for example, transactions of noncustomers, payments made to vendors and compensation paid to employees. However, the extent to which an institution includes such parties in its screening process will depend on the institution's risk profile and available technology.

667. If a transaction is sent and/or received on behalf of a third party, should the institution include the third party in its OFAC screening process?

Yes. If the institution is aware that the transaction is being sent or received on behalf of a third party, it should include the third party in its OFAC screening process.

668. Does an institution need to check the OFAC Sanctions listings when selling cashier's checks and money orders?

In theory, every transaction and every activity that a U.S. institution engages in is subject to OFAC regulations. If an institution knows or has reason to know that a target is party to a transaction, the institution's processing of the transaction would be unlawful. However, a financial institution, depending upon its risk profile and available technology, may decide to screen only some cashier's checks and money orders (e.g., higher-dollar thresholds).

669. In the instance of a wire transfer, if a "hit" is found after the payment has been completed, who has ultimate liability?

Each U.S. person who handled or permitted the transaction may be found to have violated the sanctions program. For example, the originating financial institution, the correspondent bank and the beneficiary bank could each be fined by OFAC.

670. Is an institution obligated to report a possible match with the name of someone who is not a customer of the financial institution (e.g., beneficiary of a funds transfer originated by its own customer)?

Yes. After a diligent effort is made to rule out a false hit, which may include a call to OFAC to discuss whether the name of the possible match is a party subject to the sanctions, the institution should report the hit regardless of its relationship with the individual or entity in question.

671. If a loan is approved but involves a true OFAC "hit" on the Sanctions listings, what should the customer be told as a denial reason?

If a true OFAC "hit" is confirmed, there is no reason not to explain the reason for the blocked/rejected transaction to the customer. The customer can contact OFAC directly for further information.

672. How should institutions screen information not maintained in an electronic format?

Unless previous authorization was granted by OFAC or exclusion is expressly exempted by statute, all customers and other account/transaction party names should be screened, regardless of the form in which the information is maintained. The scope and frequency of the screenings should be based on the institution's risk profile and available technology. For example, a possible risk-based approach could include screening payees of checks greater than $10,000.

673. Can an individual send money to a sanctioned country using a third-country company's website?

Although a website may say it is permissible to send funds to a sanctioned country, it would be in violation of OFAC laws and regulations to do something indirectly that is not permissible to do directly. The use of sites by U.S. persons that may be used to facilitate unauthorized transactions would be a violation of U.S. law.

674. How can institutions effectively screen customers and transactions against multiple sanctions lists?

Many institutions use interdiction software to screen customers and transactions against multiple lists simultaneously. For additional guidance on the various types of software available, please refer to the sections: AML Technology, Interdiction Software and List Providers.

675. What are cover payments and how are they a challenge to monitoring for sanctions violations?

A cover payment involves two separate transactions: one credit transfer message that travels a direct route from the originating bank to the ultimate beneficiary's bank, and a second credit transfer that travels through a chain of correspondent banks to settle or "cover" the first credit transfer message. Cover payments are used in correspondent banking to facilitate international transactions.

Prior to changes made to the Society for Worldwide Interbank Financial Telecommunication (SWIFT) Payments Messaging system in 2009, a challenge to monitoring sanctions violations stemmed from the industry's use of SWIFT MT202 transactions as cover payments.

MT202 transactions are intended for bank-to-bank transactions; however, they were sometimes used in lieu of the MT103 messages intended for use in a commercial transaction. In part, this occurred because the MT202s were more cost-effective. Regardless of the reason, however, the substitution of a MT202 for a MT103 in a commercial transaction masked the underlying parties to a transaction, thereby frustrating monitoring attempts.

To address this lack of transparency, SWIFT developed a variant of the MT202 payment message type, MT202 COV, which allows all information contained in certain fields (e.g., originator and beneficiary information) of the MT103 to be transmitted in the MT202 COV and is to be used for cover payments in lieu of MT202s.

676. What does "stripping" mean?

"Stripping" is when information is removed from payment information in order to prevent the funds transfer from being blocked or rejected when being screened for possible sanctions violations.

677. What steps can financial institutions take to mitigate the risks of stripping?

To mitigate the risks associated with "stripping," a financial institution can do the following:

- Implement a stringent OFAC training program that includes OFAC requirements and the penalties for noncompliance for all branches and operations, both foreign and domestic.
- Implement a review process of potential OFAC hits to ensure wires were not "stripped."
- Implement a review process of funds transfers with the same sender/amount coming back in a short time.

Automated Clearing House Transactions and IATs

678. Are Automated Clearing House (ACH) transactions subject to OFAC regulations?

Yes. ACH transactions, just as is the case with all other financial transactions, are subject to OFAC regulations. With the growth in ACH transactions going beyond direct deposits of payroll, government benefits and consumer bill payments to include one-time debits and check conversions, which can include cross-border transactions, the overall OFAC risk associated with ACH transactions has increased.

679. Which participants in an ACH transaction are subject to OFAC regulations?

All ACH participants, including originators, originating depository financial institutions (ODFIs), receiving depository financial institutions (RDFIs), receivers, ACH operators and third-party service processors are subject to OFAC regulations. ACH participants generally include the following:

- An originator is an organization or person that/who initiates an ACH transaction, either as a debit or credit.
- An ODFI is the originator's depository financial institution that initiates the ACH transaction into the ACH network at the request of and by agreement with its customers.

- An RDFI is the receiver's depository institution that receives the ACH transaction from the ACH operators (which may be the ODFI, another bank or a third party) and credits or debits funds to or from their receiver's accounts.
- A receiver is a person, corporation or other entity who has authorized the originator to initiate an ACH transaction, either as a debit or credit to an account held at the RDFI.
- An ACH operator processes ACH transactions that flow between different financial institutions and serves as a clearing facility that receives entries from the ODFIs and distributes the entries to the appropriate RDFI (e.g., Fed ACH, Electronic Payments Network [EPN]).
- A third-party service provider (TPSP) is an entity other than an originator, ODFI or RDFI that performs any functions on behalf of the originator, the ODFI or the RDFI with respect to the processing of ACH entries. The functions of these TPSPs can include, but are not limited to, the creation of ACH files on behalf of the originator or ODFI, or acting as a sending point of an ODFI (or receiving point on behalf of an RDFI).

For international ACHs, the NACHA operating rules define the following two new participants:

- A foreign correspondent bank is defined as a participating depository financial institution (DFI) that holds deposits owned by other financial institutions and provides payment and other services to those financial institutions.
- A foreign gateway operator (FGO) acts as an entry point to or exit point from a foreign country.

680. How is a cross-border or international ACH transaction defined by OFAC?

OFAC defines a cross-border or international ACH transaction as an ACH transaction in which at least one of the ACH participants (e.g., originator, ODFI, receiver, RDFI) is outside of the United States or a U.S. jurisdiction and at least one of the processing institutions is subject to OFAC regulations (i.e., within the United States or a U.S. jurisdiction).

For example, an international ACH transaction can include a domestic ODFI and a domestic RDFI that was initiated by a foreign originator.

681. What is an IAT?

The international automated clearing house transaction (IAT) is a new Standard Entry Class (SEC) code that is required for all international ACH debits and credits as of September 18, 2009. Additional information is required to be sent with the ACH to facilitate sanctions filtering and monitoring for potentially suspicious activity. These new fields include the following:

- Originator's name/address
- Beneficiary's name/address
- Originating bank name/ID/branch code
- Foreign correspondent bank name/ID/branch code
- Receiving bank name/ID/branch code
- Reason for payment

682. What should an ODFI do to comply with OFAC regulations?

In general, the ODFI must verify the originator is not a blocked party and make a good-faith effort to determine the originator is not transmitting blocked funds.

For cross-border ACH transactions, the ODFI is required to code the transaction as an IAT and provide the required information as detailed above.

In addition to screening the originator against OFAC Sanctions listings, ODFIs should consider including the following in agreements with originators:

- Acknowledgement that originators and the ODFI are subject to OFAC Sanctions (for certain types of ACH instructions, such an acknowledgement is required)
- Reference to possible delays in processing, settlement and/or availability for screening or investigating possible hits against the OFAC Sanctions listings

683. What should an RDFI do to comply with OFAC regulations?

An RDFI should screen its receivers against OFAC Sanctions listings. Additionally, RDFIs are obligated to unbatch ACH transactions containing IATs and screen against OFAC Sanctions listings.

684. Is additional screening required for third-party service providers (TPSPs)?

As financial institutions can be held responsible in some situations for the acts of TPSPs, the financial institution should assess these relationships and ACH transactions to determine OFAC risk and develop appropriate policies, procedures and processes to mitigate such risks. For further guidance on managing third-party risk, please refer to the sections: Know Your Third Parties and Third-Party Payment Processors.

685. Can ODFIs and RDFIs rely on each other for OFAC compliance?

Domestic ODFIs and RDFIs can rely on each other for OFAC compliance to screen the originator and receiver as described above. This reliance, however, cannot be placed upon international ODFIs and RDFIs.

686. Is an ODFI obligated to unbatch domestic ACH transactions in order to screen against OFAC Sanctions listings?

No. If an ODFI receives domestic ACH transactions that its customer already has batched, the ODFI is not responsible for unbatching those transactions to screen against OFAC Sanctions listings.

687. If an ODFI unbatches domestic ACH transactions, is it obligated to screen against OFAC Sanctions listings?

Yes. If an ODFI unbatches a file originally received from the originator in order to process “on-us” transactions, then it is obligated to screen against OFAC Sanctions listings because it is acting as both the ODFI and RDFI for these transactions.

Financial institutions should determine the level of OFAC risk of the remaining unbatched transactions that are not “on-us” and develop appropriate policies and controls to address the associated risks (e.g., screening each unbatched ACH record) through its OFAC risk assessment. For additional guidance on OFAC risk assessments, see the Risk Assessments section.

688. How should ACH transactions that violate OFAC regulations be handled?

If an ODFI processes an ACH credit for a receiver that is in violation of OFAC regulations, the RDFI should post the credit to the receiver’s account, freeze the funds and report the transaction to OFAC.

If an ODFI processes a violative ACH debit, the RDFI should return the funds to the ODFI with the Return Reason Code R16 (Account Frozen) in accordance with NACHA Operating Rules. The ODFI should then freeze the funds and report the transaction to OFAC.

All transactions that have not yet been processed by the ODFI but are believed to be in violation of OFAC regulations should be reported to OFAC for further review.

For additional guidance on ACHs, please refer to the Automated Clearing House Transactions section.

Trade Finance Transactions

689. Are trade finance transactions subject to OFAC regulations?

Yes. Trade finance transactions, just as is the case with all other financial transactions, are subject to OFAC regulations. Each institution should establish a risk-based approach to screening the following trade finance participants for possible sanctions violations related to:

- Traders (e.g., importer, exporter)
- Financial institutions facilitating trade finance transactions (e.g., in the case of letters of credit, issuing bank, confirming bank, nominated bank, accepting bank, discounting bank, reimbursing bank, paying bank)
- Insurers

- Shipping agents/couriers

690. What have been some challenges to complying with OFAC regulations with respect to trade finance?

The major challenges of complying with OFAC regulations with respect to trade finance include, but are not limited to, the following:

- Numerous parties located in foreign jurisdictions
- Frequent amendments (e.g., changes to involved parties)
- Documentary-based transactions that require manual screening

For additional guidance on the money laundering and terrorist financing risks of trade finance, please refer to the Trade Finance Activities section.

Blocking and Rejecting Transactions

691. What is the difference between "blocking" and "rejecting"?

"Blocking" simply means freezing property. It is an across-the-board prohibition against transfers or dealings of any kind with regard to the property.

For example, a U.S. bank receives instructions to wire $2,000 to a customer's relative in a country subject to OFAC Sanctions. The U.S. bank interdicts the payment, blocks it and reports it because it qualifies under the OFAC Sanctions program as a transaction to be blocked.

"Rejecting" means, simply, to not process a transaction. In some cases, an underlying transaction may be prohibited, but there is no blockable interest in the transaction. In these cases, the transaction is simply rejected or not processed.

For example, a U.S. credit union receives instructions from its customer to send $4,000 to a country subject to OFAC Sanctions. The credit union forwards the payment instructions to its correspondent that processes its wire transfers. The correspondent interdicts the payment, rejects it and reports it because it qualifies under the OFAC Sanctions program as a transaction to be rejected.

Financial institutions should consult the specific economic sanction and follow the instructions exactly as written; requirements differ among the sanctions. In most cases, blocking is required; rejections are permitted only under very limited circumstances. The financial institution should, however, contact OFAC with questions.

692. How will an institution know whether to block or reject a transaction?

An institution's obligation to block or reject a transaction depends on the requirements of the specific sanctions program involved.

693. With whom does title to blocked property rest?

Title to blocked property remains with the sanctioned target (designated country, national or blocked person), but the exercise of rights normally associated with ownership is relegated to the U.S. Treasury Department and controlled by OFAC-specific licenses or other authorization by OFAC.

694. What should be done with blocked funds?

Depository institutions must hold blocked funds in an individual account or an omnibus account (as long as an audit trail will allow specific funds to be unblocked with interest at any point in the future) that earns interest at a commercially reasonable rate. Only OFAC-authorized debits (including some normal banking service charges) can be made in these accounts. OFAC can be contacted directly for further assistance on what types of transactions or service fees are permissible.

For nondepository institutions, the same requirements apply except for one. The nondepository institution will have to engage a depository institution to open a blocked account and hold the funds. The nondepository institution maintains

the account on its books in the name of the individual or entity whose funds were blocked, but it should ensure the account is designated as a blocked account by the depository institution.

695. Can an institution inform its customers that their funds have been blocked?

Yes. Unlike with Suspicious Activity Reports (SARs), an institution can inform customers of their blocked funds, as well as their right to apply for the unblocking and release of their funds through OFAC. However, if a SAR is also filed on the customer, then the customer may not be told of the SAR.

696. When can an institution release blocked funds?

Funds can be released by the institution only upon receipt of a license or the issuance of an executive order allowing payment of the blocked funds. Usually, the customer who owns the blocked funds must apply for a license at OFAC to allow for such a payment. For additional guidance on licensing, please refer to the Licensing section.

697. Does informing a customer of the potential blocking of funds constitute assisting the customer in evading OFAC Sanctions?

It is not advisable for an institution to inform a customer that a transaction is subject to blocking, as some of the sanctions programs prohibit aiding or abetting. Institutions may want to seek legal counsel before providing a response and/or referring the customer to OFAC. In any event, if the institution receives instructions from its customer for a wire transfer to a sanctioned country or designee, the institution must act on the instructions by blocking/rejecting the funds.

698. How much has been blocked/rejected?

Based on the 2011 Terrorist Assets Report issued by OFAC, the United States has blocked $398 million in terrorist-related assets within the United States. An additional $122 million in unblocked funds also has been identified by OFAC as related to terrorism.

699. Can an institution allow a third party to conduct its screenings against the OFAC Sanctions listings?

Yes. However, ultimate responsibility for OFAC compliance still lies with the institution, not the third party.

700. How can customers request the release of blocked funds?

Customers must complete an application for the Release of Blocked Funds. Upon approval by OFAC, the application becomes a specific license authorizing the unblocking and release of funds. Funds can be released to the originator or originating bank, or in accordance with OFAC's instructions in the specific license, which usually allow payment in accordance with the original payment instructions.

Investigating Potential Matches

701. What is the most effective way of monitoring transactions for OFAC?

More institutions are beginning to appreciate the challenge of dealing with long and frequently changing OFAC Sanctions listings and, as such, are turning to interdiction software solutions to strengthen their OFAC compliance programs. Given the increasing use and complexity of international wire transactions, using interdiction software is a necessity for some institutions.

However, institutions cannot lose sight of the fact that a system is a tool, not the only solution. In the end, there can be no substitute for experienced and well-trained staff.

For smaller institutions with relatively few wire transactions, a simple in-house system using existing database software can be designed to perform the OFAC screening. This can be an effective and more cost-efficient alternative to purchasing OFAC interdiction software.

For additional guidance on interdiction software, please refer to the AML Technology section.

702. What are some tips for clearing an OFAC "hit"?

Tips for clearing OFAC "hits" include, but are not limited to, the following:

- Utilization of primary factors that by themselves provide a high probability of a false positive, including, but not limited to, the following:
    - General false positive (e.g., SDN is individual and potential match is a vessel)
    - Identification number
    - Date of birth
- When unable to clear OFAC "hits" based on primary factors, utilization of secondary factors that may not individually clear a match but together provide a high probability of a false positive, including, but not limited to, the following:
    - Not an exact name match (e.g., only one name matches the two or more names of the individual)
    - Country of origin
    - Address

If unable to clear based on primary or secondary factors, institutions should contact OFAC for further guidance.

703. What should an institution do if it confirms a positive OFAC "hit"?

Finding a "hit" may necessitate blocking or rejecting a transaction and, if it is ultimately determined to be a positive hit, it will require the filing of a Blocked Transaction or Rejected Transaction report with OFAC. An institution is required to file the OFAC report within 10 business days of the blocked/rejected transaction. However, many possible hits turn out to be "false positives," which the institution should identify and clearly document the rationale and decision during its investigation process.

704. What should an institution do when it is not comfortable that it has sufficient dispositive information to conclude the name is not a true match?

The institution should contact OFAC directly by telephone (1.800.540.OFAC) or e-mail hotlines for further guidance. The investigation should be documented and maintained in the event questions arise in the future.

705. Should a financial institution permanently suppress names causing frequent "false positives" in order to reduce the volume of transactions to be reviewed?

Financial institutions must carefully consider the risk of suppressing a name permanently. Since the Sanctions listings are dynamic, it may be best to suppress a name until the Sanctions listings are updated. A false positive at a certain time may become a true hit when the Sanctions listings are updated.

706. Is it necessary to file a SAR for an OFAC hit?

If the only "suspicious" activity was the OFAC hit, the blocked/rejected report satisfies a financial institution's reporting obligation. If the OFAC hit served as an alert generator to other suspicious activity in the customer's account, both a blocked/rejected report and a SAR are warranted, in which case the SAR should be sent promptly to FinCEN.

Reporting Requirements

Blocked/Rejected Transaction Reports

707. What are the reporting requirements for blocked and/or rejected transactions?

The following reports must be filed with OFAC:

- Report of Blocked Transactions
- Report of Rejected Transactions

- Annual Report of Blocked Property
- Reports on Litigation, Arbitration and Dispute Resolution Proceedings

A Report of Blocked Transactions must be filed for blocked transactions within 10 business days of the blocked transaction. A Report of Rejected Transactions must be filed for rejected transactions within 10 business days of the rejected transaction. If the institution is holding funds in a blocked account on June 30, it is required to file an Annual Report of Blocked Property by September 30 of that year. U.S. persons involved in litigation, arbitration or other binding alternative dispute resolution proceedings regarding blocked property must provide notice of such proceedings to the OFAC Chief Counsel and submit copies of all documents associated with such proceedings within 10 business days of their filing.

708. What is the time frame for filing a report to OFAC?

Blocked and Rejected Transaction reports must be filed within 10 business days after the date of detection of the "hit." All submissions must be received in writing and be kept on file with supporting documentation at the financial institution for five years. An Annual Report of Blocked Property must be filed by September 30 each year.

709. What does the term "date of detection" mean for OFAC purposes?

The term "date of detection" is the date of the blocked/rejected transaction.

710. Where are OFAC reports filed?

Institutions are required to submit Blocked Transactions, Rejected Transactions and Blocked Property reports to the Compliance Programs Division, OFAC, Department of the Treasury, Washington, DC, 20220.

711. Can OFAC reports be filed electronically?

No. Currently, Blocked Transactions and Rejected Transactions reports can be submitted only via regular mail or fax. The Annual Report of Blocked Property can be submitted via regular mail. However, OFAC is developing a pilot project to permit the electronic filing of reports.

712. Should supporting documentation be sent with Blocked Transactions and Rejected Transactions reports to OFAC?

Blocked Transactions and Rejected Transactions reports must include a copy of the original payment instructions and specific transaction detail. All supporting documentation should be sent to OFAC with the Blocked Transactions and Rejected Transactions reports. It may be prudent to check with OFAC at the time of filing to see if any additional documentation is needed.

713. How long should institutions retain OFAC reports and supporting documentation?

OFAC reports and supporting documentation must be retained for a minimum of five years from the date of the filing to OFAC. The retention period may be longer than five years, depending on the state or self-regulatory organization (SRO).

714. If multiple institutions are involved in processing the transaction, who ultimately is responsible for filing the appropriate reports with OFAC?

The institution that blocks or rejects the prohibited transaction is responsible for filing the required reports. However, other individuals or institutions involved in the transaction who failed to block, reject and/or report the prohibited transaction may be subject to penalties.

Licensing

715. Are there exceptions to the OFAC Sanctions programs?

Yes. OFAC can issue general licenses authorizing the performance of certain categories of transactions, as well as specific licenses, on a case-by-case basis. Additional information on how to request a license can be found in the regulations for each sanctions program on OFAC's website.

716. What is a general license?

A general license is defined by OFAC as an authorization from OFAC that allows certain transactions for a class of persons without the filing of a license application with OFAC. The terms of a general license are provided in the relevant embargo or sanctions program.

717. What is a specific license?

A specific license is defined by OFAC as a "permit issued by OFAC on a case-by-case basis to a specific individual or company allowing an activity that would otherwise be prohibited by the embargo or sanctions program."

718. How is a specific license obtained?

Individuals or entities must submit an application for specific licenses to OFAC. Application requirements are specific to the particular embargo or sanctions program. For additional details, refer to OFAC's website: www.ustreas.gov/ofac.

719. What information must be provided on an application for a specific license?

Most license programs do not have a specific application form. However, a detailed letter should be remitted to OFAC that should include all necessary information as required in the application guidelines or regulations for the specific embargo program. A detailed description of the proposed transaction, including the names and addresses of any individuals or companies involved, should be included in the letter. In many cases, OFAC's licensing division will be able to guide further through a phone consultation what is best included in the letter, as every sanctions program has different nuances for licensing.

720. Is there a formal process of appeal if an application for a specific license is denied by OFAC?

No. There is no formal process of appeal; however, OFAC will reconsider its decision for good cause, such as where the applicant can demonstrate changed circumstances or submit additional relevant information that was not presented previously.

721. How can specific licenses be verified by institutions?

Each specific license has a control number that can be verified by contacting OFAC. If a customer claims it has a specific license, the institution should verify the transaction conforms to the terms of the license before processing the transaction and retain a copy of the authorizing license.

722. Are specific licenses transferable?

In general, specific licenses are not transferable.

723. Do specific licenses expire/require renewal?

Specific licenses expire on the expiration date set forth in the license. If no expiration date is included, the institution should check with OFAC to see if the license is still valid.

724. Can specific licenses be revoked?

Yes. Specific licenses can be revoked or modified at any time at the discretion of the Secretary of the Treasury.

725. Do specific licenses provide protection from civil or criminal liability for violations of any laws or regulations?

No. A specific license is only good to conduct such business as it is approved for, and in no way prevents penalties for violations of laws or regulations.

726. Are licenses issued only by OFAC?

No. In some instances, applicants may apply for licenses with the U.S. Bureau of Industry and Security (BIS).

727. What is the U.S. Bureau of Industry and Security (BIS)?

BIS is an agency of the U.S. Department of Commerce. The mission of BIS is to advance U.S. national security, foreign policy and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership. BIS achieves this by controlling the dissemination of dual-use products and technology to destinations and end users throughout the world. BIS expertise includes engineering and product knowledge used for product classification.

728. Does BIS issue any lists similar to OFAC's SDN list?

The BIS publishes the following lists:

- **Denied Persons List (DPL) –** A list of individuals and entities that have been denied export privileges. No exporter may participate in an export or re-export transaction subject to an Export Administration Regulation (EAR) with a person or entity whose export privilege has been denied by the BIS.
- **Entity List –** List of names of certain foreign parties that are prohibited from receiving some or all items subject to the Export Administration Regulations (EAR) unless the exporter secures a license. The List can include businesses, research institutions, government and private organizations, individuals, and other types of legal persons, that are subject to specific license requirements for the export, re-export and/or transfer (in-country) of specified items;
- **Unverified List –** List of names and countries of foreign persons who in the past were parties to a transaction with respect to which BIS could not conduct a pre-license check or a post-shipment verification for reasons outside of the U.S. Government's control. The presence of a party on this list in a transaction is a "Red Flag" that should be resolved before proceeding with the transaction; and
- **BIS General Orders –** List of persons and businesses with restricted export privileges.

729. Who is required to screen against the BIS lists?

Exporters are required to screen against the BIS lists. No exporter may participate in an export or re-export transaction subject to an Export Administration Regulation (EAR) with a person or entity whose export privilege has been denied by the BIS.

730. Are financial institutions required to screen against the BIS lists?

No. It is the responsibility of the exporter to ensure that it is not transacting with an individual or entity listed on the BIS lists; however, a financial institution is still liable if it facilitates a transaction with a listed individual or entity. As a prudent measure, although not required, some financial institutions opt to screen against the DPL in addition to the OFAC Sanctions listings.

731. What action must institutions take if a positive "hit" is identified on the BIS lists?

Follow-up actions may involve restrictions on shipping to certain countries, companies, organizations and/or individuals. Unlike with OFAC, there are no reporting requirements when a positive hit is identified. For additional guidance, contact BIS's Office of Enforcement Analysis (OEA).

732. What is the interrelation between BIS and OFAC?

BIS and OFAC both work toward a common national security goal, with different functions. With regard to licensing, both BIS and OFAC can have overlapping authority. For some sanctions programs, only one of the agencies may provide a license.

733. Are there other U.S. agencies with licensing and export prohibition responsibilities beyond OFAC and BIS?

Yes. The Commerce, State, Defense and Energy departments administer the following licensing and export prohibition programs:

- The Commerce Control List (CCL), administered by the Commerce Department, is used to regulate the export and re-export of items that have commercial uses but also have possible military applications ("dual-use" items).
- The U.S. Munitions List (USML), administered by the State Department, is used to control the export of defense articles, services and related technologies.

- The Defense Department is actively involved in the interagency review of those items controlled on both the CCL and the USML. The agencies work together when there is a question about whether a proposed export is controlled on the CCL or the USML.
- The Energy Department controls nuclear technology and technical data for nuclear power.
- The Bureau of Export Administration (BXA), U.S. exporters and third parties in general are prohibited from dealing with denied parties in transactions involving U.S. items. BXA also maintains an Entities List, comprising foreign end-users engaged in proliferation activities. Since these entities pose proliferation concerns, exports to them are usually prohibited without a license. However, since the BXA guidelines are administered under a case-by-case basis, there are some listed entities that can still receive low-level technology without an export license.
- The Debarred Parties List is maintained by the State Department. It lists the names of individuals denied export privileges under the International Traffic in Arms Regulations (ITAR).

602 Letter and Prepenalty Notice

734. What is a "602 Letter"?

If OFAC learns that a prohibited transaction was processed through a U.S. institution without being blocked or rejected, it may send an administrative demand for information called a 602 Letter to the institution requesting an explanation regarding how the transaction was processed.

735. What is a Prepenalty Notice?

OFAC may issue a Prepenalty Notice in response to information provided in a 602 Letter response. The Prepenalty Notice cites the violation and states the amount of the proposed penalty.

736. What is the allotted time frame for responding to a Prepenalty Notice?

An institution has 30 days to make a written presentation on why a penalty should not be imposed, or if imposed, why the proposed civil money penalty should be reduced.

737. What are the consequences of not responding to a Prepenalty Notice?

Failure to respond to a Prepenalty Notice may result in default judgments levying maximum fines.

Voluntary Disclosure

738. What is meant by "voluntary disclosure"?

"Voluntary disclosure" is defined by OFAC as notification to OFAC of an apparent sanctions violation by the institution that has committed the violation.

739. Are there instances in which a disclosure may not be considered voluntary?

There are a few instances in which a notification may not be considered by OFAC to be voluntary. The first is if OFAC has previously received information concerning the conduct from another source, such as another regulatory or law enforcement agency, or if another person's Blocked Transactions and Rejected Transactions reports detail information that would show a violation. Similarly, responding to an administrative subpoena or another inquiry from OFAC would not be deemed voluntary. In addition, the submission of a license application may not be deemed a voluntary disclosure.

740. Should institutions voluntarily disclose past undetected violations of OFAC regulations?

Self-disclosure may be considered a mitigating factor by OFAC in civil penalty proceedings. Voluntary disclosure will be considered when determining an enforcement response. It is advisable that institutions seek legal counsel's advice before self-disclosing.

741. In what form should the voluntary disclosure be?

Self-disclosure should be in the form of a detailed letter to OFAC, with supporting documentation, as appropriate.

Independent Testing

742. What should be considered with respect to independent testing of an OFAC program?

Although OFAC audit programs will vary depending on the company's nature of business and operations, there are certain basic considerations that should be included in all OFAC audits, such as:

- Confirming that the institution's compliance policy or operating procedures detail OFAC restrictions and the roles and responsibilities of company personnel in ensuring compliance
- Confirming that the institution has provided appropriate training on the OFAC compliance requirements
- Reviewing the institution's procedures for screening new customer and other third-party relationships against the OFAC list and existing customer/third-party relationships against updates to the Sanctions listings
- Determining whether the institution's personnel understand how OFAC screening software works and its level of reliability (e.g., what degree of confidence can be expected from the algorithms used by the software)
- Determining whether any modifications have been made to the OFAC screening software and, if so, whether these are properly supported and documented
- Testing the effectiveness of the institution's monitoring procedures: where screening is manual, reviewing the company's transaction records to determine whether any OFAC transactions may have gone undetected; where screening is automated, constructing "dummy tests" of actual OFAC names to ensure that they are identified by the system
- Reviewing the institution's procedures for clearing "hits" and related documentation
- Determining whether true "hits" are reported to OFAC, according to the requirements
- Determining that the institution has effective controls for not releasing frozen assets until permitted by OFAC
- Following up on any previously identified problems or issues in past audit reports or regulatory examination reports
- Sampling transactions with missing information (e.g., country fields) and related payment orders for potential indicators of stripping

743. Is there a requirement that OFAC compliance programs be subject to periodic independent testing?

Performing independent testing of an institution's OFAC program is not mandated by regulation, but is prudent given the risks of noncompliance. Some institutions may find it beneficial to conduct a review of the OFAC program simultaneously with the review performed of the AML program. When the reviews are not performed in conjunction with one another, the time frame for performing a review should be risk-based. For institutions that have determined they are high-risk pertaining to OFAC (for additional information on determining whether an institution is high-risk for OFAC consideration, please refer to the Risk Assessments section), it may be more appropriate to conduct a review more frequently (every 12 to 18 months) to ensure that potential gaps and deficiencies, which may lead to potential sanctions violations, are identified.

744. Should independent testing of an OFAC program be risk-based?

Yes. Just as with the independent testing of the AML program, the testing of the OFAC program should be risk-based. As not every institution experiences the same level of OFAC risk, the depth of review performed may be more or less rigorous to be in line with evaluating whether the OFAC program is adequately designed and operating effectively in order to mitigate the institution's unique level of risk.

Consequences of Noncompliance

745. What are the consequences of noncompliance?

Penalties for violations may include civil fines ranging from $11,000 to $1.075 million (or even more under certain circumstances) per violation or criminal fines ranging from $50,000 to $10 million and imprisonment ranging from 10 to 30 years for willful violations. A non-negotiable part of any violation is the publication on the OFAC website of the violator's name (if it is an entity), details of the violations and amount of the fine.

In addition to monetary penalties, OFAC may impose the following actions for noncompliance:

- Cautionary or warning letter
- Revocation of license
- Civil penalty
- Criminal penalty (usually done through referral to the Department of Justice [DOJ])

746. What does it mean that OFAC is a "strict liability program"?

Strict liability means that the offender is liable even if it did not know that it violated a sanctions program.

747. What are the penalties for failing to comply with OFAC regulations?

Corporations and individuals may be subject to civil and/or criminal penalties for non-compliance with OFAC regulations and individuals may also be subject to imprisonment, as follows:

- Civil penalties equal to the greater of $250,000 or 2X the amount of the transaction (from $50,000 per transaction) up to $1,075,000 per violation
- Criminal fines of up to $1 million and 20 years in jail.

These fines apply to all Sanction programs administered by OFAC, with the exception of some cases (e.g., Cuba).

748. Are there any exceptions for first-time offenders?

Yes. First-time offenders may be eligible for a 25 percent reduction of the base penalty.

749. If the transaction was successfully blocked/rejected by the financial institution, can the individual/entity initiating the transaction still be subject to penalties?

Yes. Blocked Transactions and Rejected Transactions reports contain information that can be confirmed and examined to determine whether proper due diligence procedures were used. The Blocked Transactions and Rejected Transactions reports show that the individual/entity originating the transaction violated OFAC regulations in some manner and thus can be subject to penalties. For example, if an individual initiates a wire transfer to a Sudanese government-owned company, the payment would be blocked. The individual could be subject to penalties depending on the circumstances of the transaction under the International Emergency Economic Powers Act (IEEPA), the law that enforces the Sudanese Sanctions Regulations.

750. What is OFAC's process for issuing civil penalties?

OFAC will send a letter to the violator stating the details for each individual case. Most proceedings include the opportunity for an administrative hearing and prehearing discovery prior to imposition of a penalty or asset forfeiture. OFAC also has a process it may use for settlement of a matter before a prepayment penalty notice has been issued.

751. What factors are considered by OFAC when evaluating the severity of OFAC violations?

With respect to how it evaluates the severity of OFAC violations, the 31 CFR 501 – Economic Sanctions Enforcement Guidelines indicate that OFAC considers the following factors, though this is not necessarily an exhaustive listing:

- Evaluation of the OFAC program by the institution's regulator
- History of the institution's OFAC compliance and whether it was a first offense

- Circumstances around the identified OFAC violation and any patterns of weakness in the OFAC compliance program
- Negligence or fundamental flaw in the institution's compliance effort or system
- Whether the institution voluntarily disclosed the violation
- Actions taken by the institution to correct violations to ensure that similar violations do not reoccur

752. What is the difference between a civil penalty and a settlement?

Civil penalties require an actual agency determination of a violation. A settlement is a negotiated agreement between the agency and a company that does not require the actual determination of a violation.

753. What are some examples of OFAC violations in nonfinancial services companies?

A travel service provider could be fined for unlicensed services rendered in Cuba. A medical products manufacturer could be penalized for the shipment of unlicensed medical equipment to Iran. A casino could be fined for payment of a slot jackpot to an individual on the Specially Designated Nationals (SDN) list.

Common Gaps and Challenges

754. What have been some of the more noteworthy recent OFAC settlements?

The more recent (2009-2012) noteworthy OFAC settlements have involved foreign banking organizations with U.S. operations. These settlements stem from investigations that OFAC has conducted over the course of several years. Examples include:

- **Lloyds Bank** entered into a Deferred Prosecution Agreement (DPA) in January 2009 related to alleged "stripping" for a 12-year period of Iranian and Sudanese customer and bank names and addresses from wire transfer payment messages; this, in turn, caused U.S. financial institutions to violate OFAC Sanctions. The bank paid a $350 million fine under the DPA and was subsequently entered into a $217 million settlement with OFAC, which was deemed to have been satisfied by the $350 million fine.
- Based on allegations similar to those in the Lloyds Bank case, **Credit Suisse** entered into a DPA and paid a fine of $536 million in December 2009.
- **ABN Amro**, in a well-publicized case that took many years to reach settlement, entered into a DPA and paid a $500 million fine in March 2010 on allegations of stripping.
- In August 2010, **Barclays Bank** entered into a DPA and paid $298 million to settle allegations that, for over a decade, it used cover payments or engaged in stripping to conceal payments in violation of the Burmese, Cuban, Iranian and Sudanese sanctions, among others. These payments were processed through Barclays' New York branch and unrelated U.S. banks. Barclays' fine was considered small by some given the allegations, but may be attributable to the fact that Barclays reportedly self-disclosed some violations in 2006.
- A $619 million settlement with **ING Bank** took place in June 2012. The settlement resolves OFAC's investigation into ING Bank's intentional manipulation and deletion of information about U.S.-sanctioned parties in more than 20,000 financial and trade transactions routed through third-party banks located in the United States between 2002 and 2007, primarily in apparent violation of the Cuban Assets Control Regulations, 31 C.F.R. part 515, but also of the Iranian Transactions Regulations, 31 C.F.R. part 560; the Burmese Sanctions Regulations, 31 C.F.R. part 537; the Sudanese Sanctions Regulations, 31 C.F.R. part 538; and the now-repealed version of the Libyan Sanctions Regulations, 31 C.F.R. part 550, which was in effect until 2004.
- An $88.3 million settlement was reached with **JP Morgan Chase** (JPMC) in August 2011. The settlement involves an investigation into 1,711 wire transfers totaling approximately $178.5 million through a correspondent account between December 12, 2005, and March 31, 2006, involving Cuban persons in apparent violation of the CACR. JPMC conducted an investigation into the wire transfers it had processed through the correspondent account. The results of this investigation were reported to JPMC management and supervisory personnel, confirming that transfers of funds in which Cuba or a Cuban national had an interest were being made through the correspondent account at JPMC. Nevertheless, the bank failed to take adequate steps to prevent further transfers.

In 2012, the New York State Department of Financial Services (DFS) threatened to revoke the banking license of Standard Chartered Plc, for hiding $250 billion tied to Iran in violation of U.S. law. Standard Chartered Plc allegedly stripped approximately 60,000 transactions of the identities of sanctioned parties over a 10 year period to evade U.S. sanctions laws and regulations. Standard Chartered settled this case with the DFS by agreeing to a fine of $340 million, installing a monitor for at least two years to scrutinize its money laundering controls, and hiring an AML auditor for its New York branch. This case was noteworthy in that the action against Standard Chartered was brought unilaterally by the DFS and not in concert with a federal bank regulator and OFAC.

755. What are some of the common challenges to maintaining an effective OFAC compliance program?

The following include some of the challenges that companies have experienced in implementing an OFAC program:

- Updates to OFAC Sanctions listings are not incorporated in a timely manner
- Lack of screening for OFAC-sanctioned countries (filter includes OFAC SDN list only)
- Inadequate OFAC training and/or understanding of the various sanction programs
- Overreliance on third parties to perform the OFAC screening (e.g., correspondent banks, intermediary banks, service providers)
- Inadequate and poor documentation of due diligence in clearing potential OFAC matches
- Poor record retention
- Existing customers, employees or third-party service providers (e.g., vendors, consultants) are not screened against OFAC Sanctions listings, and/or updates to the list are performed infrequently, if at all (e.g., safe deposit box customers who do not have deposit accounts, noncustomers or parties involved in letters of credit)
- Transactions are not screened against OFAC Sanctions listings, and/or updates to the list are performed infrequently, if at all (e.g., checks, monetary instruments, ACHs, cover payments)
- Lack of screening beyond originator and beneficiary fields (e.g., cover payments often list originator/beneficiary in additional fields that may not be screened in interdiction software), additional address fields (e.g., physical, mailing, alternate)
- Ineffective use of interdiction software:
    - Utilization of high confidence levels for matches (e.g., 100 percent), thereby preventing possible hits from generating alerts for further review
    - Implementation of inconsistent matching algorithms/confidence levels for each product, transaction, customer and/or department
    - Ineffective use of exclusion features, thereby suppressing potential hits

Other U.S. and International Government Sanctions Programs

756. Should institutions include other U.S. or international government sanctions program lists as part of their OFAC programs?

U.S. government agencies, such as the Department of the Treasury, the U.S. Bureau of Industry and Security (BIS), the Department of Commerce, the Department of Labor and the State Department, have independent prohibitions on transactions with certain individuals or entities beyond those included in OFAC Sanctions listings, including, but not limited to, the following:

- **Denied Persons List (DPL), Bureau of Industry and Security (BIS) –** A list of individuals and entities that have been denied export privileges. No exporter may participate in an export or re-export transaction subject to an Export Administration Regulation (EAR) with a person or entity whose export privilege has been denied by the BIS.

- **Unverified List, (BIS) –** A list of names and countries of foreign persons who in the past were parties to a transaction with respect to which BIS could not conduct a pre-license check or a post-shipment verification for reasons outside of the U.S. Government's control. The presence of a party on this list in a transaction is a "Red Flag" that should be resolved before proceeding with the transaction.
- **The Entity List (BIS) –** A list of names of certain foreign parties that are prohibited from receiving some or all items subject to the Export Administration Regulations (EAR) unless the exporter secures a license. The List can include businesses, research institutions, government and private organizations, individuals, and other types of legal persons, that are subject to specific license requirements for the export, re-export and/or transfer (in-country) of specified items.
- **BIS General Orders –** A list of persons and businesses with restricted export privileges administered by the Department of Commerce.
- **List of Goods Produced by Child Labor or Forced Labor –** A list administered by the U.S. Department of Labor to reduce the import of goods produced with potential human trafficking and labor violations.

Institutions that operate internationally also should consider other government sanctions lists as part of an OFAC program. This would depend on the institution's internal risk assessment.

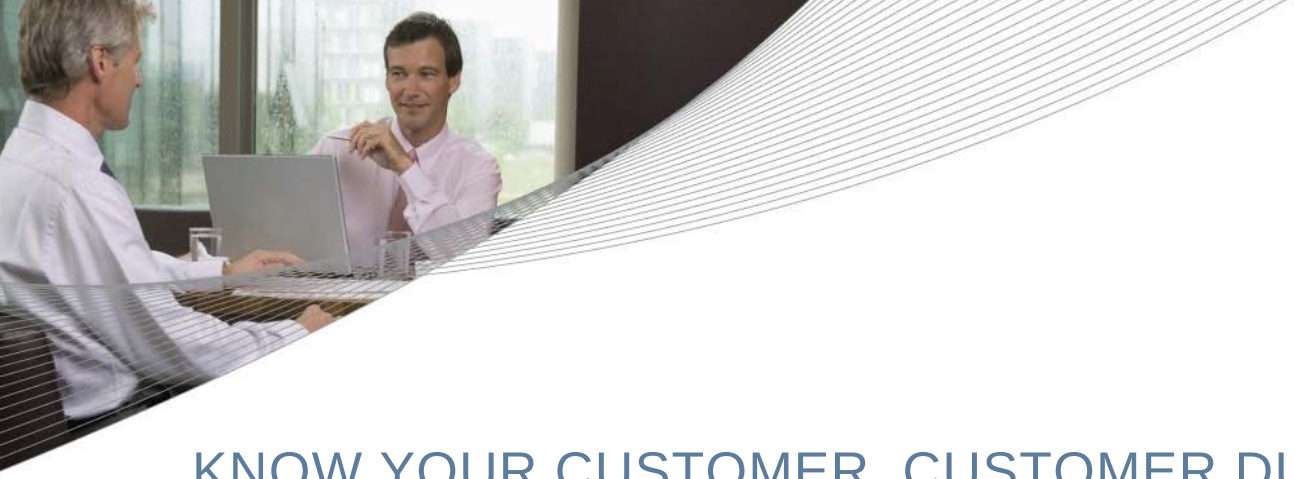
757. What other international government sanctions lists exist beyond the OFAC Sanctions lists?

There are several sanctions lists maintained by other countries that include, but are not limited to, the following:

- **Bank of England (BOE) List:** The BOE, the central bank of the United Kingdom, publishes lists of individuals and organizations against which financial sanctions have been imposed.
- **Australian Department of Foreign Affairs and Trade (DFAT) List:** The purpose of this list is to freeze assets of terrorists by making it a criminal offense for persons to hold, use or deal with assets that are owned or controlled by persons or entities on the list.
- **European Union (EU) Consolidated List:** The EU maintains a list of persons, groups and entities subject to Common Foreign Security Policy-related financial sanctions.
- **The Hong Kong Monetary Authority (HKMA) List:** Institutions that find they have done business with individuals or entities on the HKMA List are required to report such activity to the HKMA and Hong Kong's Joint Financial Intelligence Unit (JFIU).
- **Monetary Authority of Singapore (MAS) List:** The MAS issues a list of individuals who and organizations that have been sanctioned by the government of Singapore. Dealing with any of those cited on the MAS List can lead to fines, criminal penalties and increased regulatory scrutiny for financial institutions operating in that country.
- **New Zealand Police (NZP) List:** The NZP maintains the list of terrorist entities designated by the UN Security Council Regulations against the Taliban and al-Qaida, as well as those designated under the Terrorism Suppression Act 2002.
- **Canadian Government's Office of the Superintendent of Financial Institutions (OSFI) List:** Regulations mandate that every Canadian financial institution and foreign branch operating in Canada review their records on a continuing basis for the names of individuals listed in OSFI's Schedule to the Regulations.
- **Reserve Bank of Australia (RBA) List:** The RBA administers sanctions as specified in the Banking (Foreign Relations) Regulations 1959. The responsibility of DFAT is to maintain and publish the Australian government's list of terrorists and their sponsors, those in the former Iraqi regime, and the sanctions lists of those in the former government of the Federal Republic of Yugoslavia, ministers and senior officials of the Government of Zimbabwe, and entities associated with the Democratic People's Republic of Korea (North Korea).
- **UN Consolidated List:** The Security Council of the United Nations is empowered to take enforcement measures to maintain or restore international peace and security under Chapter VII of its charter. One such enforcement measure is the imposition of sanctions, including economic and trade sanctions, arms embargoes, travel bans, and other financial or diplomatic restrictions. The Security Council has imposed sanctions on individuals and organizations through a variety of resolutions.

758. How can institutions effectively screen customers and transactions against multiple sanctions lists?

Many institutions have utilized interdiction software to screen customers and transactions against multiple lists simultaneously. For additional guidance on the various types of software available, please refer to the AML Technology section.



KNOW YOUR CUSTOMER, CUSTOMER DUE DILIGENCE AND ENHANCED DUE DILIGENCE

Overview

759. What is Know Your Customer (KYC)?

KYC generally refers to the steps taken by a financial institution to establish the identity of a customer and be satisfied that the source of the customer funds is legitimate. This includes:

- Customer identification program (CIP) (For additional guidance on CIP, please refer to Section 326 – Verification of Identification section.)
- Customer due diligence (CDD)
- Enhanced due diligence (EDD)

760. What are CDD and EDD?

CDD is information obtained for all customers. Information obtained for CDD should enable a financial institution to verify the identity of a customer and assess the risks associated with that customer.

EDD refers to additional information that would be collected for those customers deemed to be of higher risk.

The specific requirements of CDD/EDD are dependent on the risk profile of a financial institution.

761. What should a financial institution consider when developing its KYC standards?

A financial institution may consider the following when developing its KYC standards:

- Complying with AML requirements (e.g., Section 326 – Verification of Identification, Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts)
- Collecting relevant information to enable the assessment of money laundering and terrorist financing risks of all customers
- Understanding the extent to which public data sources can be used to obtain reliable information about customers
- Collecting relevant information to provide business line and compliance personnel adequate context to determine if monitored transactions are consistent with the customer's nature of business/occupation
- Understanding information available to verify customer identity, which may differ across customer and geographic markets

762. What additional information might a financial institution request as part of an EDD process?

EDD might include additional steps to validate information provided by the customer, and/or conduct additional research and inquiry about the customer, which in the extreme might include engaging a third party to investigate the client. EDD also may include, but not be limited to, obtaining the following information:

- Occupation or nature of business
- Purpose of account
- Expected pattern of activity in the account in terms of transaction types, dollar volume and frequency
- Expected origination and destination of funds
- Articles of incorporation, partnership agreements and business certificates
- Understanding of the customer's customers (particularly in the case of foreign correspondent banks and international businesses)
- Identification of the nominal and beneficial owners of accounts (particularly in the case of private banking clients and foreign correspondent banks)
- Details of other personal and business relationships the customer maintains
- Details of other banking relationships the customer maintains
- Approximate salary or annual sales
- Additional sources of income
- Description/history of source of wealth
- Net worth
- Annual reports, financial statements (audited if available)
- AML policies, procedures and controls (in the case of foreign correspondent banks, money services businesses [MSBs] and other nonbank financial institutions)
- Third-party documentation, such as bank references and credit reports
- Local market reputation through review of media reports or other means
- Copies of any correspondence with client (e.g., letters, faxes, e-mails), including call reports/site visits
- Proximity of the residence/employment/place of business to the financial institution

763. Is there a difference between expected activity and average activity?

Expected activity describes anticipated activity from a particular customer or account type, including types, amounts, geographical locations where transactions are done and frequencies of transactions. Average activity describes the mean activity historically conducted by a customer through an account. Expected activity provides a narrative for the types of activities that are deemed normal for a particular customer or account. When due diligence is accurate, expected activity and average activity are consistent.

Understanding both expected and average activities are extremely important in detecting potentially suspicious activity.

764. How can a financial institution determine "normal" expected activity for each of its customers?

Expected activity can be obtained directly from each customer during the account opening process or developed independently by the financial institution based on historical transaction history for segments of its customer population or from other information.

For example, some financial institutions ask for the following information directly from their customers during the account opening process:

- Deposits/credits per month (number and volume)
- Withdrawals/debits per month (number and volume)
- Cash transactions (number and volume)
- Wire transfer transactions (number and volume)
- Purpose of account

- Origination/destination country(ies) of incoming/outgoing wire transfers or other types of payments

To facilitate the account opening process, some financial institutions provide ranges of activity with triggers to ask for additional information if specified dollar thresholds are met or higher risk activities are identified. It is important to note that although customers may answer these questions to the best of their ability, their responses are often guesstimates and may need to be reviewed and revised throughout the duration of the relationship.

Expected activity can also be obtained by analyzing underlying transaction activity based on defined segments, including, but not limited to, the following:

- Customer type (e.g., business, individual)
- Geography (e.g., home address, place of business)
- Nature of business/occupation
- Account type (e.g., savings, checking, certificate of deposit, loan, etc.)
- Account balance
- Transaction volume

For example, some financial institutions have opted to segment their customer population by customer type, geography (foreign/domestic) and class based on volume of transaction activity and balances held in their accounts to establish expected activity. In some cases, these expected activity profiles were used to compare actual transaction activity in suspicious transaction monitoring software. Typically, this due diligence is used to conduct customer risk assessments and provide context for investigations.

765. Is obtaining the occupation the same as identifying the source of income?

Typically, the source of most people's income is from their occupation. However, the source of income may be unclear if a customer responds to this question with any of the following:

- Self-employed
- Unemployed
- Housewife/househusband
- Student
- Retired

Additionally, some customers may have sources of income beyond their jobs.

766. Are there other types of customers that may present additional KYC challenges?

Yes. KYC challenges may arise with the following customer types:

- **Doing Business As (DBAs)** – In some cases, customers use personal accounts for their DBAs, and either commingle personal and business activities or simply use personal accounts for business purposes. This makes it difficult for financial institutions to collect the appropriate due diligence at the inception of the relationship and to monitor for potentially suspicious transactions on an ongoing basis.
- **Professional service providers (e.g., attorneys)** – Financial institutions should distinguish between accounts opened by professional service providers for personal use versus accounts established for business when conducting due diligence and evaluating risk. These types of customers can pose challenges when attempting to identify the source of income and, where applicable, the beneficial owners of funds/assets in these accounts, especially depending on how client funds are managed. For additional guidance, please refer to the Professional Service Provider section.
- **Charitable organizations** – A charitable organization may state its mission or status as a not-for-profit when asked to provide "nature of business." The challenge with charitable organizations is in understanding their sources of income, which ultimately speaks to understanding their donor base. For additional guidance, please refer to the Charitable Organizations and Nongovernmental Organizations section.
- **Trusts** – Similar to charitable organizations, many of the standard due diligence questions for businesses (or non-personal customer types) do not apply to trusts (e.g., source of income, nature of business). Many financial

institutions have separate trust department to manage these types of customers. For additional guidance, please refer to the Trust and Asset Management Services section.

767. What are some examples of "purpose of account"?

For individuals, common responses to the question of "purpose of account" include, but are not limited to, the following:

- Daily living expenses
- Savings (e.g., college, retirement, vacation)

For businesses, common responses include, but are not limited to, the following:

- Payroll
- Operating account
- Manage treasury activities

The challenge is obtaining a meaningful response that will aid financial institutions in understanding what types of transaction activities can be expected in their customers' accounts. Some financial institutions have gone as far as asking for the purpose of specific transactions, particularly in the case of international wire transfers. While it is common practice to ask for the purpose with lending products, it has not been consistently applied with other product types.

768. Does compliance with Section 312 of the USA PATRIOT Act satisfy a financial institution's EDD requirements?

Section 312 covers additional information required for foreign correspondent accounts, private banking accounts and politically exposed persons (PEPs). A financial institution's EDD requirements should cover all types of customers and accounts that it deems to pose higher risk (e.g., money services businesses [MSBs], trusts, private investment companies [PICs]), not just correspondents, private banking and PEPs. Detailed guidance specific to select high-risk customers have been provided in this publication for the following:

- Politically exposed persons
- Foreign embassies and consulates
- Private banking
- Professional service providers
- Trust and asset management service providers
- Business entities (e.g., shell companies, private investment companies, etc.)
- Correspondent banking
- Charitable organizations
- Third-party payment processors
- Owners of privately owned automated teller machines (ATM)

For additional information and guidance issued on EDD for these specific types of customers, please refer to the High Risk Customers section.

769. Should an institution simplify its KYC program by performing EDD on all of its customers?

Unless a financial institution operates a mono-line business where all of its customers are deemed to be high-risk (e.g., private banking), conducting EDD on all customers may create an unnecessary burden and possibly undermine the purpose of a risk-based AML program. Even in a mono-line private banking business, some customers, by nature of the types of accounts they have or the transactions they conduct, may be lower risk than others.

770. When should a financial institution collect CDD and EDD information?

Some financial institutions obtain CDD and EDD information (when necessary) during the account-opening process, while others choose to obtain CDD and EDD information afterwards to streamline the account-opening process.

771. Where should the information obtained during the CDD and EDD processes be stored?

Storing CDD and EDD information as paper files or images may limit the ability to use critical information, such as occupation or expected activity. Housing CDD and EDD information in an electronic format, such as an automated risk assessment or transaction monitoring system, however, allows it to be queried and updated and, increasingly, regulators are suggesting, at least for larger financial institutions, that customer information should be maintained electronically. For additional guidance on AML technology relating to customer databases, customer risk assessment and suspicious transaction monitoring systems, please refer to the AML Technology section.

772. Should a financial institution update CDD and EDD after the initial account-opening process?

Customer due diligence (CDD) and enhanced due diligence (EDD) should be updated if there are significant changes to the customer's profile (e.g., volume of transaction activity, risk level, account type). For example, if the customer's transaction profile indicates that the customer is expected to conduct an average of six transactions per month in an amount of $20,000 each, and then the customer's transaction size and frequency increase to 20 transactions for an average of $100,000 per month, the financial institution should seek to understand the reason for the change in transaction activity. Once the financial institution has satisfied itself that it has obtained a reasonable explanation, this information should be used to update the customer's profile. For example, a customer's employment status may change from student to professional, thereby changing the expected level and type of activity in his or her account. If the financial institution is not able to satisfy itself that the change is reasonable, then it needs to determine if a SAR must be filed and if any other actions, which may include termination, are appropriate.

Updating the customer's CDD and EDD can enable a financial institution to better direct its monitoring and investigation efforts. An up-to-date customer profile can help avoid having transactions flagged unnecessarily, thus enabling the financial institution to devote time to those transactions that need to be investigated.

Beyond updates prompted by a financial institution's monitoring activities, financial institutions should review accounts periodically to identify any changes in profile. The frequency and nature of this review should be based on the customer's risk rating.

773. What is expected of an effective CDD program under FinCEN's March 5, 2012 advanced notice of proposed rulemaking (ANPR) on "Customer Due Diligence Requirements for Financial Institutions"?

FinCEN's ANPR identifies the following as parts of an effective CDD program:

- Conducting initial due diligence on customers, including identifying the customer and verifying that customer's identity as appropriate on a risk basis, at the time of account opening;
- Understanding the purpose and intended nature of the account and expected activity associated with the account for the purpose of assessing risk and identifying and reporting suspicious activity;
- Identifying the beneficial owner(s) of all customers and verifying the beneficial owner(s)' identity pursuant to a risk-based approach; and
- Conducting ongoing monitoring of the customer relationship and conducting additional CDD as appropriate, based on such monitoring and scrutiny, for the purposes of identifying and reporting suspicious activity.

774. To what types of entities would the requirements of the "Customer Due Diligence Requirements for Financial Institutions" ANPR apply?

Currently, the ANPR would apply to the following types of entities:

- Banks
- Broker or dealers in securities
- Mutual funds

- Futures commission merchants (FCM) and introducing brokers (IB) in commodities

FinCEN is also seeking comment on whether the scope of the proposed rule should be expanded to include the following types of entities:

- Money services businesses (MSB)
- Providers of prepaid access
- Insurance companies
- Casinos and card clubs
- Dealers in precious metals, stones and jewels
- Non-bank mortgage lenders or originators

775. How is "beneficial owner" defined in the "Customer Due Diligence Requirements for Financial Institutions" ANPR?

The ANPR is considering the following as a limited definition of beneficial ownership:

- Either:
    - Each of the individual(s) who, directly or indirectly, through any contract, arrangement, understanding, relationship, intermediary, tiered entity, or otherwise, owns more than 25 percent of the equity interests in the entity; or
    - If there is no individual who satisfies the above, then the Individual who, directly or indirectly, through any contract, arrangement, understanding, relationship, intermediary, tiered entity, or otherwise, has at least as great an equity interest in the entity as any other individual; and
- The individual with greater responsibility than any other individual for managing or directing the regular affairs of the entity.

776. Does the "Customer Due Diligence Requirements for Financial Institutions" ANPR prescribe a set percentage for beneficial ownership?

The ANPR suggests more than 25 percent of equity interest, or the individual with the most equity interest if no one meets the 25 percent threshold.

777. Is there any *de mininis* exclusion for accounts for complying with the requirements of the "Customer Due Diligence Requirements for Financial Institutions" ANPR?

No, as drafted, there is no threshold. The requirements would apply to accounts of covered institutions of all types and sizes.

778. What input is FinCEN seeking before it finalizes the "Customer Due Diligence Requirements for Financial Institutions" rule?

In its ANPR, FinCEN has requested comments on the following:

- Scope of applicability to more types of financial institutions (e.g., money services businesses; providers of prepaid access; insurance companies; casinos; dealers in precious metals, stones and jewels; non-bank mortgage lenders or originators)
- Definition of beneficial ownership, its application and possible exemptions (e.g., based on risk and/or red flags, applicability to existing customers and customers currently exempt from CIP requirements, exemptions based on particular product or customer type, beneficial ownership of accounts versus assets held in accounts, etc.)
- Procedures for obtaining and verifying beneficial ownership information (e.g., requiring statements at account opening that the customer is not acting on behalf of another person or entity, verification of status versus identity of beneficial owners, difficulties associated with obtaining beneficial ownership in accounts held by intermediaries or foreign legal entities, etc.)

Additionally, FinCEN has been holding roundtables and discussions with the industry on key issues covered by the ANPR.

779. What new obligations will "Customer Due Diligence Requirements for Financial Institutions" rule, if enacted, impose on covered financial institutions?

Currently, covered financial institutions are required to obtain beneficial ownership in the following situations as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

The ANPR could categorically require all financial institutions subject to AML program requirements to identify, and in some instances verify, beneficial ownership of all of its account holders. The ANPR would also impact the OFAC and sanctions program of financial institutions, as beneficial owners would be subject to screening against required Sanctions listings to the extent that financial institutions are not screening beneficial owners today.

For further guidance on due diligence requirements for private banking and correspondent banking customers, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Private Banking and Correspondent Banking. For further guidance on sanctions requirements, please refer to the Office of Foreign Assets Control and International Government Sanctions Program section.

Beneficial Owners

780. What is a "beneficial owner"?

A "beneficial owner" generally is someone (an individual or a business) who has a level of control over, or entitlement to the funds or assets in the account that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the account. The ability to fund the account or the entitlement to the funds of the account alone, without corresponding authority to control, manage or direct the account, such as an account in which a minority age child is the beneficiary, does not cause an individual to become a beneficial owner.

The term reflects a recognition that a person in whose name an account is opened is not necessarily the person who ultimately controls such funds or who is ultimately entitled to such funds. "Control" or "entitlement" in this context is to be distinguished from mere legal title or signature authority.

FinCEN's ANPR on "Customer Due Diligence Requirements for Financial Institutions" considers the following as a limited definition of beneficial ownership:

- Either:
    - Each of the individual(s) who, directly or indirectly, through any contract, arrangement, understanding, relationship, intermediary, tiered entity, or otherwise, owns more than 25 percent of the equity interests in the entity; or
    - If there is no individual who satisfies the above, then the Individual who, directly or indirectly, through any contract, arrangement, understanding, relationship, intermediary, tiered entity, or otherwise, has at least as great an equity interest in the entity as any other individual; and
- The individual with greater responsibility than any other individual for managing or directing the regular affairs of the entity.

781. Where the ultimate account holder is a corporation, is there any guidance for determining who the actual beneficial owners are?

Both the third European Union (EU) Money Laundering Directive and the 2007 United Kingdom (U.K.) Money Laundering Regulations provide additional guidance on who qualifies as a beneficial owner, generally tying beneficial ownership to ownership or control of more than 25 percent of voting rights or the natural person(s) who exercises control over 25 percent or more of the property of a legal arrangement or entity.

FinCEN's ANPR on "Customer Due Diligence Requirements for Financial Institutions" suggests more than 25 percent of equity interest, or the individual with the most equity interest if no one meets the 25 percent threshold.

782. Do beneficial owners include anyone who can fund or is entitled to the funds in an account?

No, the ability to fund an account, or the mere entitlement to the funds in an account without corresponding control over the account, does not result in beneficial ownership. For example, a minor child who is the beneficiary of an account established by her parents is not a beneficial owner.

783. What are the money laundering risks of beneficial ownership?

By using nominal account names rather than disclosing the true owners of the funds, money launderers and other criminal elements can conceal the source, purpose or actual ownership of funds.

784. What are a financial institution's obligations with respect to identifying beneficial ownership?

Currently, covered financial institutions are required to obtain beneficial ownership in the following situations as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

FinCEN's ANPR "Customer Due Diligence for Financial Institutions" could categorically require all covered financial institutions subject to AML program requirements to identify, and in some instances verify, the beneficial ownership of its account holders. It also clarifies existing AML obligations for financial institutions. For further guidance on due diligence requirements for private banking and correspondent banking customers, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Private Banking and Correspondent Banking.

785. What other concerns should financial institutions consider when maintaining accounts for beneficial owners?

Another potential risk to financial institutions that maintain accounts for beneficial owners is that they may unknowingly be doing business with individuals or entities who/that are on government sanctions lists. Or, they may fail to obtain other records or file reports required by the Bank Secrecy Act, such as Currency Transaction Reports (CTRs).

786. Are bearer shares a type of beneficial ownership?

Yes, bearer shares, which are negotiable instruments that accord ownership in a corporation to the person who possesses the bearer share certificate, are a type of beneficial ownership. Because bearer shares are negotiable, they create additional risk for financial institutions because beneficial ownership changes if the bearer share certificate is transferred to another party.

787. What specific CDD procedures can financial institutions use to identify beneficial owners?

Financial institutions may consider, among others, the following CDD procedures for identifying beneficial owners:

- Asking customers whether they are acting on behalf of another person and, if so, obtaining information on whose behalf the customer is acting and why, and/or requiring customers to certify they are acting on their own behalf
- For non-publicly traded companies and customers such as private investment companies (PICs), trusts and foundations, requiring information on the structure and ownership of the customer
- Where the customer is a trustee, requiring information about the trust structure, the provider of funds, and any persons or entities who/that have control over the funds or have power to remove the trustees
- For bearer share accounts, requiring the account holders to provide notice to the financial institution if the bearer share certificate is transferred to another party

Financial institutions should consider implementing such policies and procedures on an enterprise-wide basis, which may include sharing or obtaining beneficial ownership information across business lines, and across separate legal entities in the enterprise and affiliated support units. The Guidance notes that AML staff may find it useful to crosscheck for beneficial ownership information in data systems maintained by the financial institution for other

purposes, such as credit underwriting or fraud detection. Additionally, as appropriate, beneficial owners should be subject to EDD. This would include, for example, PICs, shell companies, Special Purpose Vehicles (SPVs) and instances where the beneficial owners include politically exposed persons (PEPs). For additional guidance on PICs, shell companies and SPVs, please refer to the sections: Business Entities: Shell Companies and Private Investment Companies, Politically Exposed Persons.

788. What types of questions should financial institutions ask to determine the legitimacy of different vehicles used or entities controlled by beneficial owners?

Financial institutions may consider the following types of questions:

- What is the purpose of the structure or vehicle?
- Who are the underlying beneficial owners?
- In what jurisdiction is it established and why?
- When was the structure or vehicle set up?
- Is the jurisdiction one that is of high risk to money laundering?
- What kind of activity will be conducted by the entity or vehicle?
- What type of activity will be conducted through the financial institution?
- Where applicable, what is the reason why the same beneficial owners are behind multiple legal entities or vehicles?
- Do the answers provided to the questions above make sense?

789. What guidance has been issued related to the risks of beneficial ownership and expected industry procedures?

Myriad guidance has been issued on the risks of beneficial ownership and expected industry procedures. Examples include:

- **Guidance on Obtaining and Retaining Beneficial Ownership Information** (2010) by the Financial Crimes Enforcement Network (FinCEN), the Federal Reserve, Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS) and the Securities Exchange Commission (SEC)
- **Customer Due Diligence Requirements for Financial Institutions** (2012) by FinCEN
- **Advisory – Potential Money Laundering Risks Related to Shell Companies** (2006) by FinCEN
- **FAQs on Beneficial Ownership** (2012) by the Wolfsberg Group
- **FAQs on Intermediaries** (2012) by the Wolfsberg Group
- **The Misuse of Corporate Vehicles, Including Trust and Company Service Providers** (2006) by the Financial Action Task Force (FATF)
- **Behind the Corporate Veil – Using Corporate Entities for Illicit Purposes** (2001) by the Organisation for Economic Co-operation and Development (OECD)
- **Identification of Ultimate Beneficiary Ownership and Control of a Cross-Border Investor** (2007) by the Organisation for Economic Co-operation and Development (OECD)
- **Principles on Client Identification and Beneficial Ownership for the Securities Industry** (2004) by the International Organization of Securities Commissions (IOSCO)
- **The Role of Domestic Shell Companies in Financial Crime and Money Laundering: Limited Liability Companies** (2006) by FinCEN

Know Your Employee

790. Should CDD and EDD standards for customers be applied to the employees of financial institutions as well?

In addition to screening new employees during the standard hiring process, financial institutions should consider conducting ongoing due diligence and EDD on employees in positions perceived to have greater exposure to money laundering (e.g., relationship managers of private banking or institutional clients). Additionally, the history of an employee's investigations and reports of potentially suspicious activity should be noted. For instance, a general reluctance to report suspicious activity should serve as a red flag to an institution to monitor closely client relationships associated with the employee in question. A financial institution should consult with its counsel on how to conduct such due diligence and to help ensure labor laws are not violated.

Knowing both customers and employees and creating a strong internal referral and transaction monitoring (as allowed by law) system for potentially suspicious activity will help mitigate the risk of a financial institution being used for money laundering or terrorist financing.

791. Should CDD and EDD exceptions be made for senior management or owners of the financial institution?

No. CDD and EDD standards should be applied to all employees of a financial institution, regardless of status or position within the financial institution.

792. What additional risks do employees of the financial institution pose?

As a result of their access, employees pose considerable risks related to insider abuse (e.g., the ability to override or manipulate CTRs and SARs, the utilization of knowledge regarding the AML policies and procedures to evade controls designed to prevent money laundering and terrorist financing).

Accordingly, CDD and EDD standards should be applied to all employees of a financial institution, regardless of status or position within the financial institution.

Know Your Third Parties

793. Apart from customers and employees, are there other parties whose performance could jeopardize an AML Compliance Program?

Yes. The following parties, among others, could jeopardize an AML Compliance Program:

- **Other financial institutions relied upon to support the AML Compliance Program** (e.g., Customer Identification Program [CIP], sanctions screening) may not adequately execute their AML or OFAC sanctions review and responsibilities consistent with regulatory and/or internal standards.
- **Companies providing products/services, such as insurance products, to the financial institution's customers** may not identify risk or monitor activity adequately for potentially suspicious activity.
- **Companies that offer a financial institution's products to its customers and employees**, such as prepaid access program managers, may not adequately oversee the AML program and internal controls.
- **Companies, such as deposit brokers, referring customers to a financial institution** may not conduct adequate due diligence on acquired customers.
- **Third-party payment processors** (e.g., remote deposit capture [RDC] service providers or gateway processors) may not identify and manage AML risks appropriately.
- **Agents** of money services businesses (MSBs) may not appropriately manage AML risk and may expose an MSB to reputational risk as well as legal risk.
- **Vendors** (e.g., AML technology providers, consultants conducting independent tests of the AML Compliance Program) may provide products/services that fail to meet a financial institution's requirements or needs.

794. What can financial institutions do to mitigate third-party risk?

Financial institutions should conduct due diligence and ongoing monitoring of third-party relationships to mitigate third-party risk, including, but not limited to, the following:

- Limiting business to service providers that have an established relationship with the financial institution or other trusted entity or are referred from highly respected sources
- Conducting background checks on service providers, including a review of all products/services offered, methods of soliciting new clients, licensing, regulatory obligations and reputation (e.g., customer complaints)
- Performing sanctions screening on service providers, their owners and principal officers
- Reviewing the AML Compliance Program, where applicable, for adequacy and consistency with internal policies and procedures (e.g., due diligence and monitoring conducted on acquired customers, merchants, agents)
- Monitoring activity originated from the third party, where applicable, for common red flags or potentially suspicious activity that may suggest inattention or inadequacies in the third party's own compliance program or contractual obligations

For further guidance on managing third-party risk, please refer to the following sections: Nondeposit Investment Products, Deposit Broker, Third-Party Payment Processors, Remote Deposit Capture, Money Services Businesses, Agents and Unlawful Internet Gambling Enforcement Act.

795. Can a financial institution rely upon a third party to conduct all or part of the financial institution's CIP?

Yes. A financial institution may rely on another federally regulated institution to conduct all or part of the financial institution's Customer Identification Program (CIP). Such reliance is permitted only when all of the following apply:

- Such reliance is reasonable.
- The other financial institution is regulated by a federal functional regulator.
- The other financial institution is subject to a general Bank Secrecy Act (BSA) compliance program requirement.
- The other financial institution shares the customer with the financial institution.
- The two institutions enter into a reliance contract.

796. What obligations are imposed upon third parties that conduct part or all of the financial institution's CIP?

The financial institution conducting the CIP must provide an annual certification that it has implemented its AML program and that it will perform (or its agent will perform) the specified requirements of the financial institution's CIP.

For additional guidance on CIP, please refer to Section 326 – Verification of Identification.

797. Can financial institutions rely on third parties for other elements of an AML program beyond CIP (e.g., suspicious activity reporting)?

Financial institutions may outsource other elements of their AML programs (e.g., monitoring, collection and verification of customer information, OFAC screening, 314(a) searches) to third parties (e.g., car dealers who accept loan applications on behalf of a bank or technology service providers). In these instances, financial institutions cannot rely on the third parties in the same manner as they may if they delegate elements of their CIP programs to regulated financial institutions. Rather, financial institutions that do outsource parts of their AML program to a third party must do the following:

- Ensure they have obtained a written agreement for the services to be performed by the service provider and that the terms of the agreement meet the financial institution's requirements.
- Monitor the third party's performance under the contract on a continuing basis.
- Conduct adequate due diligence on the third party's AML program and/or its understanding of AML requirements.
- Perform adequate due diligence of the third party's operations on a periodic basis.

It is important to note that the institution is ultimately responsible for its compliance with AML requirements, whether or not it relies upon a third party.

798. Should third-party service providers be included in the independent testing requirement of an AML program?

Third-party service providers are required to comply with the CIP rule and maintain an AML program, and may not, in many circumstances, need to be included in the independent testing of a financial institution's AML program because these companies are themselves subject to regulatory examination. For other third-party service providers, the independent test should consider how the financial institution conducted its due diligence of the third party and how it assures itself that the third party is meeting its obligations effectively on a continual basis.

799. What guidance has been issued on third-party service providers (TPSP)?

The following are examples of guidance that has been issued on third-party service providers:

- **Third-Party Payment Processors – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 17: Reliance on Third Parties** (2012) by the Financial Action Task Force (FATF)
- **Retail Payment Systems** and **Wholesale Payment Systems Booklet** (2004) within the FFIEC Information Technology Examination Handbook by the FFIEC
- **Third-Party Senders and the ACH Network: An Implementation Guide** (2012) by The Electronic Payments Association (NACHA) (formerly National Automated Clearing House Association)
- **Bank Use of Foreign-Based Third-Party Service Providers** (2002) by the Office of the Comptroller of the Currency (OCC)
- **Risk Management Principles for Third-Party Relationships** (2001) by the OCC
- **Payment Processor Relationships** (2012) by the Federal Deposit Insurance Corporation (FDIC)
- **Guidance on Managing Third-Party Risk** (2008) by the FDIC

RISK ASSESSMENTS

Overview

The Risk Assessments section covers the definitions of the following key risk assessments that are expected to be executed by most financial institutions:

- Enterprise-wide risk assessment
- Business line risk assessments
- Customer risk assessments
- Office of Foreign Assets Control (OFAC) risk assessments

800. What is a risk assessment?

There are different types of risk assessments. One type measures (a) the inherent risks in a business and/or processes; (b) the strength of current controls and any noted gaps in the compliance program; and (c) the residual risk of a business and/or processes. Another may only measure inherent risk in order to later develop controls to mitigate those specific risks.

801. What is inherent risk?

Inherent risk is the risk to an entity in the absence of any actions management might take (e.g., controls) to alter either the risk's likelihood or impact.

802. What is a control?

A control is a process, designed and/or performed by an entity, to mitigate or reduce the likelihood or impact of a risk. Control processes may be manual, automated, proactive and/or reactive.

In terms of a financial institution's AML program, the following are examples of controls:

- The financial institution sets a policy prohibiting the offering of products/services to a particular type of customer (e.g., money services businesses).
- Supervisors or managers review and approve a documentation checklist, completed by an account officer, prior to account opening, as a control to ensure the necessary customer information is collected according to the financial institution's policies and procedures.
- The financial institution's systems require the input of necessary customer information before the account officer can proceed to the account opening screen as an automated control to ensure the necessary customer information is collected according to the financial institution's policies and procedures.
- The financial institution utilizes an automated monitoring system to detect potentially suspicious activity.

803. What is residual risk?

Residual risk is the risk remaining after all controls have been applied to reduce the likelihood or impact of the risk. An acceptable level of residual risk is determined by the risk appetite or tolerance of the financial institution.

804. Are financial institutions required to conduct risk assessments?

Financial institutions are expected to develop and maintain risk-based compliance programs. This requires that they conduct risk assessments. Bank regulators, in particular, expect the financial institutions they supervise to conduct, among others:

- Business line risk assessment
- Customer risk assessment
- OFAC risk assessment
- Enterprise-wide risk assessment

805. Who should be responsible for designing the risk assessment methodology?

A risk assessment methodology engages senior management, business or process owners, and compliance personnel. Compliance should develop the risk assessment methodology with input from the business or process owners; senior management should review and approve the methodology.

806. Who should be responsible for conducting risk assessments?

A risk assessment should engage the business and process owners (i.e., the people who best understand the business and/or processes). Compliance should, however, review and approve business- or process-owner-assigned ratings. Results of the risk assessment should be presented to an institution's board of directors.

807. Is the risk assessment for money laundering and terrorist financing the same?

No. Although some risk factors and red flags that apply to other types of money laundering also may apply to terrorist financing, the patterns of activity tend to be very different. Terrorist financing often involves very small amounts of funds that may be moved through charities or nontraditional banking systems, whereas other types of money laundering may involve large volumes of funds. It is important to understand the different patterns to assess risks.

808. Do any customer types, products, services or transactions pose zero risk of money laundering or terrorist financing?

No. Every customer type, product, service or transaction poses some degree of risk to money laundering and terrorist financing; therefore, it is recommended that "zero" not be used when assigning risk to customer types, products, services and transactions. However, some customers, products, services and transactions may pose only a very minimal risk, such as a customer who performs a one-time, low-dollar amount transaction or who only has direct deposits of payroll and performs only low-dollar transactions.

809. Should a financial institution reduce the inherent risk score of a high-risk customer type, product, service or transaction to moderate or low if it has significant familiarity with that customer type, product, service or transaction?

No. The scale used to assign risk to customer types, products, services and transactions should be an absolute scale, not a relative scale particular to the financial institution. The inherent risks of customer types, products, services and transactions do not vary by financial institution or region. A financial institution's familiarity with a particular type of customer, product, service or transaction should factor into adjusting the residual risk by implementation of appropriate controls, not into adjusting the inherent risk.

For example, if a financial institution has a significant number of money services businesses (MSBs), the inherent risk of its customer base will be higher. However, due to the financial institution's substantial experience with MSBs and its enhanced due diligence (EDD) and monitoring program, its residual risk may be lower. It would be unacceptable for the financial institution to reduce the risk associated with MSBs from high to moderate or low, as the industry standard designates MSBs as high-risk. However, the financial institution may incorporate additional risk factors to differentiate the risk of its MSBs (e.g., consider product/service offerings of the MSB, geography of operations).

810. What guidance has been provided on risk assessments?

The FFIEC BSA/AML Examination Manual provides guidance for banks with respect to the identification of specific risk categories, the level of detail of the analysis of specific risk categories, the impact of the risk assessment on the organization's AML program, the recommended frequency with which the assessment should be conducted and the

circumstances prompting an organization to update its risk assessments. However, it does not dictate the format the risk assessment should take.

Additional resources include, but are not limited to, the following:

- **Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing** (2007) by the Financial Action Task Force (FATF)
- **FATF Recommendation 1: Assessing Risks & Applying a Risk-Based Approach** (2012) by the Financial Action Task Force (FATF)
- **Guidance for Dealers, Including Certain Retailers, of Precious Metals, Precious Stones, or Jewels, on Conducting a Risk Assessment of Their Foreign Suppliers** (2008) by the Financial Crimes Enforcement Network (FinCEN)
- **Guidance on a Risk-Based Approach for Managing Money Laundering Risks** (2006) by the Wolfsberg Group
- **Money Laundering and Terrorist Financing Risk Assessment Strategies** (2008) by FATF
- **Risk-Based Approach for Casinos** (2008) by FATF
- **Risk-Based Approach Guidance for Legal Professionals** (2008) by FATF
- **Risk-Based Approach for the Life Insurance Sector** (2009) by FATF
- **RBA Guidance for Trust and Companies Service Providers (TCSPs)** (2008) by FATF
- **RBA Guidance for Real Estate Agents** (2008) by FATF
- **RBA Guidance for Accountants** (2008) by FATF
- **RBA High-Level Principles and Procedures for Dealers in Precious Metals and Dealers in Precious Stones** (2008) by FATF
- **Guidance for Money Services Businesses – Risk-Based Approach** (2009) by FATF
- **Risk Matrix for Financial Institutions** (2005) by the Office of Foreign Assets Control (OFAC)
- **Risk Matrix for the Securities Sector** (2008) by OFAC
- **Risk Matrix for the Charitable Sector** (2007) by OFAC

Enterprise-wide Risk Assessment

811. What is an enterprise-wide risk assessment?

An enterprise-wide risk assessment is an exercise intended to identify systemic money laundering risk that may not be apparent in a risk assessment focused on a business line or other assessment unit. In other words, it is the big picture view of an organization's money laundering risks that aggregates the results of other risk assessment exercises.

812. Why are enterprise-wide risk assessments important?

Enterprise-wide risk assessments may disclose systemic money laundering risk that is not otherwise apparent. For example, multiple business lines may note certain money laundering risk, but conclude that the risk is not high for the business line. When aggregated across the organization, however, the perception of such risk and the need to better manage it might take on greater significance.

813. How frequently should enterprise-wide risk assessment be performed?

Enterprise-wide risk assessments should be performed annually or when any material changes occur in other risk assessments performed by the organization.

Business Line Risk Assessment

814. What is a business line risk assessment?

A business line risk assessment is an exercise that attempts to identify each business line's level of vulnerability to money laundering and terrorist financing risk. This is accomplished by evaluating, for a specific business line, among other factors, the inherent risk of products/services, the customer base (e.g., type, location) and geography (e.g., customers, transactions, operations) at a macro level and the controls (e.g., policy and procedures, customer acceptance and maintenance standards, transaction monitoring, management oversight, training, personnel) mitigating those risks at the business line level.

Results of business line risk assessments then can be aggregated to provide an enterprise-level assessment of the financial institution's AML risks and controls. Business line risk assessments are sometimes referred to as AML risk assessments.

815. What are the typical components of a business line risk assessment methodology?

A typical business line risk assessment methodology addresses inherent risks and mitigating controls. Inherent risk includes the risks posed by the customer base, products/services/transactions, and geographic footprint (e.g., customers, transactions, operations) of the financial institution. Controls or the control environment can include the customer acceptance and maintenance program, the transaction monitoring program, training, and management oversight (e.g., compliance, audit, senior management, board of directors).

Residual risk is then determined by netting the level of risk (e.g., high, moderate, low) against the strength of the control and control environment (e.g., strong, moderate, low).

816. What is the difference between a business line risk assessment and a customer risk assessment?

A business line risk assessment assesses money laundering and terrorist financing risk on an enterprise or macro level. A customer risk assessment, as discussed in the following Customer Risk Assessment section, assesses money laundering and terrorist financing risk on a customer level. The customer risk assessment results can be used to support the business line risk assessment (e.g., to understand risks of the customer base overall). The business line risk assessment assists Compliance with developing the overall AML Compliance Program, whereas the customer risk assessment assists with allocating AML resources to the customers who/that pose the highest risk to the financial institution.

817. How should the business line risk assessment be conducted?

The method used to conduct the business line risk assessment will depend on the complexity of the financial institution and the technology support available to the organization. A combination of methods (e.g., questionnaires, internally or externally developed databases, web-based applications) often is used to collect the business line information effectively. These methods should enable Compliance to review and validate the risk assessment results and engage in discussions with business line management to discuss the final risk rating and ensure business line management understands the money laundering and terrorist financing risk in the business line.

818. Should all business lines of a financial institution be included in the business line risk assessment?

The business lines included in the business line risk assessment will vary by organization; however, all business lines providing products and services to customers or supporting customer transactions (e.g., deposit or wire operations) should be included in the business line risk assessment to ensure no potential area of risk is overlooked. Business lines with risk management functions (e.g., customer acceptance, monitoring) should be included to ensure all controls/control environments are assessed.

819. How often should a business line risk assessment be conducted?

At a minimum, business line risk assessments should be conducted annually. Additionally, the business line risk assessment methodology should be reassessed when new products or services are introduced, with each merger/acquisition, or when new markets are targeted (e.g., type of customer, country of domicile of customer).

820. Should a financial institution be concerned if many of its business lines result in a high inherent risk rating?

An institution should be concerned if there are nonexistent or ineffective controls to mitigate the high inherent risk.

821. Should a financial institution use the same business line risk assessment methodology to assess each of its business lines?

In general, it is recommended that a financial institution use the same methodology to assess the risks and controls of its business lines to ensure that risk is measured consistently across the institution.

Business lines have flexibility in their response to the risks identified in the assessment. For example, one business line may have a higher risk appetite/tolerance than another business line and, therefore, may choose to implement more limited controls to mitigate these risks.

822. What are the most common gaps with business line risk assessments?

The most common gaps with business line risk assessments include, but are not limited to, the following:

- The methodology does not identify and/or quantify, in whole or partially, all inherent risk factors.
- The methodology does not identify and/or assess, in whole or partially, all controls/control environments.
- The methodology does not calculate residual risk.
- A consistent methodology is not used by each business line.
- The classifications of high, moderate and/or low risk are inconsistent with leading practices.
- Only the results, and not the methodology itself, are documented.
- The results of the executed methodology are not used to drive strategic changes in the AML Compliance Program.
- The results are not current.
- The methodology is not current.
- There is a lack of or inadequate training on the purpose of the assessment and the meaning of the results with compliance personnel, business line management and senior management.
- There is over-reliance on a third party to develop and execute the assessment.

Customer Risk Assessment

823. What is a customer risk assessment?

A customer risk assessment is a process that identifies the level of money laundering and terrorist financing risk inherent in a financial institution's customer base.

824. When should a customer risk assessment be conducted?

Customer risk assessments typically are conducted at the inception of each new client relationship, based on information provided during the account-opening process. Some institutions initially flag a customer as new, but defer conducting the assessment for a short period (e.g., three months) to include actual transaction activity as a factor in the assessment.

While some believe it is more advantageous to conduct the customer risk assessment at the inception of the relationship, others argue that a customer risk assessment is more meaningful if it includes actual transaction activity as a factor as opposed to just theory (e.g., expected transaction activity). In either instance, customers should be assessed continually throughout the duration of the relationship.

825. Are financial institutions required to implement a customer risk assessment?

The risk assessment guidance provided in the FFIEC BSA/AML Examination Manual cautions financial institutions not to "define or treat all members of a specific category of customer as posing the same level of risk." Further guidance is provided to consider other customer-specific risk factors to assess customer risk. Leading practice dictates all financial institutions should have a customer risk assessment methodology in place.

826. How is a customer risk assessment used?

Customer risk assessments are used to determine the extent of due diligence for each customer (e.g., requiring provision of additional information, site visits, senior management approvals, reviews of profiles) and the scope and frequency of monitoring.

827. How should a customer risk assessment be conducted?

Risk assessment methodologies can be implemented using automated or manual processes. Automating customer risk assessments (e.g., as part of the account-opening platform, transaction monitoring system, back-end system) promotes consistency and objectivity in the process. Some institutions have implemented procedures whereby risk ratings are produced automatically based on the information provided in the account-opening process. In some institutions, the responsible account officer will assign the initial risk rating, and Compliance will review and approve the rating, either for all new customers, high-risk customers or on a sample basis.

If automated risk ratings are used, financial institutions should ensure they are updatable, particularly when the customer profile changes after the account-opening process.

For additional information on automating the customer risk assessment methodology, please refer to the AML Technology section.

828. What factors should financial institutions consider in their customer risk assessment methodology?

Financial institutions should consider the following factors, as applicable, when assessing the money laundering and terrorist financing risk of customers:

- Occupation or nature of business
- Method/channel of account opening (e.g., face-to-face, mail, Internet)
- Length of relationship with the client
- Financial institution's prior experience with and knowledge of the customer and his/her/its transactions (e.g., previous internal investigations, Currency Transaction Report [CTR] and/or Suspicious Activity Report [SAR] filings)
- Source(s) of income
- Type(s) of product(s)/service(s) provided
- Expected pattern of activity and actual transaction activity in the account in terms of transaction types, dollar volume and frequency
- Geographic considerations (e.g., residency or principal place[s] of business, incorporation, citizenship, origination/destination of funds, location of primary customers)
- Status as or relationship with other high-risk individuals/entities (e.g., politically exposed persons [PEPs])

A customer risk assessment is not one-dimensional. A customer may have a low-risk business/occupation but reside in a high-risk geographic jurisdiction. Money laundering and terrorist financing risks are assessed on the overall profile of a customer, not on any one factor.

829. Should a financial institution develop one risk assessment methodology that applies to all of its customers?

It may be desirable to develop different risk assessment methodologies for different types of customers (e.g., individuals, nonindividuals) or customer segments (e.g., corporate, financial institution, retail, private banking) in order to consider specific factors that may not apply to all customers. For example, a risk assessment methodology for correspondent customers should consider the underlying customers of the bank who/that may utilize the U.S.

correspondent account. For PEPs, a risk assessment methodology may consider the country, level of office and degree of relationship of the PEP (in the case of family members and close affiliates).

830. Is it always necessary or appropriate to risk-rate each customer separately?

In some instances, it may be acceptable to risk-rate customers on a segment basis. For example, homogeneous segments of retail customers might be risk-rated by groups based on the nature of products provided and levels of activity, rather than risk-rated individually.

831. Should a customer risk assessment methodology be developed on an account level, customer level or household level?

A customer risk assessment methodology should be developed on a customer level, not an account level. Conducting a risk assessment on an account level prevents the financial institution from assessing the risk of all of the customer's relationships; rather, it focuses on a small snapshot of the customer's activity. Conducting a risk assessment on the customer level helps to ensure the financial institution understands the risks posed by all of the customer's accounts and relationships (e.g., household).

Ideally, risk should be assessed on a household or relationship level; however, the ability of an institution to do this will be a function of how it manages its data (i.e., its ability to link related accounts). For example, if high-risk business ABC Company and its owners have accounts at an institution, both the business and retail accounts should be rated as high-risk.

832. How is the term "household" defined?

A "household" is generally defined as an entity consisting of two or more distinct customers who share a common factor such as an address, phone number or business owner.

833. What should a financial institution do if it can only conduct an assessment on an account level as opposed to a customer level?

To compensate for this data limitation, a financial institution can conduct monitoring or request enhanced due diligence (EDD) on a customer or a household level. For example, if a customer has 10 accounts, of which only one resulted in a high-risk rating, all nine other accounts can be assigned a high-risk rating and be included in the monitoring or EDD request.

834. How can a financial institution stratify the risk of its customers if all of its target customers are considered high-risk by industry standards (e.g., a financial institution and its customers are located primarily in high-risk jurisdictions)?

One high-risk factor alone does not necessarily mean a customer is high-risk. Financial institutions should use multiple factors when stratifying customers into high-, moderate- and low-risk segments. For example, a community bank located in a High Intensity Drug Trafficking Area (HIDTA) may have many customers with elevated risk based only on their location in the HIDTA zone. Upon further review, however, a majority of these customers may have had a relationship with the financial institution for more than five years, and most of them have been using low-risk products and services (e.g., safe deposit boxes, five-year CDs). These factors, combined with others, can be used to separate high-risk customers from moderate- and low-risk customers.

835. Should financial institutions consider not opening an account or terminating an existing relationship if a customer is rated as high-risk?

A rating of high risk does not imply that a customer relationship should not be extended or should be terminated. The decision to open or retain a relationship with high-risk customers should be defined in policy and by the risk tolerances established by the institution's senior management and board of directors. Opening or maintaining the relationship simply means that due diligence for the customer should be more extensive and that the customer's transactions should be subject to heightened scrutiny.

High-Risk Geographies

836. What countries should financial institutions classify as increased risk for the purpose of performing a customer risk assessment or transaction monitoring?

Financial institutions should develop an objective approach to determine which countries should be considered at increased risk to money laundering or terrorist financing. Factors that can be considered include, but are not limited to, the following:

- Strength of AML infrastructure (e.g., legal and regulatory framework)
- Subject to government sanctions
- Degree of corruption
- Designation as a sponsor of terrorism
- Designation as a tax haven
- Strength of secrecy laws (i.e., favors/encourages secrecy)
- Designation as a drug trafficking region
- Designation as a human trafficking/smuggling region

837. Where can a financial institution obtain information on high-risk countries?

Fortunately, analyses performed by numerous government agencies and organizations can be leveraged to help in the process of identifying high-risk countries.

Commonly used sources for this purpose include the following:

- Office of Foreign Assets Control (OFAC) Blocked Countries List
- International Narcotics Control Strategy Report (INCSR) issued by the U.S. Department of State
- Global Corruption Report and Corruption Perceptions Index issued by Transparency International (TI)
- Offshore financial centers (OFC), as identified by the International Monetary Fund (IMF)
- Uncooperative tax havens, as identified by the Organisation for Economic Co-operation and Development (OECD)
- Jurisdictions or countries identified as “high-risk and non-cooperative jurisdictions” by the Financial Action Task Force (FATF)
- Trafficking in Persons Report (TIP Report) by the U.S. State Department

Financial institutions should consider adding countries identified as high-risk based on prior experiences and transaction history.

Additional guidance can be found in numerous other government and not-for-profit agencies. It is important to note, however, that the rationale for assigning country risk should be both well documented and defendable.

838. Is it only a customer’s country of domicile that should be considered or are there other geographic considerations that may have a bearing on risk?

In addition to the country of domicile, a customer’s risk to money laundering and terrorist financing also may be impacted by where the customer conducts activities (e.g., business operations, origination/destination countries of wire transfers), so it also may be appropriate for the risk assessment to consider the following:

- Countries/jurisdictions where the customer principally operates
- Countries/jurisdictions of the customers/suppliers of the business
- Origination/destination countries/jurisdictions of transactions

- Countries/jurisdictions of other relationships (e.g., accounts held at financial institutions in tax havens, PEPs)

839. Are high-risk jurisdictions limited to international locations?

No. High-risk geographic locations may include domestic locales, such as financial institutions doing business within, or having customers located within, a U.S. government-designated high-risk geographic location.

Domestic high-risk geographic locations include, but are not limited to, the following:

- High Risk Money Laundering and Related Financial Crimes Areas (HIFCA)
- High Intensity Drug Trafficking Areas (HIDTA)
- States with weak anti-human trafficking laws identified in the Polaris Project's Annual State Ratings Report

840. What is a High Risk Money Laundering and Related Financial Crimes Area (HIFCA)?

HIFCAs were defined in the Money Laundering and Financial Crimes Strategy Act of 1998 to assist law enforcement with concentrating its efforts in high-intensity money laundering zones at the federal, state and local levels. HIFCAs may be defined geographically; they also can be created to address money laundering in an industry sector, a financial institution, or group of financial institutions.

841. What is the purpose of designating a HIFCA?

The HIFCA designation serves to concentrate federal, state and local law enforcement efforts in order to combat money laundering in an area designated as a high-intensity money laundering zone. To accomplish this coordinated effort, a money laundering action team is created within each HIFCA. This team contains members from all relevant federal, state and local law enforcement, prosecutors, and financial regulators. It focuses on tracing funds to/from the HIFCA to/from other areas, and on collaborating on investigative techniques within the HIFCA and between the HIFCA and other areas. It also has an asset forfeiture component, and the setup of the team provides for an easier flow of information among all members of the HIFCA.

842. How are HIFCAs designated?

HIFCAs can be designated in two ways:

- Areas can be proposed by the Secretary of the Treasury or the Attorney General.
- Designations can come through an application process in which localities submit applications through FinCEN.

843. How does a locality petition to become a HIFCA?

If a locality wishes to be designated as a HIFCA, it should request HIFCA designation in writing to the FinCEN Director. The letter should include:

- A description of the proposed area/entity/industry
- A focus and plan for the counter-money laundering projects to be supported
- Reasoning as to why such a designation is appropriate, which considers relevant statutory standards
- A designated point of contact

Applications are first reviewed by the HIFCA Designation Working Group, which is co-chaired by the Departments of the Treasury and Justice, and composed of senior officials from the Criminal Division of the DOJ, FBI, DEA, IRS-CID, U.S. Customs Service, FinCEN, U.S. Secret Service, U.S. Postal Inspection Service and other appropriate agencies. The Working Group then provides a recommendation to the Treasury Secretary and the Attorney General. Finally, the decision made by the Treasury Secretary and Attorney General is provided to the applicant in writing.

844. What is a High Intensity Drug Trafficking Area (HIDTA)?

HIDTAs were authorized in the Anti-Drug Abuse Act of 1988 to assist law enforcement with concentrating its efforts with drug control at the federal, state and local levels. HIDTAs are designated by area. Since the original designation of five HIDTAs in 1990, the program has expanded to 32 areas of the country, including five partnerships along the southwest border.

845. What is the purpose of designating a HIDTA?

The HIDTA designation serves to enhance and coordinate federal, state and local law enforcement drug control efforts. The program accomplishes this by institutionalizing teamwork among the agencies, synchronizing investments in strategy-based systems, and better focusing all agencies on the same outcomes. The program provides agencies with coordination, equipment, technology and additional resources to combat drug trafficking and its harmful consequences in critical regions of the United States.

846. How are HIDTAs designated?

HIDTAs are designated by the Director of the Office of National Drug Control Policy (ONDCP), in consultation with the Attorney General, the Secretary of the Treasury, the Secretary of Homeland Security, heads of the national drug control program agencies, and the governor of each applicable state. A coalition of interested law enforcement agencies from an area also may petition for designation as a HIDTA.

847. What primarily is taken into consideration when designating a HIDTA?

The primary factors considered by the Director of the ONDCP when reviewing a petition to create a HIDTA are the extent to which:

- The area is a significant center of illegal drug production, manufacturing, importation or distribution.
- State, local and tribal law enforcement agencies have committed resources to respond to the drug trafficking problem in the area, thereby indicating a determination to respond aggressively to the problem.
- Drug-related activities in the area are having a significant, harmful impact in the area and in other areas of the country.
- A significant increase in allocation of federal resources is necessary to respond adequately to drug-related activities in the area.

High-Risk Customers

848. What business types/occupations pose a higher money laundering and terrorist financing risk?

Business types and occupations considered to be high-risk for money laundering and terrorist financing include those that are cash-intensive; those that allow for the easy conversion of cash into other types of assets; those that provide opportunity to abuse authoritative powers and assist in disguising the illegal transfer of funds; those that lack transparency; those that involve international transactions/customers; and those that offer high-risk or high-value products. High-risk business types/occupations include, but are not limited to, the following:

- Accountants/accounting firms
- Aircraft engine/part and military armored vehicle manufacturing
- Amusement, gambling and recreation activities
- Attorneys/law firms
- Art/antiques dealers
- Car washes
- Charitable organizations/Nongovernmental organizations (NGOs)
- Cigarette distributors
- Consumer electronics rentals and dealers
- Convenience stores
- Flight training
- Gas stations
- Importers/exporters

- Leather manufacturing, finishing and goods stores
- Liquor stores
- Bank and Nonbank Financial Institutions (NBFIs) or their agents
- Notaries
- Offshore companies
- Parking garages
- Pawnbrokers
- Precious metals, stones or jewelry dealers and wholesalers
- Racetracks
- Real estate brokers
- Restaurants/bars
- Retail establishments
- Politically exposed persons (PEPs) and political organizations
- Small arms and ammunition manufacturing
- Sole practitioners
- Tobacco wholesalers
- Transportation services and equipment rental
- Trusts and custodial entities
- Textile businesses
- Travel agencies and traveler accommodations
- Vehicle dealers
- Vending machine operators

Financial institutions may decide it is appropriate to add other business types/occupations based on a variety of sources, such as guidance provided by regulatory agencies or the FATF, or their own risk analyses. For example, as an institution's internal investigation database expands, an institution may consider adding the business type/occupation of customers who/that have had a significant number of SAR/CTR filings.

Certain crimes, such as human trafficking may have their own high risk types/occupations. For further guidance, please refer to the Human Trafficking section.

849. Should financial institutions consider not opening an account or terminating an existing relationship if a customer is high-risk?

Status as a high-risk customer does not mean an account should not be opened or an existing relationship automatically terminated. It simply means due diligence for the high-risk customer should be more extensive than for a standard customer and that the customer's transactions should be subject to heightened scrutiny.

850. Are high-risk activities limited to businesses?

No. High-risk activities include activities for both businesses and individuals (e.g., accountants, attorneys). For example, if a customer owns or is a principal of a high-risk business, that factor should be considered as part of the risk assessment. It is important to note that accounts established to support an accountant's or attorney's business pose different risks than personal accounts of these high-risk professional service providers.

851. Should each nature of business/occupation be treated with the same risk within its scoring methodology?

A financial institution should clearly document how each nature of business/occupation is treated in its methodology. Some financial institutions, in line with the guidance issued by the FATF, risk-rate certain businesses/occupations by

the types of services provided (e.g., lawyers who sell real estate on behalf of their customers are risk-rated differently than those who draft wills), thus allowing one nature of business/occupation to have a different risk rating depending upon the services provided.

852. How can financial institutions identify high-risk customers in their existing customer bases?

Financial institutions can identify high-risk customers in their existing customer bases by doing the following:

- Reviewing North American Industry Classification System (NAICS) codes for high-risk business activities
- Conducting keyword searches (e.g., check casher, *casa de cambio*, jewelry, car) in customer databases and transaction details (e.g., wires)
- Reviewing high-volume/value transaction reports (e.g., cash, wires)
- Screening against FinCEN's MSB list
- Screening against proprietary databases (e.g., PEPs)
- Querying account officers
- Reviewing subjects of investigations and SARs

Nonresident Aliens and Foreign Persons

853. What is the difference between the terms "resident alien" and "nonresident alien"?

An alien is any person who is not a U.S. citizen. For tax purposes, the Internal Revenue Service (IRS) classifies aliens as either resident aliens or nonresident aliens (NRAs) based on (1) a Green Card test or (2) a Substantial Presence test.

- **Resident Alien**: If the alien has a Green Card, also known as an alien registration receipt card, or if he or she was physically present in the United States for 31 days during the current year and 183 days during a three-year period that includes the current year and the two years immediately before that, the alien is then classified as a resident alien and his or her earned income is taxed like a U.S. citizen's earned income.
- **Nonresident Alien (NRA)**: A nonresident alien is an alien who does not meet the Green Card test or the Substantial Presence test. For NRAs, only income that is generated from U.S. sources, excluding certain investments such as stocks, is subject to taxation.

854. What is the difference between the terms "NRAs" and "foreign persons"?

NRAs are foreign individuals who (or businesses that) are not permanent residents of the United States but may reside on a part-time basis in the United States. "Foreign persons" generally refers to individuals who (or businesses that) do not reside in the United States for any amount of time. In some instances, the term "NRA" is used interchangeably with "foreign persons" to describe all non-U.S. persons, regardless of actual residency.

855. What is the difference between the terms "NRAs" and "illegal aliens"?

Illegal aliens are foreigners who have violated U.S. laws and customs in establishing permanent residence in the United States. NRAs are foreign individuals who (or businesses that) have not met the criteria described above to be classified as resident aliens.

856. Why do NRAs and foreign persons establish account relationships at U.S. financial institutions?

Nonresident aliens and foreign persons establish accounts at U.S. financial institutions for various reasons, including, but not limited to, the following:

- Asset preservation
- Access to investments
- Unstable financial system in their home country

- Expansion in business

857. Are NRAs and foreign persons required to provide a taxpayer identification number to establish account relationships at U.S. financial institutions?

No. According to the USA PATRIOT Act's Section 326 – Verification of Identification, commonly referred to as the Customer Identification Program (CIP) requirement, individuals and businesses must provide the following information prior to establishing an account at a U.S. financial institution:

- Name
- Date of birth (DOB) for individuals
- Address
- Identification number

A taxpayer identification number (TIN) should always be obtained for U.S. persons. For non-U.S. persons, one or more of the following should be obtained for the identification number:

- TIN
- Passport number and country of issuance
- Alien identification card number
- Number and issuing country of any other unexpired government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard

For further guidance on the CIP requirement, please refer to the Section 326 – Verification of Identification section.

858. What are W-8BEN forms and why might an NRA complete one when establishing an account with a financial institution?

A W-8BEN form, formally known as the "Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding," is an IRS form that attests to the NRA's tax-exempt status. As a result, financial institutions, as the withholding agents, will not withhold taxes for income earned on accounts held by the NRA.

859. What responsibilities do financial institutions have with respect to W-8BEN forms?

Financial institutions are responsible for maintaining completed W-8BEN forms in accordance with AML recordkeeping requirements, ensuring they are updated as necessary, providing completed forms to the IRS upon request, and monitoring customer activity for patterns that indicate U.S. resident status or other potentially suspicious activity.

860. Are financial institutions responsible for determining whether a potential or existing customer is an NRA or an illegal alien?

No. Financial institutions are not responsible for determining whether a customer is an NRA or an illegal alien. If a financial institution detects patterns that indicate U.S. resident status for a customer who certified otherwise, it is only responsible for reporting potentially suspicious activity – in this case, false or inaccurate information provided on official IRS forms.

861. Would resident aliens complete the same W-8BEN forms when establishing accounts with a financial institution?

No. Similar IRS forms exist for individuals who (and businesses that) are not NRAs who would like to certify their citizenship/residence status and/or tax-exempt status. Exceptions exist in applicability, but in general, the forms are:

- **Resident aliens/U.S. citizens** complete a **W-9** form, formally called a "Request for Taxpayer Identification Number and Certification."
- **Persons claiming that income is effectively connected with the conduct of a trade or business in the United States** complete **W-8ECI** forms, formally known as "Certificate of Foreign Persons Claim That Income Is Effectively Connected With the Conduct of a Trade or Business in the United States."

- **Foreign partnerships, foreign simple trusts, or foreign grantor trusts** complete **W-8ECI** forms or **W-8IMY** forms, formally referred to as "Certificate of Foreign Intermediary, Foreign Flow-Through Entity, or Certain U.S. Branches for United States Tax Withholding."
- **Foreign governments, international organizations, foreign central banks of issue, foreign tax-exempt organizations, foreign private foundations, or governments of a U.S. possession that received effectively connected income** complete **W-8ECI** forms or **W-8EXP** forms, formally called "Certificate of Foreign Government or Other Foreign Organization for United States Tax Withholding."
- **Persons acting as intermediaries** complete **W-8IMY** forms, formally known as "Certificate of Foreign Intermediary, Foreign Flow-Through Entity, or Certain U.S. Branches for United States Tax Withholding."

862. What are the heightened money laundering and terrorist financing risks of NRAs?

The heightened risk of NRAs lies in the following:

- Challenges in verifying their identities, source of funds and source of wealth
- Increased frequency of international transactions
- Possible residency in a high-risk jurisdiction with lax AML laws and regulations
- Increased chance of being identified as a politically exposed person (PEP)

863. As customers, do all NRAs and foreign persons pose the same degree of risk?

No. The risks of each NRA and foreign person should be assessed based on a variety of factors (e.g., products/services, occupation/nature of business, associated geographies, transaction activity). Status as an NRA or foreign person is only one risk factor. Evaluating the risks of NRAs and foreign persons in this manner will result in different risk ratings (e.g., low, moderate, high).

Professional Service Providers

864. How is the term "professional service provider" defined?

A professional service provider, also referred to as a "gatekeeper," acts as an intermediary between its client and a third-party financial institution and may conduct or arrange for financial dealings and services on its client's behalf (e.g., management of client finances, settlement of real estate transactions, asset transfers, investment services, trust arrangements). Examples of professional service providers include lawyers, notaries and accountants.

865. What are the heightened money laundering and terrorist financing risks of professional service providers?

The heightened risk of professional service providers lies in their ability to mask the identity of underlying clients when conducting financial services on their behalf. Financial institutions often do not have any information on underlying clients as their account relationship is with the professional service provider. As such, financial institutions must rely on professional service providers to conduct appropriate due diligence to mitigate the risks of doing illicit business.

Additionally, the privacy and confidentiality adhered to by some of these service providers can be exploited by criminals, money launderers and terrorists.

866. What is an "Interest on Lawyers Trust Account"?

An "Interest on Lawyers Trust Account" (IOLTA) is a bank account that contains funds for various clients held in trust by the attorney where interest earned on the account is ceded to the state bar association or another entity for public interest and pro bono purposes.

867. What are the heightened money laundering and terrorist financing risks of IOLTAs?

In addition to its association with high-risk professional service providers who may mask the identity of underlying clients, the heightened risk of an IOLTA lies in the commingling of multiple client funds in the IOLTA. This makes it difficult for a financial institution to understand the source and purpose of incoming and outgoing funds. Additionally, since many IOLTA accounts for different attorneys can be assigned the same taxpayer identification number (TIN) (e.g., of the state bar association or another entity for public interest), this makes it difficult to identify activity that may warrant Currency Transaction Report (CTR) and/or Suspicious Activity Report (SAR) filing.

868. As customers, do all professional service providers pose the same degree of risk?

No. The risks of each professional service provider should be assessed based on a variety of factors (e.g., products/services offered by the provider, associated geographies, transaction activity, history of regulatory report filings). Status as a professional service provider is only one risk factor. Evaluating the risks of professional service providers to include other variables will result in different risk ratings (e.g., low, moderate, high).

869. Are there specific AML requirements for professional service providers?

Currently, there are no specific AML requirements for professional service providers in the United States, though other jurisdictions do impose requirements. Trade associations and key international groups such as the Financial Action Task Force (FATF) have highlighted the need for professional service providers to establish AML controls due to their positions as gatekeepers and intermediaries to the financial system. In order to establish accounts at financial institutions, professional service providers already may be required by their banks to implement basic AML controls to mitigate the risks associated with their professions.

Additionally, assuming they are U.S. persons, professional service providers are required to comply with the Office of Foreign Assets Control (OFAC) laws and regulations. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

870. What guidance has been issued on professional service providers?

The following key guidance has been issued on professional service providers:

- **Professional Service Providers – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendations 22 - 23: Designated Non-Financial Businesses and Professions (DNFBP)** (2012) by the Financial Action Task Force (FATF)
- **Guardians at the Gate: The Gatekeeper Initiative and the Risk-Based Approach for Transactional Lawyers** (2009) by the American Bar Association (ABA)
- **Forty Recommendations and Nine Special Recommendations on "Designated Nonfinancial Businesses and Professions (DNFBP)"** (2012) by FATF
- **RBA Guidance for Trust and Companies Service Providers (TCSPs)** (2008) by FATF
- **RBA Guidance for Real Estate Agents** (2008) by FATF
- **RBA Guidance for Accountants** (2008) by FATF
- **Risk-Based Approach Guidance for Legal Professionals** (2008) by FATF
- **Wolfsberg FAQs on Intermediaries** (2012) by the Wolfsberg Group
- **OFAC Regulations for the Corporate Registration Industry** (2004) by the Office of Foreign Assets Control (OFAC)

Trust and Asset Management Services

871. How are "trust accounts" defined?

The FFIEC BSA/AML Examination Manual defines "trust accounts" as legal arrangements in which one party (the trustor or grantor) transfers ownership of assets to a person or financial institution (the trustee) to be held or used for the benefit of others. These legal arrangements include:

- Broad categories of court-supervised accounts (e.g., executorships and guardianships)
- Personal trusts (e.g., living trusts, trusts established under a will, charitable trusts)
- Corporate trusts (e.g., bond trusteeships)

872. What is the difference between "fiduciary capacity" and "trust"?

"Fiduciary capacity" is more broadly defined than "trust" as it includes the following:

- A trustee, an executor, an administrator, a registrar of stocks and bonds, a transfer agent, a guardian, an assignee, a receiver, or a custodian under the Uniform Gifts to Minors Act
- An investment adviser, if the bank receives a fee for its investment advice
- Any capacity in which the bank possesses investment discretion on behalf of another

The Office of the Comptroller of the Currency (OCC) uses the broader term "fiduciary capacity" instead of "trust."

873. How are "agency accounts" defined?

According to the FFIEC BSA/AML Examination Manual, unlike trust arrangements, "agency accounts are established by contract and governed by contract law. Assets are held under the terms of the contract, and legal title or ownership does not transfer to the bank as agent. Agency accounts include custody, escrow, investment management and safekeeping relationships. Agency products and services may be offered in a traditional trust department or through other bank departments."

874. How are "asset management services" defined?

The FFIEC BSA/AML Examination Manual defines "asset management accounts" as trust or agency accounts and are managed by a financial institution, including, but not limited to, the following:

- Personal and court-supervised accounts
- Trust accounts formed in the private banking department
- Asset management and investment advisory accounts
- Global and domestic custody accounts
- Securities lending
- Employee benefit and retirement accounts
- Corporate trust accounts
- Transfer agent accounts

875. How are "asset protection trusts" defined?

The FFIEC BSA/AML Examination Manual defines asset protection trusts (APTs) as "a special form of irrevocable trust, usually created (settled) offshore for the principal purpose of preserving and protecting part of one's wealth against creditors. Title to the asset is transferred to a person named as the trustee. APTs are generally tax neutral with the ultimate function of providing for the beneficiaries."

876. What are the heightened money laundering and terrorist financing risks of trust and asset management services?

The heightened risk of trust and asset management services lies in the lack of transparency with regard to ownership. Additionally, the privacy and confidentiality adhered to by some trust and asset management service providers can be exploited by criminals, money launderers and terrorists.

877. Do all trust and agency accounts pose the same degree of risk?

Typically, employee benefit accounts and court-supervised accounts are among the lowest risk. Factors that can be used to assess the level of risk associated with trusts include, but are not limited to, the following:

- Type of trust or agency account
- Types, size and frequency of transactions
- Geographic considerations (e.g., country of residence of the principals or beneficiaries, country where the trust was established, origination/destination country of incoming/outgoing funds)
- Relationship with high-risk entities (e.g., politically exposed persons [PEPs], private investment companies [PICs], charitable organizations or other nongovernmental organizations [NGOs])

878. Is there a legitimate purpose for utilizing trust and asset management services?

The legitimate reasons for utilizing these services may include the following:

- Asset protection
- Estate planning
- Privacy and confidentiality
- Reduction of tax liability

879. Who are the common participants in a trust?

Common participants in a trust include the following:

- **Trustee** – Person or entity that holds legal title to the trust and is obliged to administer the trust in accordance with both the terms of the trust document and the governing law
- **Trustor/Settlor/Grantor/Donor** – Creator of the trust who entrusts some or all of his or her property to people of his or her choice
- **Beneficiaries** – Beneficial owners of the trust

880. Who is the customer of the financial institution, the trust or the beneficiaries of the trust?

For the purpose of the CIP rule, the "customer" is the trust that opens the account with the financial institution, whether or not the financial institution is the trustee for the trust.

881. Should other parties to the trust beyond the account holder be subject to the CIP rule?

Although not currently required, financial institutions should determine the identity of other parties that may have control over the account or have authority to direct the trustee, such as grantors, co-trustees and settlors.

FinCEN's advanced notice of proposed rule "Customer Due Diligence Requirements for Financial Institutions" does not amend what financial institutions must collect pursuant to Section 326, but it does expand the parties for which they would be expected to collect information. Currently, covered financial institutions are required to obtain beneficial ownership in the following situations as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

The ANPR could categorically require all financial institutions subject to AML Program requirements to identify, and in some instances, verify the identity of beneficial ownership of all of its account holders. For further guidance, please refer to the Beneficial Owners section.

882. Since beneficiaries of trusts are not currently subject to verification under the CIP rule, are financial institutions required to screen them for possible OFAC Sanctions violations?

Beneficiaries who have a future or contingent interest in funds in an account should be screened for possible OFAC violations. Some institutions opt to screen beneficiaries at the time funds are transferred as opposed to the inception of the relationship.

Screenings for sanctions violations should be risk-based and consistent with the risk profile of the financial institution. For additional guidance, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

883. Are there specific AML requirements for financial services companies offering trust and asset management services?

The USA PATRIOT Act expanded the definition of "financial institutions" subject to AML requirements to include trust companies and investment advisers. Additionally, in other countries, certain professional service providers are

subject to AML requirements as well. In short, the legal entity type and the types of trust and asset management services offered will dictate the AML requirements of those businesses offering these services.

For example, a trust company is a corporation organized to perform as the fiduciary of trusts and agencies. Many trust companies are owned by commercial banks and, as such, would be required to comply with the following AML requirements:

- Establishment of an AML program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program and conducts an independent review of the AML program
- Establishment of a Customer Identification Program (CIP)
- Filing of Suspicious Activity Reports (SARs)
- Filing of Currency Transaction Reports (CTRs)
- Filing of Reports of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300) (only where not required to file a CTR)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Recordkeeping and retention (e.g., Funds Transfer Rule, Travel Rule, Purchase and Sale of Monetary Instruments)
- Information sharing (314(a) (mandatory), 314(b) (optional))
- Complying with Special Measures
- Obtaining Foreign Bank Certifications
- Establishing an enhanced due diligence (EDD) program for foreign correspondent account relationships, private banking relationships and politically exposed persons (PEPs)

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to investment providers is provided in the Investment Advisers and Unregistered Investment Companies section. For further guidance on professional service providers, please refer to the Professional Service Providers section.

884. What guidance has been issued on trust and asset management services?

The following key guidance has been issued on trust and asset management services:

- **Trust and Asset Management Services – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendations 22 - 23: Designated Nonfinancial Businesses and Professions (DNFBP)** (2012) by the Financial Action Task Force (FATF)
- **RBA Guidance for Trust and Companies Service Providers (TCSPs)** (2008) by FATF

Deposit Broker

885. What does the term “deposit broker” mean?

A deposit broker is an individual or a firm that, for a fee, places customers’ deposits with insured depository institutions.

886. What is a brokered deposit?

A brokered deposit is a deposit solicited by a third party. Usually, but not always, it is for a figure slightly below the amount covered by deposit insurance so that all interest as well as the principal is covered.

887. What are the heightened money laundering and terrorist financing risks of deposit brokers?

The potential heightened risk of brokered deposits lies in the following:

- Use of international brokers
- Targeting of higher risk customers – e.g., nonresident aliens, offshore customers, politically exposed persons (PEPs)
- Reliance on third parties to conduct adequate due diligence and monitor for potentially suspicious activity
- Use of front companies/shells to obscure the beneficial owner and/or source of funds
- Higher-risk methods of account opening
- Commingling of funds/anonymity of underlying depositor
- Lesser degree of regulatory oversight relative to financial institutions

888. Who is the customer of the financial institution, the deposit broker or the clients of the deposit broker?

For the purpose of the CIP rule, the "customer" is the deposit broker who opens the account with the financial institution. The identity of each individual "sub-account holder" does not require verification.

889. What steps can a financial institution take to mitigate the risk associated with deposit brokers?

To mitigate the risks that lie with deposit brokers, financial institutions may consider executing the following at the inception of the relationship and on an ongoing basis:

- Limiting business dealings to include only deposit brokers who have an established relationship with the financial institution or other trusted entity
- Conducting background checks on deposit brokers, including a review of all services offered, methods of soliciting new clients, licensing, regulatory obligations and reputation
- Restricting services for certain high-risk customer types – e.g., nonresident aliens (NRAs), PEPs or customers located in high-risk jurisdictions
- Evaluating whether the deposit broker's AML/OFAC compliance program is adequate and consistent with the policies of the financial institution

890. Are there specific AML requirements for deposit brokers?

Many U.S. deposit brokers, such as broker-dealers, are subject to their own AML requirements. All U.S.-based deposit brokers, whether firms or individuals, are also obligated to comply with OFAC. The requirements affecting international deposit brokers vary by jurisdiction.

891. What specific guidance has been issued on the money laundering risk of deposit brokers?

The **Brokered Deposits – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC) offers specific guidance on the money laundering risk of brokered deposits.

Private Banking

892. How is the term "private banking" defined?

For the purpose of Section 312 of the USA PATRIOT Act, a private banking account is defined as an account (or combination of accounts) maintained at a financial institution that meets the following criteria:

- Requires a minimum aggregate deposit of funds or other assets of not less than $1 million

- Is established on behalf of or for the benefit of one or more non-U.S. persons who are direct or beneficial owners of the account
- Is assigned to, or is administered or managed by, in whole or in part, an officer, employee or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account

893. What are the heightened money laundering and terrorist financing risks of private banking customers?

Private banking can be vulnerable to money laundering schemes for the following reasons:

- Strict privacy and confidentiality culture of private bankers
- Powerful clientele (e.g., PEPs)
- Use of trusts, private investment companies (PICs) and other types of nominee companies
- Increased frequency of international transactions

894. As customers, do all private banking customers pose the same degree of risk?

No. The risks of each private banking customer should be assessed based on a variety of factors (e.g., products/services, occupation/nature of business, associated geographies, transaction activity). Status as a private banking customer is only one risk factor. Evaluating the risks of private banking customers in this manner will result in different risk ratings (e.g., low, moderate, high).

895. Are there specific AML requirements for private banking customers?

Yes. Due to the high-risk nature of private banking, Section 312 of the USA PATRIOT Act, formally referred to as "Special Due Diligence for Correspondent Accounts and Private Banking Accounts," outlines specific due diligence and enhanced due diligence required to be conducted by financial institutions that have private banking customers.

896. What guidance has been issued on private banking?

The following are examples of key guidance that has been issued on private banking:

- **Private Banking Due Diligence Program (Non-U S Persons)** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Wolfsberg AML Principles on Private Banking** (2012) by the Wolfsberg Group
- **Wolfsberg FAQs on Beneficial Ownership** (2012) by the Wolfsberg Group
- **Private Banking and Money Laundering: A Case Study of Opportunities and Vulnerabilities** (2001) by the U.S. Senate (Hearing)

For additional guidance on private banking customers and required due diligence, please refer to the Due Diligence for Private Banking Accounts and Enhanced Due Diligence for Private Banking Accounts sections.

Politically Exposed Persons

897. How is the term "politically exposed person" defined?

A "politically exposed person" (PEP) is a senior foreign political figure. Section 312 defines the term "senior foreign political figure" to include a current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned commercial enterprise; a corporation, business or other entity formed by or for the benefit of any such individual; an immediate family member of such an individual; or any individual publicly known (or actually known by the financial institution) to be a close personal or professional associate of such an individual.

"Immediate family member" means an individual's spouse, parents, siblings, children and spouse's parents or siblings. "Senior official" or "senior executive" means an individual with substantial authority over policy, operations or the use of government-owned resources.

898. Is the definition of a PEP limited to individuals?

No. In the broadest sense, PEPs can be nonindividuals. For example, government entities or corporations that have the authority to award government contracts also could be considered PEPs.

899. Is the definition of a PEP limited to "foreign" senior officials?

Many financial institutions extend the definition of PEP to include domestic senior political figures as well, though this is not required by Section 312.

900. Is the definition of a PEP limited to private banking customers?

No. Status as a PEP is not dependent on the types of products and services utilized by the PEP.

901. Do embassy and foreign consulate accounts fall within the definition of a PEP?

Certain individuals within an embassy or consulate may fall within the definition of a PEP (e.g., the ambassador or a high-ranking military officer). The average employee in an embassy or consulate is unlikely to reach PEP status. For further guidance on embassy accounts, please refer to the Foreign Embassy and Consulates section.

902. What are the heightened money laundering and terrorist financing risks of politically exposed persons?

Access to government funds may increase the potential for corruption and bribery.

903. Do all PEPs pose the same degree of risk?

No. Not all PEPs pose the same degree of risk. A financial institution may consider, for example, the country of domicile, level of office, negative history/media on the PEP, and the degree of affiliation to the PEP (in the case of family members and close associates) when assessing the degree of risk.

904. How should assets of political parties be treated?

Though political parties are not covered by the PEP definition, financial institutions should consider applying heightened scrutiny to business relationships holding assets of *foreign* political parties.

905. Is someone who was a PEP always a PEP?

The most conservative approach would be "once a PEP, always a PEP." A moderate approach, endorsed by the Wolfsberg Group and outlined in the European Union's Third Money Laundering Directive, would be for a financial institution to remove the individual from the institution's PEP list one year after the individual is no longer in a political function. However, if derogatory information or suspicious activity is detected, a financial institution should continue to categorize the customer as a PEP.

906. How would a financial institution monitor for transactions involving proceeds of foreign corruption?

Financial institutions can monitor for proceeds of foreign corruption by identifying customers and transaction counter-parties who may have greater access to foreign government funds (i.e., PEPs).

907. What steps should a financial institution take when determining if a customer is a PEP?

The rules provide that reasonable steps are in place to ascertain whether any account holder may be a senior foreign political figure. These steps should include, but not be limited to, holding conversations with the client, conducting reference checks, and reviewing information available in databases provided by list providers or public sources on the Internet.

908. Where can a financial institution find a list of PEPs?

Financial institutions can use several third-party vendors that provide a variety of Know Your Customer (KYC) and customer identification solutions, such as a list of PEPs. Public resources include, but are not limited to, lists published by OFAC, the FBI, the Central Intelligence Agency (CIA), Interpol, the Drug Enforcement Administration (DEA) and the United Nations.

909. How can a multinational financial institution manage its multi-country list of PEPs?

Some multinational financial institutions may modify their definition of PEPs to include senior foreign officials of all countries, irrespective of where each bank/branch is based. Additionally, they may utilize a risk-based approach and only include PEPs from countries with lax AML laws and regulations or a high index of corruption. For guidance in evaluating high-risk countries and jurisdictions, please refer to the High-Risk Geographies section.

910. Should financial institutions consider not opening an account or terminating an existing relationship if a customer is a PEP?

Status as a PEP does not mean that an account should not be opened or that an existing relationship should be automatically terminated. It simply means that due diligence for the PEP should be more extensive than for a standard customer and that the PEP's transactions should be subject to heightened scrutiny.

911. Are there specific AML requirements for PEPs?

Yes. Due to the high-risk nature of PEPs, Section 312 of the USA PATRIOT Act, formally known as "Special Due Diligence for Correspondent Accounts and Private Banking Accounts," outlines specific due diligence and enhanced due diligence required to be conducted by financial institutions that have PEPs as customers. For further guidance, please refer to Senior Foreign Political Figure section.

912. What guidance has been issued on PEPs?

The Financial Action Task Force (FATF), an intergovernmental policy-making body created to establish and promote international legislative and regulatory standards in the areas of money laundering and terrorist financing, defines PEPs as individuals who are or have been entrusted with prominent public functions in a foreign country (e.g., heads of state, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials). FATF also states that business relationships with family members or close associates of PEPs have similar reputational risks to PEPs themselves and, therefore, should be included in the definition of PEP, as well.

FATF also advises that the definition of PEP was not meant to include junior- or middle-ranking individuals in the categories mentioned above. FATF also suggests that domestic individuals who hold prominent public positions should be subject to enhanced due diligence (EDD).

Additional guidance includes the following:

- **Politically Exposed Persons – Overview** (2008) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 12: Politically Exposed Persons** (2012) by the Financial Action Task Force (FATF)
- **Guidance to Financial Institutions on Filing Suspicious Activity Reports Regarding the Proceeds of Foreign Corruption** (2008) by the FinCEN
- **Wolfsberg FAQs on Politically Exposed Persons** (2012) by the Wolfsberg Group
- **Guidance on Enhanced Scrutiny for Transactions That May Involve the Proceeds of Foreign Official Corruption** (2001) by the U.S. Treasury, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision and the U.S. Department of State
- **Stolen Asset Recovery: Politically Exposed Persons, A Policy Paper on Strengthening Preventive Measures** (2009) by the World Bank
- **Stolen Asset Recovery: Guide on Non-Conviction Based (NCB) Asset Forfeiture** (2009) by the World Bank

Foreign Embassy and Consulates

913. How are the terms "foreign embassy" and "consulate" defined?

The embassy, led by the ambassador, is a foreign government's official representation in the United States (or other country).

Consulate offices act as branches of the embassy and perform various administrative and governmental functions (e.g., issuing visas, handling immigration matters).

914. Do embassy and foreign consulate accounts fall within the definition of a PEP?

Certain individuals within an embassy or consulate may fall within the definition of a PEP (e.g., the ambassador or a high-ranking military officer). The average employee in an embassy or consulate is unlikely to reach PEP status.

915. Why do embassies and foreign consulates establish account relationships at U.S. financial institutions?

Embassies and foreign consulates establish accounts at U.S. financial institutions for various reasons, including, but not limited to, the following:

- Manage operational expenses (e.g., payroll, rent, utilities)
- Facilitate inter- and intra-governmental transactions (e.g., commercial and military purchases)
- Provide ancillary services or accounts to embassy staff, families, and current or prior foreign government officials

916. What are the heightened money laundering and terrorist financing risks of foreign embassies and consulates?

The heightened risk of embassies and foreign consulates lies in the following:

- Customers from high-risk jurisdictions
- Increased volume of high-risk products/services and transactions (e.g., cash, pouch activity)
- Increased frequency of international transactions
- Increased chance of being affiliated with a politically exposed person (PEP)

917. As customers, do all foreign embassies and consulates pose the same degree of risk?

No. The risks of each embassy and foreign consulate customer should be assessed based on a variety of factors (e.g., the strength of AML laws in the home country, services provided, employees who meet the definition of a PEP). Evaluating the risks of embassy and foreign consulate customers in this manner will result in different risk ratings (e.g., low, moderate, high).

918. Are there specific AML requirements for foreign embassies and consulates?

Certain individuals within an embassy or consulate may fall within the definition of a PEP (e.g., the ambassador or a high-ranking military officer). The average employee in an embassy or consulate is unlikely to reach PEP status. Due to the high-risk nature of PEPs, Section 312 of the USA PATRIOT Act, formally known as “Special Due Diligence for Correspondent Accounts and Private Banking Accounts,” outlines specific due diligence and enhanced due diligence required to be conducted by financial institutions who have PEPs as customers. For further guidance, please refer to Senior Foreign Political Figure section.

919. What guidance has been issued on foreign embassies and consulates?

The following are examples of information and guidance that have been issued on foreign embassies and consulates:

- **Embassy and Foreign Consulate Accounts – Overview & Politically Exposed Persons – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Guidance on Accepting Accounts from Foreign Governments, Foreign Embassies and Foreign Political Figures** (2004) by FinCEN
- **Interagency Guidance on Accepting Accounts from Foreign Embassies, Consulates and Missions** (2011) by FinCEN
- **Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Official Corruption** (2001) by the U.S. Treasury, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision and the U.S. Department of State

- **Money Laundering and Foreign Corruption: Enforcement and Effectiveness of the PATRIOT Act: Case Study Involving Riggs Bank Report** (2004) by the United States Senate Permanent Subcommittee on Investigations

Business Entities: Shell Companies, Private Investment Companies

920. What types of business entities pose heightened money laundering and terrorist financing risks?

The term "business entities" generally refers to partnerships, corporations, limited liability companies (LLCs), trusts and other entities that may be used for many purposes, such as tax and estate planning. The following business entity types pose heightened risk:

- **Shell Company** generally refers to an entity without a physical presence in any country.
- **International Business Corporations (IBCs)** are corporations established in offshore jurisdictions and generally licensed to conduct business only outside the country of incorporation.
- **Private Investment Companies (PICs)** are a subset of IBCs and generally refer to companies formed by one or more individuals to own and manage his/her/their assets. Like IBCs, PICs typically are established in offshore jurisdictions with lax AML laws and regulations. Ownership is often vested through bearer shares or trusts.
- **Nominee Incorporation Services (NIS)** are intermediaries that establish U.S. shell companies, open bank accounts and act as registered agents on behalf of foreign clients.

921. What are the heightened money laundering and terrorist financing risks of these high-risk business entities?

The heightened risk of these business types lies in the lack of ownership transparency and minimal or no recordkeeping requirements, financial disclosures and supervision.

Additionally, the privacy and confidentiality adhered to by some of these service providers can be exploited by criminals, money launderers and terrorists.

922. Is there a legitimate purpose for establishing these types of business entities?

The legitimate reasons for establishing these businesses include:

- Asset protection
- Estate planning
- Privacy and confidentiality
- Reduction of tax liability
- Engagement in international business
- Assistance in organizing complex legal entities
- Gaining access to investments in foreign jurisdictions that otherwise would be inaccessible due to the residency status of the investor

923. What are "special purpose vehicles"?

A special purpose vehicle (SPV), also known as a special purpose entity (SPE), bankruptcy-remote entity or orphan company, is a corporation, trust, partnership or limited liability company that is created for a limited purpose, generally to isolate financial risk. An SPE may be owned by one or more other entities. Similar to the business entities described above, SPEs can be exploited by criminals.

924. What are offshore financial centers?

Offshore financial centers (OFCs) are jurisdictions that have a relatively large number of financial institutions engaged primarily in business with nonresidents. OFCs are generally known for their favorable tax climate and bank secrecy laws. Some examples of OFCs include Bermuda, the British Virgin Islands, the Cayman Islands, Cyprus, the Isle of

Man and Panama. Additional information, including assessments of OFCs, can be found on the International Monetary Fund's (IMF) website: www.imf.org.

925. How is the term "beneficial owner" defined?

The term "beneficial owner" means an individual who has a level of control over, or entitlement to, the funds or assets in the account. This control or entitlement allows the individual (directly or indirectly) to control, manage or direct the account.

926. How is the term "bearer share ownership" defined?

Bearer share ownership is based on physical possession of the stock certificates.

927. As customers, do all of the business entities described above pose the same degree of risk?

No. The risks of each business entity should be assessed based on a variety of factors (e.g., entity was created by the financial institution [e.g., trust], status as an affiliate of a trusted entity, products/services offered by the entity, associated geographies, transaction activity). Status as the aforementioned business entity types is only one risk factor. Evaluating the risks of the business entities in this manner will result in different risk ratings (e.g., low, moderate, high).

928. Are there specific AML requirements for the aforementioned high-risk business entities?

Currently, there are no specific AML requirements for professional service providers. However, similar to guidance issued for professional service providers, key domestic and international groups such as the Financial Action Task Force (FATF) have highlighted the need for these high-risk business entities to establish AML controls due to their positions as "gatekeepers" and intermediaries to the financial system. In order to establish accounts at financial institutions, these business entities already may be required to implement basic AML controls to mitigate the risks associated with their business.

Additionally, assuming they are U.S. companies, all businesses are required to comply with Office of Foreign Assets Control (OFAC) laws and regulations. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

929. What guidance has been issued on high-risk business entities?

The following are examples of information and guidance that have been issued on high-risk business entities:

- **Business Entities (Domestic and Foreign) – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendations 24 – 25: Transparency and Beneficial Ownership of Legal Persons and Arrangements** (2012) by the Financial Action Task Force (FATF)
- **Potential Money Laundering Risks Related to Shell Companies** (2006) by the Financial Crimes Enforcement Network (FinCEN)
- **Company Formations – Minimal Ownership Information Is Collected and Available** (2006) by the U.S. Government Accountability Office (GAO)
- **The Misuse of Corporate Vehicles, Including Trust and Company Service Providers** (2006) by FATF
- **Wolfsberg FAQs on Beneficial Ownership** (2012) by the Wolfsberg Group
- **Wolfsberg FAQs on Intermediaries** (2012) by the Wolfsberg Group
- **Failure to Identify Company Owners Impedes Law Enforcement** by the United States Senate Permanent Subcommittee on Investigations (2006)
- **Tax Haven Abuses: The Enablers, the Tools and Secrecy** by the United States Senate Permanent Subcommittee on Investigations (2006)
- **Failure to Identify Company Owners Impedes Law Enforcement** by the United States Senate Permanent Subcommittee on Investigations (2006)

- **OFAC Regulations for the Corporate Registration Industry** (2004) by the Office of Foreign Assets Control (OFAC)

Correspondent Banking

930. How is the term "correspondent banking" defined?

The term "correspondent account" is defined broadly for banking organizations to include any account or formal relationship established by a financial institution to receive deposits from, make payments to or other disbursements on behalf of a foreign financial institution, or to handle other financial transactions related to the foreign financial institution.

In the case of securities broker-dealers, futures commission merchants (FCMs) and introducing brokers (IBs) in commodities and mutual funds, a correspondent account would include, but not be limited to, any account or formal relationship that permits the foreign financial institution to engage in regular services, including, but not limited to, those established to engage in trading or other transactions in securities and commodity futures or options, funds transfers, or other types of financial transactions.

931. What is the heightened money laundering and terrorist financing risk of correspondent accounts?

Correspondent banking relationships may expose the U.S. financial system to heightened money laundering and terrorist financing risk if they are established for foreign financial institutions located in jurisdictions with nonexistent or weak AML laws and regulations. Additionally, correspondent banking involves high-volume, international transactions involving multiple parties in which no one institution may have a direct relationship with all parties involved nor have a complete view of the entire transaction.

932. As customers, do all correspondent banking customers pose the same degree of risk?

No. The risks of each correspondent banking customer should be assessed based on a variety of factors, including, but not limited to, the following:

- The nature of, and markets served by, the foreign respondent's business
- The type, purpose and anticipated activity of the foreign respondent's account
- The nature and duration of the relationship with the foreign respondent (and any of its affiliates)
- The AML and supervisory regime of the jurisdiction that issued the charter or license to the foreign respondent
- The AML and supervisory regime of the jurisdiction in which any company that is an owner of the foreign respondent is incorporated or chartered (if reasonably available)
- Information known or reasonably available about the foreign respondent's AML record

Evaluating the risks of correspondent banking customers in this manner will result in different risk ratings (e.g., low, moderate, high).

933. Are there specific AML requirements for correspondent banking customers?

Yes. Due to the high-risk nature of correspondent banking, Section 312 of the USA PATRIOT Act, formally referred to as "Special Due Diligence for Correspondent Accounts and Private Banking Accounts," outlines specific due diligence and enhanced due diligence required to be conducted by financial institutions that have correspondent banking customers. Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks prohibits U.S. financial institutions from establishing relationships with foreign shell banks. Section 319 – Forfeiture of Funds in U.S. Interbank Accounts outlines circumstances in which funds can be seized from a U.S. interbank account. Foreign respondents that maintain correspondent accounts with any U.S. bank or U.S. broker-dealer in securities must provide a "foreign bank certification" that certifies the following:

- Physical presence/regulated affiliated status
- Prohibition of indirect use of correspondent accounts by foreign shell banks
- Ownership status (for nonpublic institutions)

Additionally, Section 311 – Special Measures imposes requirements ranging from additional recordkeeping requirements to the collection of information relating to beneficial ownership, payable through accounts (PTAs) and correspondent accounts to outright prohibitions against a foreign jurisdiction, financial institution, or classes of international transactions or types of accounts.

Recently, the United States imposed sanctions on Iran under the Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA), the Iran Threat Reduction and Syria Human Rights Act of 2012 (ITRSHRA) and the National Defense Authorization Act for Fiscal Year 2012 (NDAA) that require the U.S. Treasury Department to issue regulations restricting or prohibiting the opening or maintenance of correspondent or payable through accounts (PTA) by designated foreign financial institutions including but not limited to foreign financial institutions affiliated with the Government of Iran, the Central Bank of Iran, Iranian-linked financial institutions and financial institutions that facilitate significant transaction(s) or provides financial services to the (Islamic Revolutionary Guard Corps) IRGC or any of its agents or affiliates or to financial institutions subject to U.S. blocking requirements.

For additional guidance on Iranian sanctions, please refer to the Iranian Sanctions Overview section.

934. What guidance has been issued on correspondent banking?

The following are examples of information and key guidance that have been issued on correspondent banking:

- **Correspondent Banking – Overview (Domestic and Foreign)** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 13: Correspondent Banking** (2012) by the Financial Action Task Force (FATF)
- **Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking** (2002) by The New York Clearing House Payments Co., LLC
- **Wolfsberg AML Principles for Correspondent Banking** (2012) by the Wolfsberg Group
- **Wolfsberg Frequently Asked Questions on Correspondent Banking** (2012) by the Wolfsberg Group
- **The Wolfsberg Group and the Clearing House Association: Cover Payments: Some Practical Questions Regarding the Implementation of the New Payments** (2009) by the Wolfsberg Group
- **Correspondent Account KYC Toolkit: A Guide to Common Documentation Requirements** (2010) by the International Finance Corporation (IFC), the private sector arm of the World Bank Group
- **Application of Correspondent Account Rules to the Presentation of Negotiable Instruments Received by a Covered Financial Institution for Payment** (2008) by Financial Crimes Enforcement Network (FinCEN)
- **Application of the Correspondent Account Rule to Executing Dealers Operating in Over-the-Counter Foreign Exchange and Derivatives Markets Pursuant to Prime Brokerage Arrangements** (2007) by FinCEN
- **Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries** (2006) by FinCEN
- **Application of the Regulations regarding Special Due Diligence Programs for Certain Foreign Accounts to NSCC Fund/SERV Accounts** (2006) by FinCEN
- **Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-border Wire Transfers** (2008) by the Basel Committee on Banking Supervision of the Bank of International Settlements (BIS)
- **Role of U.S. Correspondent Banking in International Money Laundering** by the United States Senate Permanent Subcommittee on Investigations (2001)
- **U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History** by the United States Senate Permanent Subcommittee on Investigations (2012)

For additional guidance on correspondent banking, please refer to the following sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks, Section 319 – Forfeiture of Funds in U.S. Interbank Accounts, Foreign Bank Certifications, and Section 311 – Special Measures.

Nonbank Financial Institutions

935. What is meant by the term "nonbank financial institution" (NBFI)?

For purposes of our discussion, NBFIs include all entities, excluding depository institutions, considered financial institutions under the USA PATRIOT Act. These include, but are not limited to, the following:

- Money services businesses (MSBs)
- Broker-dealers
- Futures commission merchants (FCMs) and introducing brokers (IBs)
- Commodity trade advisers (CTAs)
- Commodity pool operators (CPOs)
- Mutual funds
- Insurance companies
- Casinos and card clubs
- Trust companies
- Operators of credit card systems
- Dealers in precious metals, stones or jewels
- Persons involved in real estate settlements and closings
- Investment advisers
- Unregistered investment companies
- Loan or finance companies
- Nonbank Residential Mortgage Lenders and Originators (RMLO)
- Housing Government Sponsored Enterprises (GSE)
- Businesses engaged in vehicle sales, including automobile, airplane and boat sales
- Travel agencies
- Pawnbrokers
- Telegraph companies

For additional guidance on nonbank financial institution customers, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

936. What are the heightened money laundering and terrorist financing risks of nonbank financial institution customers?

The following characteristics heighten the money laundering and terrorist financing risks of NBFIs:

- Cash-intensiveness
- High volume of transactions
- High-risk nature of customer base (e.g., high net worth; geographically dispersed; financially sophisticated; increased use of corporate structures, such as offshore private investment companies; lack of ongoing relationships with customers, such as MSBs and casinos)

- High-risk product offerings (e.g., ability to transfer funds domestically and internationally, particularly to jurisdictions with weak AML requirements; stored-value cards; transportability of merchandise; high-value merchandise; merchandise that is difficult to trace, such as precious stones)
- Ability to store and transfer value (e.g., conversion to precious gems, immediate or deferred income through insurance and other investment products, real estate)
- Grants access to funds held in foreign financial institutions or gives foreigners access to funds held in domestic financial institutions
- Subject to varying, often fewer, levels of regulatory requirements and oversight as compared to traditional financial institutions (e.g., banks, credit unions)
- Potentially weaker controls than traditional financial institutions
- Difficulty in monitoring for suspicious activity due to complex nature of transactions (e.g., involvement of multiple third parties, therefore decreasing transparency of transaction details)
- Operation without proper registration or licensing (e.g., MSBs)
- History of abuse by money launderers and terrorists

937. Are there specific AML requirements for NBFIs?

Some NBFIs are currently subject to their own AML requirements. For example, money services businesses (MSBs) and broker-dealers are required to establish a risk-based AML Compliance Program, and file Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs). Some financial institutions that establish account relationships with NBFIs review the AML Compliance Program of NBFIs as part of the due diligence process of their customer acceptance and maintenance programs.

For further guidance on the AML requirements of NBFIs, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

938. Are NBFIs required to comply with OFAC and other sanction regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. In addition, under limited circumstances, OFAC sanctions apply to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

Charitable Organizations and Nongovernmental Organizations

939. How are the terms “charitable organizations” and “nongovernmental organizations” defined?

A charitable organization is generally defined as an organization that is established and operated for purposes that are beneficial to the public interest. Private charitable organizations generally receive funding from an individual, family, corporation or other singular source, whereas public charities solicit funds from the general public. Specific definitions of charitable organizations and related requirements (e.g., registration, tax filing) are determined by the laws and regulations within the jurisdiction(s) in which the charitable organization is established and/or operates. Charitable organizations can be based locally, regionally, nationally or internationally.

Nongovernmental organizations (NGOs) are organizations that are independent from government. Some are for-profit organizations, but the majority of NGOs are not-for-profits with a wide range of causes (e.g., human rights abuses, environmental degradation).

940. What are the heightened money laundering and terrorist financing risks of charitable organizations?

The heightened risk of charitable organizations lies in the following:

- Cash-intensive

- Lack of transparency in complex transactions
- Increased frequency of international transactions
- Global presence facilitates quick transfer of funds internationally
- Varied source of funds (e.g., funds received from donors around the world)
- Subject to little or no oversight

Historically, NGOs and charities have been susceptible to abuse by terrorists.

941. As customers, do all charitable organizations pose the same degree of risk?

No. The risks of each charitable organization should be assessed based on a variety of factors (e.g., the strength of AML laws in the home country, affiliation with a trusted entity, reputation of the principals/owners, nature and geography of volunteer, donor and recipient base, size and geography of operations, purpose of the charitable organization, funding and disbursement criteria). Evaluating the risks of charitable organizations in this manner will result in different risk ratings (e.g., low, moderate, high).

942. Are there specific AML requirements for charitable organizations?

Currently, there are no specific AML requirements for charitable organizations. However, key domestic and international groups such as the Financial Action Task Force (FATF) have highlighted the need for charitable organizations to establish AML controls due to their risk of being abused by money launderers and financiers of terrorism. In order to establish accounts at financial institutions, charitable organizations already may be required to implement basic AML controls to mitigate the risks associated with their work.

Additionally, assuming they are U.S. companies, all charitable organizations are required to comply with Office of Foreign Assets Control (OFAC) laws and regulations. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

943. What agency is responsible for providing oversight of charitable organizations?

The IRS Tax Exempt and Government Entities Division (IRS-TEGE) provides federal oversight to all nonprofit organizations in the United States through the review of applications for tax-exempt status and subsequent audits. The IRS-TEGE also conducts examinations of applications and returns filed to determine if the nonprofit organizations are facilitating terrorist financing.

944. What guidance has been issued on charitable organizations?

The following are examples of key guidance that has been issued on charitable organizations:

- **Nongovernmental Organizations and Charities – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 8: Non-profit Organizations** (2012) by the Financial Action Task Force (FATF)
- **FATF Interpretive Note to Special Recommendation Eight: Non-Profit Organizations** (2012) by FATF
- **FATF International Best Practices for Combating the Abuse of Non-Profit Organizations** (2002) by FATF
- **Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities** (2010) by the U.S. Department of the Treasury
- **Office of Foreign Assets Control Regulations for Non-Governmental Organizations** (2012) by the Office of Foreign Assets Control (OFAC)
- **Risk Matrix for the Charitable Sector** (2006) by OFAC
- **Frequently Asked Questions on NGO Registration Numbers** (2002) by OFAC

Third-Party Payment Processors

945. What is a third-party payment processor?

Third-party payment processors (TPPPs) provide services that include, but are not limited, to the following:

- Check clearing
- Debit/credit cards processing
- ATM networks
- Remote deposit capture (RDC) services
- Automated clearing house (ACH) networks

Financial institutions and retailers, also referred to as merchants, utilize third-party payment processors to assist with their payment processing needs. Additionally, third-party payment processors may be customers of financial institutions that may use their accounts to conduct payment processing for their merchant clients.

946. What is the relationship between a merchant and a payment processor?

A merchant is a business that has contracted with an acquirer for card-processing services and accepts credit cards as a method of payment for goods or services. Information from the merchant is transferred through a payment gateway to a TPPP for processing.

947. What is a payment gateway?

A payment gateway is a secure e-commerce connection that authorizes payments for e-businesses, online retailers, bricks and clicks businesses, or traditional brick and mortar businesses.

948. Is a payment gateway the same as a payment processor?

No. A payment gateway is software running on a server that receives information from a company's website (or virtual terminal) and passes it securely along to the payment processor. The payment processor receives the information from the gateway and handles the transfer of money from the customer's account to the company's bank account.

949. What are the heightened money laundering and terrorist financing risks of third-party payment processors?

Third-party payment processors are considered higher risk because they are not subject to AML requirements and their accounts at the financial institution are used to conduct payment processing services for merchants with whom financial institutions may not have a direct relationship. This increases risk because of the complexity of verifying the merchant identities and business practices, and the difficulty in identifying the nature and the source of the transactions.

950. What types of merchants are considered higher-risk?

Merchants that pose a higher risk to fraud, money laundering and terrorist financing include, but are not limited to, the following:

- Online gambling operations
- Payday lenders
- Mail order and telephone order companies
- Telemarketing companies
- Adult entertainment businesses
- Entities located in high-risk jurisdictions (e.g., offshore)

Some higher-risk merchants routinely use third-party payment processors to process their transactions because of the difficulty they have in establishing a direct account relationship.

951. What are some examples of due diligence that should be conducted on customers that are third-party payment processors?

Following are examples of the type of due diligence that can be performed on customers who are third-party payment processors:

- Review the third-party payment processor's corporate documentation, including independent reporting services, contracts or references.
- Review public databases, such as the Better Business Bureau (BBB) and Federal Trade Commission (FTC), to identify potential problems or concerns with the merchant, Independent Sales Organization (ISO) and/or principal owners.
- Review the third-party payment processor's and merchant's promotional materials and website to determine the target clientele.
- Determine if the processor resells its services to a third party who may be referred to as an "agent or provider of ISO (independent sales organization) opportunities."
- Review the processor's policies, procedures and processes to determine the adequacy of due diligence standards for new merchants.
- Identify the major lines of business and volume for the processor's customers.
- Verify directly, or through the processor, that the merchant is operating a legitimate business by comparing the merchant's identifying information against public record, fraud and bank check databases.
- Visit the processor's business operations center.

952. What is an independent sales organization?

The FDIC defines an independent sales organization (ISO) as an "outside company contracted to procure new merchant relationships."

953. What type of information can a financial institution request about a third-party payment processor's merchants in order to better understand the relationship?

Financial institutions can request the following merchant information:

- Merchant's name
- Principal business activity
- Geographic location
- Sales techniques, such as telemarketing, online sales, etc.
- Charge-back history, including rates of return for ACH debit transactions and remotely created checks (RCCs)
- Method of credit card payment (i.e., swiping the credit card versus keying in the card number)
- Consumer complaint history

954. What is a remotely created check?

A remotely created check (RCC), also known as a demand draft, telecheck, preauthorized draft, paper draft or digital check, is a payment instrument that is typically created by the payee when an account holder authorizes a payee to draw a check on his or her account but does not sign the check. In lieu of a signature, the RCC may bear the customer's printed name or a statement that the customer authorized the RCC. Because RCCs do not have signatures, they are more difficult to authenticate and therefore more susceptible to fraud.

955. Are third-party payment processors included in the definition of money services businesses?

No. A money services business (MSB) is defined as any organization offering one or more of the following services:

- Issuer and sellers of money orders and traveler's checks
- Check casher
- Dealer in foreign exchange
- Provider or seller of prepaid access
- Money transmission (domestic or international)

According to FinCEN Ruling 2003-8, a merchant payment processor, also known as a third-party payment processor, processes payments from consumers as an agent of the merchant to which the consumers owe money, rather than on behalf of the consumers themselves; therefore, it does not meet the regulatory definition of a money transmitter. The role of the merchant payment processor in these transactions is to provide merchants with a portal to a financial institution that has access to the payment system (e.g., ACH, etc.); it is not to transmit funds on behalf of third parties. For further guidance on MSBs, please refer to the Money Services Businesses section.

956. Are there specific AML requirements for third-party payment processors?

Generally, there are no specific AML requirements for third-party payment processors; however, in order to establish accounts at financial institutions, payment processors already may be required to implement basic AML controls to mitigate the risks associated with their services.

Additionally, participants in some payment systems (i.e., ACH systems, card systems, check collection systems, money transmitting businesses, wire transfer systems) are required to comply with the Unlawful Internet Gambling Enforcement Act (UIGEA) and Regulation GG. For further guidance, please refer to the Unlawful Internet Gambling Enforcement Act section.

957. How should third-party payment processors be monitored for potentially suspicious activity?

Financial institutions should examine the accounts of third-party payment processors for potentially suspicious activity by monitoring for common red flags including, but not limited to, the following:

- There are high rates of returns/charge-back history (e.g., ACH debit transactions and RCCs returned for insufficient funds and/or as unauthorized). A high charge-back history is often indicative of merchants processing fraudulent transactions such as unauthorized ACH debits (e.g., customer discontinues a service, therefore stops payment; however, merchant continues to process ACH debits), fraudulent checks (e.g., unauthorized RCCs, altered payees, amounts, dates).
- There is significant variance in expected/historical activity versus actual activity in terms of the volume and types of transactions conducted through the account.

Since many financial institutions will not have access to the underlying details of transactions conducted by merchants, they must rely on the monitoring conducted by their third-party payment processors to detect potentially suspicious activity. As stated above, financial institutions should conduct appropriate due diligence of third-party payment processors at the inception of the relationship, including a review of applicable merchant due diligence and monitoring programs.

For additional guidance on red flags, please refer to the Suspicious Activity Red Flags section.

958. Are third-party payment processors obligated to report potentially suspicious activity of their merchants?

Businesses that function solely as third-party payment processors (i.e., are not included in the definition of “financial institution” per AML laws and regulations) are currently not required to file SARs; however, as stated above, participants in some payment systems are required to report suspected illegal gambling activities of its merchants pursuant to the Unlawful Internet Gambling Enforcement Act (UIGEA) and Regulation GG. For further guidance, please refer to the Unlawful Internet Gambling Enforcement Act section.

959. What guidance has been issued on third-party payment providers?

The following are examples of guidance that has been issued on third-party payment providers:

- **Third-Party Payment Processors – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 17: Reliance on Third Parties** (2012) by the Financial Action Task Force (FATF)
- **Retail Payment Systems** and **Wholesale Payment Systems Booklet** (2010) within the FFIEC Information Technology Examination Handbook by the FFIEC
- **Third-Party Senders and the ACH Network: An Implementation Guide** (2012) by The Electronic Payments Association (NACHA) (formerly National Automated Clearing House Association)

- **Bank Use of Foreign-Based Third-Party Service Providers** (2002) by the Office of the Comptroller of the Currency (OCC)
- **Risk Management Principles for Third-Party Relationships** (2002) by the OCC
- **Payment Processor Relationships** (2012) by the Federal Deposit Insurance Corporation (FDIC)
- **Guidance on Managing Third-Party Risk** (2008) by the FDIC

Privately Owned Automated Teller Machines (ATMs)

960. What is a "privately owned automated teller machine (ATM)"?

A privately owned automated teller machine is an ATM not owned by a financial institution. Privately owned ATMs are often found in convenience stores, bars, restaurants, grocery stores and check-cashing establishments.

961. What are the heightened money laundering and terrorist financing risks associated with privately owned ATMs?

Privately owned ATMs are considered high risk because U.S. law enforcement has observed an increase in their use in money laundering, identity theft and fraud schemes. Owners of privately owned ATMs may use illicit cash to replenish their ATMs, as opposed to legitimate sources (e.g., cash from sales, cash from a financial institution).

Additionally, most states do not monitor or require registration of owners of privately owned ATMs, thereby making it difficult to track current owners.

962. How can financial institutions identify which customers have privately owned ATMs?

If due diligence does not include an inquiry as to whether the customer maintains a privately owned ATM, financial institutions may be able to identify these customers by performing site visits and/or monitoring the accounts of select high-risk customers (e.g., stores, bars, restaurants, grocery stores, check-cashing establishments) for spikes in cash activity.

963. What steps can a financial institution take to mitigate the risks of customers with privately owned ATMs?

To mitigate the risk of privately owned ATM relationships, financial institutions should perform initial and ongoing due diligence on privately owned ATM relationships. They also should consider including contractual commitments advising of the financial institution's expectations with respect to preventing the use of the machines for illicit activities, requiring notification of a change in ownership and monitoring shipments for unusual activity.

964. What type of due diligence can be collected on privately owned ATM relationships?

Following are examples of the type of due diligence that may be performed on privately owned ATM relationships:

- Review corporate documentation, licenses, permits, contracts or references.
- Review public databases to identify potential problems or concerns with principal owners or an independent sales organization (ISO).
- Review existing relationships with other financial services providers (e.g., sources of replenishment currency, method of delivery of currency shipment).
- Review expected volumes.
- Review and/or visit locations of privately owned ATMs.

965. What is an independent sales organization (ISO)?

The FDIC defines an independent sales organization (ISO) as an "outside company contracted to procure new merchant relationships." For additional guidance on independent sales organizations, please refer to the Third-Party Payment Processors section.

966. How can privately owned ATMs be monitored for suspicious activity?

Financial institutions should monitor privately owned ATMs for suspicious activity by comparing expected versus actual ATM activity levels, and also compare the level of activity to other privately owned or bank-owned ATMs in comparable geographic and demographic locations. For additional guidance on red flags for potentially suspicious activity, please refer to the sections: Suspicious Activity Red Flags and Privately Owned ATM Red Flags.

High-Risk Products, Services and Transactions

967. What products/services/transactions pose a higher money laundering and terrorist financing risk?

Products/services that allow unlimited third-party transactions (e.g., demand deposit accounts), those that operate with limited transparency (e.g., Internet banking, telephone banking, pouch activity, prepaid access, ATM, trust), and those that may involve significant international transactions (e.g., correspondent banking) pose the highest risk.

Transactions that are processed quickly and electronically for customer convenience (e.g., wire transfers), are difficult to trace (e.g., cash), and are negotiable (e.g., monetary instruments, drafts, bearer securities, stored-value cards) also are susceptible to money laundering and terrorist financing.

968. What is a third-party transaction?

A third-party transaction is defined as a transfer of funds to/from the account holder to/from an individual/entity that is different than the account holder. It includes all types of transactions (e.g., wires, checks), regardless of direction (i.e., incoming, outgoing). “Third party” distinguishes the recipient/sender of the funds from the account holder. The individual/entity also can be a customer of the same financial institution, although the risk is greater when the individual/entity is not a customer of the financial institution, as the latter was not subject to the same customer acceptance procedures. Examples of third-party transactions are provided below:

- **Example 1**: Customer John sends a wire to beneficiary Jane from his deposit account. The deposit account allows third-party activity.
- **Example 2**: Customer John establishes a loan with Bank ABC and wishes to disburse the proceeds of the loan to his business partner, Jane. The financial institution’s policy does not allow loan proceeds to be disbursed to a third party, as Jane is a third party.
- **Example 3**: Customer John established a CD account with Bank ABC and wishes to liquidate the CD and disburse the funds to his wife, Jane. The financial institution’s policy does not allow funds from the CD to be disbursed to a third party.

Currency Transactions

969. What do the terms “currency” and “cash” mean?

Currency and cash are defined differently for Currency Transaction Reports (CTR) and Form 8300 reporting requirements.

- For CTRs, currency means the coin and paper money of the United States or any other country, which is circulated and customarily used and accepted as money.
- “Cash” is defined, for Form 8300 purposes, as:
    - U.S. and foreign coin and currency received in any transaction
    - A cashier’s check, money order, bank draft or traveler’s check having a face amount of $10,000 or less received in a designated reporting transaction, or received in any transaction in which the recipient knows that the instrument is being used in an attempt to avoid reporting requirements

For further guidance, please refer to the sections: Currency Transactions, Currency Transaction Reports and Form 8300.

970. What are the heightened money laundering and terrorist financing risks of currency transactions?

The vast majority of criminal dealings are conducted in cash. The inability to trace the origin or owner heightens the money laundering and terrorist financing risk of currency transactions. Currency transactions are typically used during the placement phase of money laundering.

971. Are there specific AML requirements for currency transactions?

Yes. The following are required for large currency transactions:

- **Currency Transaction Reports (CTRs)**: CTRs are reports filed by certain types of financial institutions for cash currency transactions of more than $10,000 in one business day. Multiple transactions must be treated as a single transaction (aggregated) if the financial institution has knowledge the transactions are by or on behalf of the same person and result in cash-in or cash-out totaling more than $10,000 in any one business day. For additional guidance, please refer to the Currency Transaction Reports section.
- **Form 8300**: Form 8300 should be completed and submitted to the IRS if a person engaged in trade or business who, in the course of that trade or business, receives more than $10,000 in single or multiple related transactions in:
    - Cash; or
    - Covered monetary instruments that are either received in a "designated reporting transaction" or in a transaction in which the recipient knows the monetary instrument is being used to try to avoid the reporting of the transaction.

  For additional guidance, please refer to the Form 8300 section.
- **Report of International Transportation of Currency or Monetary Instruments (CMIR)**: The CMIR is required to be filed by:
    - Each person who physically transports, mails or ships, or causes to be physically transported, mailed or shipped, currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time from the United States to any place outside of the United States or into the United States from any place outside of the United States; and
    - Each person who receives U.S. currency or other monetary instrument(s) in an aggregate amount exceeding $10,000 at one time, which has been transported, mailed or shipped from any place outside of the United States.

  For further guidance, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

Additionally, in instances where potentially suspicious activity is detected, a financial institution may need to file a Suspicious Activity Report (SAR). For further guidance, please refer to the Suspicious Activity Reports section.

972. How can currency transactions be monitored for potentially suspicious activity?

Financial institutions should examine currency transactions for suspicious activity by monitoring for common red flags such as:

- Deposits of currency just below the reportable threshold conducted with multiple branches, tellers, accounts and/or on different days
- Deposits of currency by multiple individuals into the same account
- Deposits of currency wrapped in currency straps that have been stamped by other financial institutions
- Frequent exchanges of small dollar denominations for large dollar denominations

For additional guidance, please refer to the sections: Currency Red Flags, Bulk Shipments of Currency Red Flags, Branch and Vault Shipments Red Flags, and Safe Deposit Box Red Flags.

Bulk Shipments of Currency

973. What does the term “bulk shipment of currency” mean?

The FFIEC Manual defines a bulk shipment of currency as “the use of common, independent, or postal service air/land/sea carriers to transport large volumes of bank notes (U.S. or foreign) from sources either inside or outside the United States to a bank in the United States. Often, but not always, shipments take the form of containerized cargo.”

Financial institutions can receive bulk shipments of currency, directly or indirectly through cash letter notifications. When received through cash letters, the currency is received by the Federal Reserve Bank, where it is recorded as held on the financial institution’s behalf.

974. Who are common shippers of bulk currency?

Common shippers of bulk currency include:

- **Currency originators** are individuals and businesses, foreign or domestic, who generate currency from cash sales of commodities or other products or services (including monetary instruments or exchanges of currency).
- **Intermediaries** are other banks, central banks, nondeposit financial institutions or agents of these entities that ship currency gathered from their customers who are currency originators or other intermediaries.

975. What does the term “cash letter” mean?

A cash letter, also known as a transit letter, is a group of negotiable items (e.g., checks, drafts) accompanied with documentation that lists the number of items, total dollar amount, and instructions for transmittal to a clearinghouse, a correspondent bank or a Federal Reserve Bank.

976. What does the term “cash smuggling” mean?

Cash smuggling is the smuggling of or the attempt to smuggle more than $10,000 in currency or monetary instruments into or out of the United States, with the specific intent to evade the U.S. currency-reporting requirements.

Common methods of smuggling cash include, but are not limited to, the following:

- Transport in commercial and private passenger vehicles
- Commercial airline shipments
- Passengers and pedestrians crossing U.S. borders with Mexico and Canada

Smuggled cash is often repatriated into the United States through the receipt of bulk currency shipments.

977. What are the heightened money laundering and terrorist financing risks of bulk shipments of currency?

Bulk shipments of currency are considered a higher risk service because of the following:

- Complex transactions involving multiple parties that may disguise the source of currency
- Involvement of foreign financial institutions that may or may not be complicit in the laundering of illicit currency
- An increase in the use of bulk shipments of currency as a method for reintegrating currency into U.S. financial institutions as observed by U.S. law enforcement

978. What steps can a financial institution take to mitigate the risk of bulk shipments of currency?

To mitigate the risk of bulk shipments of currency, financial institutions may consider adding these provisions to the signed contract with the shipping party:

- Each party’s responsibilities
- Expectations about due diligence

- Circumstances under which the financial institution will not accept bulk currency shipments
- Permitted third-party usage of the shipper's services

979. Should enhanced controls be applied only to foreign shipments of bulk currency?

No. There are varying degrees of risks associated with interstate shipments and shipments along international borders as well as foreign shipments of bulk currency. Appropriate controls should be applied to bulk shipments of currency, whether of domestic or foreign origin.

980. What can a financial institution do to assess the risk posed by a relationship that intends to conduct bulk shipments of currency?

To assess the risk of bulk shipments of currency, financial institutions should conduct a risk assessment to identify relationships and transactions that present a higher risk of money laundering or terrorist financing. The factors used to assess the risk of bulk shipments of currency may include the following:

- Ownership
- Geographies
- Nature and source of currency
- Control of bulk currency

In addition to conducting a risk assessment, financial institutions should use the risk assessment to drive the collection of due diligence on relationships that intend to conduct bulk shipments of currency, and monitor shipments for unusual activity.

981. What types of due diligence can be collected on relationships that intend to conduct bulk shipments of currency?

The following are examples of the types of due diligence that may be collected on relationships that intend to conduct bulk shipments of currency:

- Intended use of the relationship
- Expected volumes
- Sources of funds
- Reasonableness of volumes based on originators and shippers

In addition to collecting the due diligence above, financial institutions should consider periodic site visits to assess the legitimacy of the source of funds.

982. How can bulk shipments of currency be monitored for suspicious activity?

Financial institutions can monitor bulk cash shipments for suspicious activity by conducting a comparison of expected versus actual shipping volumes, monitoring for spikes in activity with foreign currency dealers or exchangers also known as *casas de cambio*, and monitoring for significant changes in branch and vault shipments. For additional guidance on indicators of potentially suspicious activity, please refer to the Suspicious Activity Red Flags, Bulk Shipments of Currency Red Flags and Branch and Vault Shipments Red Flags sections.

983. Are financial institutions required to file Reports of International Transportation of Currency or Monetary Instruments (CMIRs) on shipments of bulk currency?

Yes. Any shipment of currency outside of the United States that is greater than $10,000 must be reported via FinCEN Form 105, Report of International Transportation of Currency or Monetary Instruments (CMIR). For additional guidance, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

984. Are financial institutions required to file CMIRs on shipments of currency via the postal service?

31 CFR 103.23 exempts the CMIR reporting requirement if currency is shipped via the postal service or common carrier. However, currency shipped by other methods, including via air courier or the airlines, is not exempt. For

additional guidance on requirements of and exemptions to the filing of CMIRs, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

985. Are financial institutions required to file Currency Transaction Reports (CTRs) for currency shipments?

Yes. For all receipts or disbursement of currency in excess of $10,000, financial institutions are required to file a CTR. For additional guidance, please refer to the Currency Transaction Reports section.

986. Does the filing of CMIRs obviate the financial institution's responsibility for filing CTRs or vice versa for the same shipment of currency?

No. The reporting requirements of CMIRs and CTRs are independent of each other. The financial institution may have to file one or both, depending on the amount and how the bulk currency was transported.

987. Does the filing of CMIRs or CTRs obviate the financial institution's responsibility to monitor for potentially suspicious activity in its shipments of bulk currency?

No. A financial institution is still responsible for monitoring for potentially suspicious activity, regardless of whether a CMIR or CTR is filed.

988. What guidance has been issued on bulk shipping and/or smuggling of currency?

The following guidance has been issued on the bulk shipping and/or smuggling of currency:

- **Guidance to Financial Institutions on the Repatriation of Currency Smuggled into Mexico from the U.S.** (2006) by the Financial Crimes Enforcement Network (FinCEN)
- **FATF Recommendation 32: Cash Couriers** (2012) by the Financial Action Task Force (FATF)
- **Bulk Cash Smuggling Center (BCSC),** a centralized source for information and support for identifying, investigating and disrupting bulk cash smuggling activities around the world established by the U.S. Immigration and Customs Enforcement (ICE) agency

Funds Transfers

989. What does the term "funds transfer" mean?

According to the Funds Transfer Recordkeeping Requirement, a funds transfer is a series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order. The term includes any payment order issued by the originator's bank or an intermediary bank intended to carry out the originator's payment order. A funds transfer is completed by acceptance by the beneficiary's bank of a payment order for the benefit of the beneficiary of the originator's payment order. Funds transfers governed by the Electronic Fund Transfer Act of 1978, as well as any other funds transfers made through an automated clearing house (ACH), ATM or a point-of-sale (POS) system, are excluded from this definition.

990. What are the heightened money laundering and terrorist financing risks of funds transfers?

Wire transactions can move funds quickly and internationally, and in some instances, with limited transparency (e.g., online, remote access, cover payments). Funds transfers typically are used during the layering and integration phases of money laundering.

991. Are there specific AML requirements for funds transfers?

Yes. The following are required for funds transfers:

- **Funds Transfer Recordkeeping Requirement**: The basic requirements of the Funds Transfer Recordkeeping Requirement vary depending on the role the financial institution plays in the funds transfer (e.g., originating institution, intermediary institution, beneficiary institution). For each funds transfer of $3,000 or more, the originating institution is required to obtain and retain information including, but not limited to, the name and address of the originator, the amount of the payment order, the execution date of the payment order, and the name and address of the beneficiary.

- **Travel Rule**: The Travel Rule refers to the requirement for financial institutions that participate in funds transfers of $3,000 or more to pass along certain information about the funds transfer to the next financial institution involved in the funds transmittal. The requirements of the Travel Rule vary depending on the role the financial institution plays in the funds transfer (e.g., originating institution, intermediary institution). For additional guidance, please refer to the Funds Transfer Recordkeeping Requirement and Travel Rule section.
- **Office of Foreign Assets Control (OFAC) Sanctions Screening**: All U.S. financial institutions are required to screen transactions, including funds transfers, for possible OFAC Sanctions violations. For additional guidance, please refer to the sections Office of Foreign Assets Control and International Government Sanctions Programs and Blocking and Rejecting Transactions.

In instances where potentially suspicious activity is detected, a financial institution may need to file a Suspicious Activity Report (SAR). For further guidance, please refer to the Suspicious Activity Reports section.

Additionally, FinCEN recently issued a proposed rule that would impose additional recordkeeping requirements for "cross-border electronic transmittals of funds" (CBETF). For further guidance, please refer to the Cross-Border Electronic Transmittals of Funds section.

992. Do the CFPB's remittance rules impose additional AML-related requirements on financial institutions?

No. The CFPB's remittance rules, which amend Regulation E, are intended to protect consumers who send money electronically to foreign countries by providing more information about the costs of remittances. The rules apply to most international remittances regardless of their purpose, including, but not limited to funds transfers and automated clearing house (ACH) transactions. Specifically, the rules would require the following:

- Disclosures including:
    - A prepayment disclosure (listing the exchange rate, fees and taxes, and the amount to be delivered abroad) at the time the person initiates; and
    - A receipt disclosure which must be provided to the sender once the payment has been made.
- A provision that consumers can cancel a transfer within 30 minutes (and sometimes more) of originating it;
- Requirements that companies must investigate problems consumers report about transfers and provide standards for error resolutions;
- Companies are made responsible for mistakes made by certain people who work for them; and
- Provisions relating to transfers pre-scheduled on a regular basis.

The rules are applicable to banks, thrifts, credit unions, money transmitters and broker-dealers that consistently execute 100 or more remittance transfers per calendar year and apply to remittance transfers that are more than $15, made by a consumer in the United States, and sent to a person or company in a foreign country. The rules are effective February 7, 2013, though at the time of the publication of this Guide there continues to be significant industry pressure to delay the implementation given the perceived burden on the industry, particularly smaller institutions. The CFPB has provided model forms as well as a International Funds Transfer Small Entity Compliance Guide; these and other information related to the rules can be found on the CFPB's website at http://www.consumerfinance.gov/regulations/final-remittance-rule-amendment-regulation-e.

993. How can funds transfers be monitored for potentially suspicious activity?

Financial institutions should examine funds transfers for suspicious activity by monitoring for common red flags such as:

- Frequent, large, round dollar wire transactions
- A large deposit followed by numerous, smaller wire transactions
- Several deposits, particularly in currency or monetary instruments, followed by international wire transactions
- Wire transfers to and from bank secrecy haven countries and countries known for or linked to terrorist activities, drug trafficking, illegal arms sales or other illegal activity
- Unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity

For additional guidance, please refer to the Wire Transfer Red Flags section.

994. What guidance has been issued on funds transfers?

The following are examples of key guidance that has been issued on fund transfers:

- **Funds Transfers Recordkeeping — Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 16: Wire Transfers** (2012) by the Financial Action Task Force (FATF)
- **The Wolfsberg Group and the Clearing House Association: Cover Payments: Some Practical Questions Regarding the Implementation of the New Payments Messages** (2009) by Wolfsberg
- **Alternative Remittance Systems and Terrorism Financing: Issues in Risk Management** (2009) by the World Bank
- **Bilateral Remittance Corridor Analysis (BRCA)** (2007) by the World Bank
- **Regulatory Frameworks for Hawalas and Other Remittance Systems** (2005) by the International Monetary Fund (IMF)
- **Feasibility of a Cross-Border Electronic Funds Transfer Reporting System under the Bank Secrecy Act** (2010) by FinCEN
- **Implications and Benefits of Cross-Border Funds Transmittal Reporting** (2010) by FinCEN
- **Fact Sheet: Cross-Border Electronic Transmittal of Funds** (2010) by FinCEN
- **Funds "Travel" Regulations: Questions and Answers (Background Information and Notes)** (2010) by FinCEN

Automated Clearing House Transactions

995. How has the use of ACH transactions evolved?

ACH transactions are commonly utilized for direct deposits of payroll, government benefits and tax refunds and payments of consumer bills (e.g., mortgages, utility bills, insurance premiums). The most significant growth in the use of ACH transactions has occurred with nonrecurring payments including, but not limited to, the following:

- Accounts receivable conversion (ARC)
- Point-of-purchase (POP)
- Internet-initiated (WEB)
- Telephone-initiated (TEL)
- Re-presented check (RCK) entries

996. Are ACH transactions limited to domestic payments?

No. ACH transactions can be processed for both domestic and international (cross-border) payments.

997. What are the heightened money laundering and terrorist financing risks of ACH transactions?

The risks of ACH transactions differ depending on whether the entity is originating, receiving or processing ACH transactions, or outsourcing these activities to a third party.

An ACH transaction may be conducted with a high degree of anonymity, especially since an originator is not obligated to conduct an ACH transaction with a financial institution with which that originator has an account. This increases the product's risk. Additionally, ACH activity permits the originator to execute numerous payments for multiple receivers in one transaction, helping to disguise the source and beneficiary of the movement of funds. This same function of ACH enables large volumes of funds to be moved and can be done very rapidly. As a result, the ability of an individual or entity to hide the source of illicit funds is great with ACH transactions, thus heightening its risk of money laundering and terrorist financing.

998. Do all ACH transactions pose the same risk?

No. There is increased risk with nonrecurring ACH payments, ACH transactions processed on behalf of high-risk customers (e.g., online gambling operations, payday lenders, mail order and telephone order companies, adult entertainment businesses), ACH transactions initiated through non-face-to-face methods (e.g., telephone, Internet), ACH transactions initiated through third-party payment providers and cross-border ACH transactions.

999. What is the role of the Electronic Payments Association (formerly known as the National Automated Clearing House Association)?

The Electronic Payments Association (NACHA) issues rules and guidance for acceptable business, operating and risk management practices within electronic payment systems, including the ACH network. NACHA also provides training, facilitates communication between ACH Network members, and acts as a liaison between regulatory and government bodies.

Additional information on NACHA's role and responsibilities is available at http://www.nacha.org/.

1000. Who are the participants in an ACH system?

According to the FFIEC BSA/AML Examination Manual, participants within an ACH system include the following:

- The **originator** is an organization or person that initiates an ACH transaction to an account either as a debit or credit.
- The **originating depository financial institution (ODFI)** forwards the ACH transaction into the national ACH network through an ACH operator.
- The **ACH operator** processes all ACH transactions that flow between different financial institutions. An ACH operator serves as a central clearing facility that receives entries from the ODFIs and distributes the entries to the appropriate receiving depository financial institution (RDFI).
- The **receiving depository financial institution (RDFI)** receives the ACH transaction from the ACH operators and credits or debits funds from their receivers' accounts.
- The r**eceiver** is an organization or person that authorizes the originator to initiate an ACH transaction, either as a debit or credit to an account.
- The **gateway operator (GO)** is a financial institution, ACH operator or ODFI that acts as an entry or exit point to or from the United States. A formal declaration of status as a gateway operator is not required. ACH operators and ODFIs acting in the role of gateway operators have specific warranties and obligations related to certain international entries. A financial institution acting as a gateway operator generally may process inbound and outbound debit and credit transactions. ACH operators acting as gateway operators may process outbound debit and credit entries, but can limit inbound entries to credit entries only and reversals.

For international ACHs, the NACHA operating rules define the following two new participants:

- A **foreign correspondent bank** is defined as a participating depository financial institution (DFI) that holds deposits owned by other financial institutions and provides payment and other services to those financial institutions.
- A **foreign gateway operator (FGO)** acts as an entry point to or exit point from a foreign country.

1001. How many ACH operators exist in the United States?

There are currently two ACH operators:

- **FedACH** is a central clearing facility for transmitting and receiving domestic ACH payments.
    - **FedGlobal** sends cross-border ACH credits payments to more than 35 countries around the world, plus debit payments to Canada only. Both the FedACH and FedGlobal are operated by the Federal Reserve.
- **Electronic Payments Network (EPN)** is the only private-sector version of the FedACH.

1002. What roles can third-party service providers and third-party senders play in the ACH Network?

According to the OCC, a third-party service provider (TPSP) is "an entity other than an originator, ODFI or RDFI that performs any functions on behalf of the originator, the ODFI or the RDFI with respect to the processing of ACH entries. The functions of these TPSPs can include, but are not limited to, the creation of ACH files on behalf of the Originator or ODFI, or acting as a sending point of an ODFI (or receiving point on behalf of an RDFI)."

Third-party senders, a subset of TPSPs, are "bank customers to which originators outsource payment services, but the bank has no direct customer or contractual relationship with the originator. The third-party sender provides services to the originator and, in that capacity, acts as an intermediary between the originator and the ODFI."

1003. Are there specific AML requirements for ACH transactions and/or ACH operators?

Generally, there are no specific AML requirements for operators of ACH systems/third-party payment processors; however, in order to establish accounts at financial institutions, payment processors already may be required to implement basic AML controls to mitigate the risks associated with their services. Businesses that function solely as operators of ACH systems/third-party payment processors (e.g., are not included in the definition of "financial institution" per AML laws and regulations) are currently not subject to AML requirements.

OFAC has issued very specific regulations with respect to cross-border ACH transactions, formally known as International Automated Clearing House transactions (IAT). For further guidance, please refer to the Automated Clearing House Transactions and IATs section.

Additionally, participants in some payment systems (e.g., ACH systems, card systems, check collection systems, money transmitting businesses, wire transfer systems) are required to comply with the Unlawful Internet Gambling Enforcement Act (UIGEA) and Regulation GG. For further guidance, please refer to the Unlawful Internet Gambling Enforcement Act section.

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. For further guidance on professional service providers, please refer to the Professional Service Providers section.

1004. Does filing an ACH Data Breach Form relieve a financial institution's obligation to file a SAR?

No. The ACH Data Breach Form is designed to identify instances where nonproprietary information (e.g., account numbers) may have been compromised during the processing of an ACH transaction. If the financial institution is required to file SARs, the ACH Data Breach Form would not relieve a financial institution's obligation to file a SAR when potentially suspicious activity has been detected. For further guidance on SARs, please refer to the Suspicious Activity Reports section.

1005. How can ACH activity be monitored for potentially suspicious activity?

Financial institutions should examine ACH transactions for suspicious activity by monitoring for common red flags such as:

- There are high rates of returns/charge-back history (e.g., ACH debit transactions returned for insufficient funds and/or as unauthorized). A high charge-back history is often indicative of merchants processing fraudulent transactions such as unauthorized ACH debits (e.g., customer discontinues a service, therefore stops payment; however, merchant continues to process ACH debits).
- There is significant variance in expected/historical activity versus actual activity in terms of the volume and types of transactions conducted through the account.

Since many financial institutions will not have access to the underlying details of many ACH transactions, they may have to rely on the monitoring conducted by third-party payment processors to detect potentially suspicious activity. As stated above, financial institutions should conduct appropriate due diligence of third-party payment processors at the inception of the relationship, including their due diligence and monitoring programs. For further guidance on red flags, please refer to the Suspicious Activity Red Flags section.

In addition, financial institutions should consider incorporating NACHA's Originator Watch List into their due diligence and monitoring program. Administered by NACHA's Risk Investigations & Services, the Originator Watch List identifies originators and third-party senders that are considered high-risk. Inclusion on the Originator Watch List does

not imply any prohibition on initiating entries for entities listed and is only available to employees of financial institutions that utilize the ACH network, regional payments associations and ACH operators. For further guidance on due diligence for third-party payment processors, please refer to the Third-Party Payment Processors section.

1006. Do the CFPB's remittance rules impose additional AML-related requirements on automated clearinghouse transactions?

No. The CFPB's remittance rules, which amend Regulation E, are intended to protect consumers who send money electronically to foreign countries by providing more information about the costs of remittances. The rules apply to most international remittances regardless of their purpose, including, but not limited to funds transfers and automated clearing house (ACH) transactions. Specifically, the rules would require the following:

- Disclosures including:
    - A prepayment disclosure (listing the exchange rate, fees and taxes, and the amount to be delivered abroad) at the time the person initiates; and
    - A receipt disclosure which must be provided to the sender once the payment has been made.
- A provision that consumers can cancel a transfer within 30 minutes (and sometimes more) of originating it;
- Requirements that companies must investigate problems consumers report about transfers and provide standards for error resolutions;
- Companies are made responsible for mistakes made by certain people who work for them; and
- Provisions relating to transfers pre-scheduled on a regular basis.

The rules are applicable to banks, thrifts, credit unions, money transmitters and broker-dealers that consistently execute 100 or more remittance transfers per calendar year and apply to remittance transfers that are more than $15, made by a consumer in the United States, and sent to a person or company in a foreign country. The rules are effective February 7, 2013, though at the time of the publication of this Guide there continues to be significant industry pressure to delay the implementation given the perceived burden on the industry, particularly smaller institutions. The CFPB has provided model forms as well as an International Funds Transfer Small Entity Compliance Guide; these and other information related to the rules can be found on the CFPB's website at http://www.consumerfinance.gov/regulations/final-remittance-rule-amendment-regulation-e.

1007. What key guidance has been issued on ACH activities?

The following are examples of guidance that has been issued on ACH activities:

- **Automated Clearing House Transactions – Overview** (2010) within the FFIEC BSA/AML Examination Manual by the FFIEC
- **Automated Clearing house Activities – Risk Management Guidance** (2006) by the Office of the Comptroller of the Currency (OCC)
- **International ACH Transaction (IAT) Frequently Asked Questions** (2012) by the Federal Reserve Financial Services
- **FedGlobal® Frequently Asked Questions** (2010) by the Federal Reserve Financial Services
- **Guidance to National Automated Clearing House Association (NACHA) on Domestic and Cross-border ACH Transactions** (2004) by OFAC
- **Update on OFAC Requirements for Gateway Operators' Processing of Inbound IAT Debits** (2009) by NACHA
- **NACHA Operating Rule & Guidelines** by NACHA (2012)
- **Comptroller's Handbook: Merchant Processing** (2001) by the OCC
- **FFIEC IT Examination Handbook on Retail Payment Systems** (2006) by the FFIEC

Monetary Instruments

1008. What does the term "monetary instrument" mean?

Monetary instruments include bank checks or drafts, foreign drafts, cashier's checks, money orders or traveler's checks.

1009. What are the heightened money laundering and terrorist financing risks of monetary instruments?

Similar to cash, the inability to trace the origin or owner heightens the money laundering and terrorist financing risk of monetary instruments. Monetary instruments are typically used during the layering phase of money laundering (e.g., transfers between bank accounts of related entities or charities for no apparent reason).

1010. Are there specific AML requirements for monetary instruments?

Yes. The following is required for monetary instruments:

- **Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments**: A financial institution that issues or sells for currency a monetary instrument (e.g., bank check or draft, foreign draft, cashier's check, money order, traveler's check) for amounts between $3,000 and $10,000 inclusive must first obtain specific information if the individual has a deposit account at the institution (e.g., name of the purchaser, date of purchase, type of instrument purchased, amount, serial numbers). For additional guidance, please refer to the Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments section.
- **Form 8300**: Form 8300 should be completed and then submitted to the IRS if a person engaged in trade or business who, in the course of that trade or business, receives more than $10,000 in single or multiple related transactions in:
    - Cash, or
    - Covered monetary instruments that are either received in a "designated reporting transaction" or in a transaction in which the recipient knows the monetary instrument is being used to try to avoid the reporting of the transaction.

  For additional guidance, please refer to the Form 8300 section.
- **Report of International Transportation of Currency or Monetary Instruments (CMIR)**: The CMIR is required to be filed by:
    - Each person who physically transports, mails or ships, or causes to be physically transported, mailed or shipped, currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time from the United States to any place outside of the United States or into the United States from any place outside of the United States; and
    - Each person who receives U.S. currency or other monetary instrument(s) in an aggregate amount exceeding $10,000 at one time, which has been transported, mailed or shipped from any place outside of the United States.

In October 2011, FinCEN proposed amending the definition of "monetary instruments" to include tangible prepaid access devices that would be subject to reporting on CMIRs; no final rule on this proposed change has yet been issued. For further guidance on CMIRs and prepaid access, please refer to the sections Report of International Transportation of Currency or Monetary Instruments and Prepaid Access, Stored Value and E-Cash.

Additionally, in instances where potentially suspicious activity is detected, a financial institution may need to file a Suspicious Activity Report (SAR). For further guidance, please refer to the Suspicious Activity Reports section.

1011. How can monetary instruments be monitored for potentially suspicious activity?

Financial institutions should examine monetary instruments for suspicious activity by monitoring for common red flags such as:

- Monetary instruments purchased on the same or consecutive days at different locations, and/or are numbered consecutively in amounts designed to evade reporting requirements (i.e., under $3,000 or $10,000), or are purchased in round amounts

- Blank payee lines
- Instruments which contain the same stamp symbol or initials

For additional guidance, please refer to the Monetary Instruments Red Flags section.

1012. What guidance has been issued on monetary instruments?

The following key guidance has been issued on monetary instruments:

- **Purchase and Sale of Monetary Instruments Recordkeeping – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 32: Cash Couriers** (2012) by the Financial Action Task Force (FATF)
- **Guidance – International Best Practices: Detecting and Preventing the Illicit Cross-Border Transportation of Cash and Bearer Negotiable Instruments** (2012) by the Financial Action Task Force (FATF)

U.S. Dollar Drafts

1013. What is a U.S. dollar draft?

A U.S. dollar draft is a bank draft or check denominated in U.S. dollars, which is offered by foreign financial institutions and drawn on a U.S. correspondent account of the foreign financial institution.

1014. What are the heightened money laundering and terrorist financing risks of U.S. dollar drafts?

U.S. dollar drafts are considered higher risk because, historically, they have been susceptible to abuse by money launderers, particularly in the layering and integration phases. For example, criminals are able to convert smuggled cash into a U.S. dollar draft purchased at a foreign financial institution in order to integrate the funds back into the U.S. financial system.

FinCEN, for instance, has long cautioned about schemes to launder smuggled currency from drug trafficking and other criminal activities back into the United States from Mexico through the purchase of a “Mexican bank draft” – a U.S. dollar denominated draft drawn on a Mexican bank’s U.S. correspondent. The draft may be carried into the United States and negotiated or endorsed to a third party who negotiates the draft at the U.S. correspondent institution or uses the money to buy goods that are ultimately converted into cash. In all scenarios, the draft eventually finds its way back to the U.S. bank on which it was drawn.

1015. What steps can a financial institution take to mitigate the risk associated with its foreign financial institutions providing U.S. dollar drafts?

U.S. dollar drafts are one of many foreign correspondent banking services used by foreign financial institutions, also known as foreign respondents. Due to the risks associated with foreign correspondent banking, Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts of the USA PATRIOT Act outlines the following sample due diligence and enhanced due diligence that should be conducted on these high-risk relationships:

- Determine whether a correspondent account, because it allows U.S. dollar drafts or other high-risk products/services, is subject to enhanced due diligence requirements under Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts of the USA PATRIOT Act.
- Assess the money laundering and terrorist financing risk posed, based on a consideration of relevant risk factors such as:
    - The nature of, and markets served by, the foreign respondent’s business.
    - The type, purpose and anticipated activity of the foreign respondent’s account.
    - The nature and duration of the relationship with the foreign respondent (and any of its affiliates).
    - The AML and supervisory regime of the jurisdiction that issued the charter or license to the foreign respondent.

    - The AML and supervisory regime of the jurisdiction in which any company that is an owner of the foreign respondent is incorporated or chartered (if reasonably available).
    - Information known or reasonably available about the foreign respondent's AML record.

- Apply risk-based policies, procedures and controls to each such respondent reasonably designed to detect and report known or suspected money laundering or terrorist financing activity. Controls should include a periodic review of the respondent's account activity to determine consistency with information obtained about the type, purpose and anticipated activity of the account.

For additional guidance on due diligence for foreign correspondent banking customers, please see sections: Due Diligence for Correspondent Accounts, Enhanced Due Diligence for Correspondent Accounts.

1016. How should U.S. dollar drafts be monitored for potentially suspicious activity?

Financial institutions should examine accounts with U.S. dollar draft activity for suspicious activity by monitoring for common red flags such as:

- Significant variance in expected/historical activity versus actual activity in terms of the volume of U.S. dollar draft activity
- Dollar amounts that appear to be designed to evade reporting requirements (i.e., under $3,000 or $10,000) or are purchased in round amounts
- Multiple, sequentially numbered U.S. dollar drafts
- High volume of U.S. dollar drafts to the same payee or from the same remitter
- Drafts issued by *casas de cambio*
- Third-party endorsed drafts

In addition, financial institutions should obtain and consider information related to the respondent's AML Compliance Program and conduct enhanced monitoring of transactions to and from the account.

For additional guidance on red flags for potentially suspicious activity, please refer to the Suspicious Activity Red Flags section.

Pouch Activity

1017. What does the term "pouch activity" mean?

Pouch activity, also known as "pouch services" or "cash letters," is the use of a courier to transport currency, monetary instruments, loan payments and other financial documents from outside the United States to a U.S. financial institution. Pouches can be sent by another financial institution or by an individual and are commonly offered in conjunction with correspondent banking services.

1018. What are the heightened money laundering and terrorist financing risks of pouch activity?

Financial institutions often do not have any information on underlying clients and transactions within a pouch, as their account relationship is with the foreign respondent utilizing the pouch services. As such, financial institutions must rely on foreign respondents to conduct appropriate due diligence to mitigate risks of doing illicit business. The commingling of multiple client funds in the pouch may make it difficult for a financial institution to understand the source and purpose of incoming and outgoing funds.

The increased risk of pouch activities is also attributed to a high volume of international transactions and high-risk products (e.g., money orders, traveler's checks and bank checks) that are characteristic of pouch activity.

1019. What steps can a financial institution take to mitigate the risk of pouch activity?

To mitigate the risk of pouch activity, U.S. financial institutions should ensure they have a signed contract with the foreign financial institution that includes the following:

- Roles and responsibilities of each party

- Restrictions on types of transactions (e.g., monetary instruments with blank payee lines, unsigned monetary instruments and a large number of consecutively numbered monetary instruments)

In addition, financial institutions should collect due diligence on relationships that intend to conduct pouch activity, and monitor transactions for unusual activity.

1020. What type of due diligence can be collected on foreign financial institution relationships that intend to utilize pouch services?

Pouch services are one of many foreign correspondent banking services used by foreign financial institutions, also known as foreign respondents. Due to the risks associated with foreign correspondent banking, Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts of the USA PATRIOT Act outlines the following sample due diligence and enhanced due diligence that should be conducted on these high-risk relationships:

- Determine whether the account is subject to enhanced due diligence requirements under Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts of the USA PATRIOT Act.
- Assess the money laundering and terrorist financing risk posed, based on a consideration of relevant risk factors such as:
    - The nature of, and markets served by, the foreign respondent's business.
    - The type, purpose and anticipated activity of the foreign respondent's account.
    - The nature and duration of the relationship with the foreign respondent (and any of its affiliates)
    - The AML and supervisory regime of the jurisdiction that issued the charter or license to the foreign respondent.
    - The AML and supervisory regime of the jurisdiction in which any company that is an owner of the foreign respondent is incorporated or chartered (if reasonably available).
    - Information known or reasonably available about the foreign respondent's AML record.
- Apply risk-based policies, procedures and controls to each such respondent reasonably designed to detect and report known or suspected money laundering or terrorist financing activity. Controls should include a periodic review of the respondent's account activity to determine consistency with information obtained about the type, purpose and anticipated activity of the account.

For additional guidance on due diligence for foreign correspondent banking customers, please see sections: Due Diligence for Correspondent Accounts, Enhanced Due Diligence for Correspondent Accounts.

1021. How can pouch activity be monitored for potentially suspicious activity?

Financial institutions should examine pouch activity for suspicious activity by monitoring for common red flags such as:

- Monetary instruments purchased on the same or consecutive days at different locations, and/or are numbered consecutively in amounts designed to evade reporting requirements (i.e., under $3,000 or $10,000) or are purchased in round amounts
- Blank payee lines
- Instruments that contain the same stamp symbol or initials

For additional guidance, please see section: Suspicious Activity Red Flags.

1022. Are there specific AML requirements for pouch activities?

Yes. The content of pouches may be subject to the following reporting requirements:

- **Currency Transaction Reports (CTRs)**: CTRs are reports filed by certain types of financial institutions for cash currency transactions of more than $10,000 in one business day. Multiple transactions must be treated as a single transaction (aggregated) if the financial institution has knowledge that they are by or on behalf of the same person and result in cash-in or cash-out totaling more than $10,000 in any one business day. For additional guidance, please refer to the Currency Transaction Reports section.

- **Report of International Transportation of Currency or Monetary Instruments** (**CMIR)**: The CMIR is required to be filed by:
    - Each person who physically transports, mails or ships, or causes to be physically transported, mailed or shipped, currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time from the United States to any place outside of the United States or into the United States from any place outside of the United States; and
    - Each person who receives U.S. currency or other monetary instrument(s) in an aggregate amount exceeding $10,000 at one time, which has been transported, mailed or shipped from any place outside of the United States.

  For further guidance, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

Additionally, in instances where potentially suspicious activity is detected, a financial institution may need to file a Suspicious Activity Report (SAR). For further guidance, please refer to the Suspicious Activity Reports section.

Payable Through Accounts

1023. What does the term "payable through account" (PTA) mean?

A PTA, also known as a "pass through" or "pass-by" account, is an account maintained for a respondent that permits the respondent's customers to engage, either directly or through a subaccount, in banking activities (e.g., check writing, making deposits) usually in the United States.

1024. What are the heightened money laundering and terrorist financing risks of PTAs?

PTAs do provide legitimate business benefits, but the operational aspects of the accounts make them particularly vulnerable to abuse as a mechanism to launder money. Multiple individuals can have signatory authority over a single correspondent account and can, therefore, conduct transactions with limited transparency. Often, PTA arrangements are customers in less-regulated financial markets. Unless a financial institution is able to identify adequately and understand the transactions of the ultimate users of the respondent's bank account, there is significant potential risk for money laundering and terrorist financing.

1025. What is the difference between PTAs and traditional correspondent banking?

In traditional correspondent banking, customers do not have the authority to transact through the respondent's account on their own. In order to send or receive funds through the respondent's account, the customer must send instructions to the respondent so that the respondent can transact on behalf of the customer. In other words, with PTAs, customers of the respondent have direct access to the account.

1026. What steps can a financial institution take to mitigate the risk associated with PTAs?

To mitigate the risk of PTAs, financial institutions may consider adding the following provisions to the signed contract with the respondent financial institution:

- Roles and responsibilities of each party
- Limits or restrictions on transaction types and amounts (e.g., currency deposits, funds transfers, check cashing)
- Restrictions on types of subaccount holders (e.g., *casas de cambio*, finance companies, funds remitters or other nonbank financial institutions)
- Prohibitions or restrictions on multi-tier subaccount holders
- Access to the foreign financial institution's internal documents and audits that pertain to its PTA activity
- Requirement to obtain the same account opening information from subaccount holders as required by the PTA holding institution for its own direct customers and to make this information available as needed

In addition to conducting a risk assessment, financial institutions should collect due diligence on relationships that intend to conduct PTA activity and monitor transactions for unusual activity.

1027. What are some examples of due diligence that should be collected on foreign financial institution relationships that intend to conduct PTA transactions?

PTAs are one of many foreign correspondent banking services used by foreign financial institutions, also known as foreign respondents. Due to the risks associated with foreign correspondent banking, Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts of the USA PATRIOT Act outlines the following sample due diligence and enhanced due diligence that should be conducted on these high-risk relationships:

- Obtain and consider information related to the respondent's AML Compliance Program
- Conduct enhanced monitoring of transactions to and from the account
- Obtain and consider information about the identity of any person with authority to direct transactions through the PTA account
- Obtain and consider information on the identity of each owner of the respondent

For further guidance on the due diligence that should be conducted on foreign respondents, please refer to Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts.

1028. Are there specific AML requirements for PTAs?

Yes. The following are required for PTAs:

- **USA PATRIOT Act Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts**: In addition to outlining required due diligence for correspondent banking customers, Section 312 also outlines instances when a financial institution should consider terminating a PTA relationship:
    - Adequate information about the ultimate users of the PTAs cannot be obtained
    - Weak AML regulations and controls regarding customer identification and transaction monitoring exist in the jurisdiction of the foreign bank itself
    - Ongoing suspicious and unusual activities occur in the PTA
    - The financial institution is unable to conclude that PTAs are not being used for illicit purposes

  For further guidance on the due diligence that should be conducted on foreign respondents, please refer to Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts.

- **Iranian Sanctions pursuant to the Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA), the Iran Threat Reduction and Syria Human Rights Abuse Act of 2012 (ITRSHA) and the National Defense Authorization Act for Fiscal Year 2012 (NDAA):** Recently, the United States imposed sanctions on Iran under the Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA), the Iran Threat Reduction and Syria Human Rights Act of 2012 (ITRSHRA) and the National Defense Authorization Act for Fiscal Year 2012 (NDAA) that require the U.S. Treasury Department to issue regulations restricting or prohibiting the opening or maintenance of correspondent or payable through accounts (PTA) by designated foreign financial institutions including but not limited to foreign financial institutions affiliated with the Government of Iran, the Central Bank of Iran, Iranian-linked financial institutions and financial institutions that facilitate significant transaction(s) or provides financial services to the (Islamic Revolutionary Guard Corps) IRGC or any of its agents or affiliates or to financial institutions subject to U.S. blocking requirements.

  For additional guidance, please refer to the Iranian Sanctions Overview section.

Concentration Accounts

1029. What does the term "concentration account" mean?

Within the industry, a concentration account is an account that a financial institution uses to aggregate funds from different customers' accounts. Concentration accounts are also known as collection, intraday, omnibus, settlement, special-use or sweep accounts.

1030. What is the heightened money laundering and terrorist financing risk of concentration accounts?

Concentration accounts involve the commingling of different customers' funds. They also can involve the commingling of customer funds with a financial institution's funds in a way that conceals the identity of underlying parties to a transaction.

1031. How should concentration accounts be monitored for potentially suspicious activity?

Financial institutions should examine concentration accounts for suspicious activity by identifying and monitoring common red flags such as:

- Cash transactions for Currency Transaction Report (CTR) aggregation and filing purposes
- Employee access and use of concentration accounts
- Funds sent directly to a concentration account
- Exception reports for transactions processed in violation of the financial institution's policy

1032. Are there specific AML requirements for concentration accounts?

The USA PATRIOT Act introduces the possibility of future regulation relating to concentration accounts; however, the U.S. Treasury Department has not issued regulations. Financial institutions are advised to recognize and take appropriate actions to control the risks of these accounts by:

- Prohibiting financial institutions from allowing customers to direct transactions through a concentration account
- Prohibiting financial institutions and their employees from informing customers of the existence of the institution's concentration accounts
- Establishing written procedures governing documentation of transactions involving concentration accounts (e.g., capturing customer transactions in the customer's account statements, retaining appropriate transaction and customer identifying information)
- Establishing controls over the opening, maintenance and reconcilement of concentration accounts
- Subjecting concentration accounts to AML monitoring

Electronic Banking

1033. What does the term "electronic banking" mean?

Electronic banking, or e-banking, provides electronic delivery of financial products to customers. Examples of e-banking include automated teller machine (ATM) transactions; online account opening and banking transactions; telephone banking and remote deposit capture (RDC) services.

1034. What are the heightened money laundering and terrorist financing risks of electronic banking?

The lack of face-to-face contact in e-banking transactions heightens the risks of transactions conducted through this method. This introduces vulnerabilities such as exposure to unauthorized users and foreign jurisdictions.

Additionally, the reliance on third-party services, and in some cases providers, elevates the risk.

1035. What steps can a financial institution take to mitigate the risk associated with electronic banking?

To mitigate the risks associated with electronic banking, financial institutions may consider implementing the following:

- Limiting the types of transactions that can be conducted through electronic banking (e.g., information only, initiation of transactions)
- Imposing risk-based transaction limits and/or monitoring thresholds (e.g., per transaction, monthly)

- Limiting the opening of new accounts online to existing customers who have established relationships through a branch or other process involving face-to-face contact with an employee
- Applying additional controls (e.g., authentication) prior to executing transactions initiated through electronic banking methods

1036. What is the difference between electronic banking and e-cash?

Electronic banking generally refers to the method of access, whereas e-cash refers to the actual "value" that can be accessed through multiple methods, including, but not limited to, electronic banking. For further guidance on e-cash, please refer to the Prepaid Access, Stored-Value and E-Cash section.

Online Banking

1037. What does the term "online banking" mean?

Online banking, also known as Internet banking, refers to the method of e-banking in which a customer accesses financial services through an Internet connection.

1038. What steps can a financial institution take to mitigate the risks associated with online banking?

Financial institutions offering Internet-based products and services should use risk-based methods to authenticate the identity of customers using these products and services to safeguard customer information, prevent money laundering and terrorist financing, reduce fraud, and inhibit identity theft. For further guidance on identity theft, please refer to the CIP vs. Identity Theft Prevention Program section.

1039. Is "authentication" the same as "verification" as defined in Section 326 – Verification of Customer Information, also known as the Customer Identification Program (CIP)?

No. Authentication attempts to ensure that the individual providing the information, or accessing the account(s), is the person he or she claims to be. Authentication is accomplished by requesting information that is not necessarily "found in a wallet" (e.g., previous address, previous employer).

Verification confirms that the information provided by a customer is valid (e.g., an individual with the provided name, address and TIN matches with an independent source, such as a credit reporting database).

Often, once an individual has been verified, financial institutions will ask customers to create custom security questions (e.g., mother's maiden name, favorite movie, pet's name) that serve to authenticate customers.

1040. Is requiring a username and password an adequate control for online banking transactions?

No. Single-factor authentication (e.g., username/password) is inadequate for high-risk transactions (e.g., access to customer information and the movement of funds) as it is easier to compromise than multi-factor authentication methods. Additional methods of authentication include, but are not limited to, the following:

- Shared-secret techniques (e.g., personal identification numbers [PINs])
- Physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of "tokens"
- Biometric identification (e.g., fingerprint recognition, face recognition, voice recognition, retinal scan)
- Customer verification techniques
    - Positive verification ensures that material information provided by customers matches information from third-party sources.
    - Negative verification ensures that information provided is not linked to previous fraudulent activity.
    - Logical verification ensures that the information is consistent (e.g., area code of the home number is within the ZIP code of the address provided by the customer).

Automated Teller Machines

1041. Is single-factor authentication an adequate control for ATM transactions?

No. Two-factor authentication is most widely used with ATMs. For example, to withdraw money from an ATM, customers must present both an ATM card and a password or PIN.

1042. What is a "privately owned automated teller machine"?

A privately owned ATM is not owned by a financial institution. Privately owned ATMs are often found in convenience stores, bars, restaurants, grocery stores and check-cashing establishments.

1043. What are the heightened money laundering and terrorist financing risks associated with privately owned ATMs?

Privately owned ATMs are considered high risk because U.S. law enforcement has observed an increase in their use in money laundering, identity theft and fraud schemes. Owners of privately owned ATMs may use illicit cash to replenish their ATMs, as opposed to legitimate sources (e.g., cash from sales or a financial institution).

Additionally, most states do not monitor or require registration of owners of privately owned ATMs, thereby making it difficult to track current owners.

For additional guidance on privately owned ATM machines, please refer to the Privately Owned ATM Red Flags section.

Remote Deposit Capture

1044. What does the term "remote deposit capture" mean?

Remote deposit capture (RDC) is an electronic deposit delivery system by which customers deposit checks or monetary instruments into a bank account from a remote location via transmission to the financial institution of digital information or a scanned image, rather than delivery of the physical item (e.g., check, monetary instrument).

Scanning and transmission activities can take place at branches, ATMs, domestic and foreign correspondents, and locations owned or controlled by customers, as well as through the use of mobile technology such as mobile phones.

1045. How does RDC occur at remote locations controlled by customers?

Customers make deposits by scanning items from their homes or on the premises of their businesses utilizing RDC processing technology, and send images of deposit items for processing through check-clearing networks or the deposit data for processing and clearing through the ACH network.

1046. Are RDC services limited to checks and monetary instruments?

No. Some RDC services facilitate the electronic capture of cash and card payments.

1047. How can cash be deposited through RDC?

RDC also may include the electronic capture of deposit information comprised of cash through remote safekeeping arrangements at customer locations or through other intermediaries.

1048. Are RDC services limited to business customers?

No. Many RDC services allow individuals to make remote deposits utilizing smartphone technology.

1049. Are RDC services limited to scanning items from the home or premise of the customer?

No. Customers can make deposits utilizing RDC processing technology at their home or place of business, through a lockbox arrangement, through a mail drop or kiosk.

1050. What are the heightened money laundering and terrorist financing risks of RDC?

RDC is considered a higher-risk service since the financial institution never receives original physical items from customers, thereby increasing the risk of checks, money orders and traveler's checks being physically altered. This may increase the difficulty of complying with recordkeeping and reporting requirements and monitoring for potentially suspicious activity, such as sequentially numbered documents. RDC services increasingly are being utilized by foreign correspondent banking customers and money services businesses (MSBs) to replace pouch services and certain instrument processing and clearing activities.

Further, because RDC equipment is portable, it is difficult to ensure that the equipment is actually being used by the registered owner.

Additionally, operational risks at a business location include unauthorized access to technology systems and electronic data images, ineffective controls over physical deposit handling and storage procedures, and inadequate background checks on employees who have access to physical deposit items or technology.

1051. What steps can a financial institution take to mitigate the risk associated with RDC?

To mitigate the risks associated with RDC, a financial institution may consider adding the following provisions to the signed contract with customers establishing an RDC relationship:

- Each party's roles, responsibilities and liabilities
- Record retention expectations for RDC data
- Physical security of RDC equipment and original documents
- Expectations regarding controls to prevent the inappropriate use of RDC equipment
- Authority to request original documents, conduct audits and/or terminate RDC relationships

1052. What can a financial institution do to mitigate the risk posed by RDC customers?

To mitigate the risk associated with customers utilizing RDC services, a financial institution should conduct a suitability review on the customer prior to establishing the RDC relationship. Following are examples of factors that may be used to assess a customer's suitability:

- Nature of the customer's business compared to a list of acceptable types of businesses
- Credit history
- Financial statements
- Ownership structure
- Customer's risk management processes
- Geographic location of the operations

In addition to information collected during the suitability review, following are examples of due diligence that may be collected on customers who wish to establish an RDC relationship:

- Customer base
- Expected activity
- Type of activity (e.g., payroll checks, third-party checks or traveler's checks)
- Location of RDC technology

A financial institution may consider conducting site visits in order to evaluate the customer's operational controls in place, as well.

1053. How should RDC activities be monitored for potentially suspicious activity?

In addition to money laundering and terrorist financing risks, other risks include check fraud, check kiting and duplication of deposits through different channels, so financial institutions should train employees to be aware of these activities when monitoring RDC transactions. Common red flags include, but are not limited to, the following:

- High volume of rejected and returned items
- High volume of deposit items from foreign correspondent accounts, particularly those associated with money services businesses (MSBs) and *casa de cambios*
- Consistently poor image quality of scanned deposits
- High volume of checks missing endorsements or appearing altered
- Significant variance in expected/historical activity versus actual activity in terms of the volume and types of transactions conducted through the account
- Dollar amounts that appear to be designed to evade reporting requirements (i.e., under $3,000 or $10,000) or are purchased in round amounts
- Multiple, sequentially numbered monetary instruments

The utilization of interdictive software based on "negative databases" of customers previously associated with fraudulent activity is another effective method for detecting potentially suspicious activities. For additional guidance on red flags, please refer to the sections: Suspicious Activity Red Flags and Pouch Activity and Remote Deposit Capture.

1054. What can a financial institution do to mitigate the risks posed by RDC vendors?

Financial institutions should conduct due diligence on their RDC technology service providers and RDC hardware and software suppliers as part of their overall vendor management program. For additional guidance, please refer to the Third-Party Payment Processors section.

1055. What AML guidance has been issued on RDC and electronic banking activities?

The following are examples of information and key guidance that have been issued:

- **Electronic Banking – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **"Remote Deposit Capture" within Retail Payment System Overview** (2010) within the FFIEC IT Examination Handbook by the FFIEC
- **FATF Recommendation 15: New Technologies** (2012) by the Financial Action Task Force (FATF)
- **Interagency Guidance on Authentication in an Internet Banking Environment** (2005) by the FFIEC
- **E-Banking Booklet** (2003) by the FFIEC
- **Risk Management for Electronic Banking and Electronic Money Activities** (1998) by the Bank for International Settlements (BIS)
- **Security of Electronic Money** (1996) by the BIS
- **ML and TF Vulnerabilities of Commercial Websites and Internet Payment Systems** (2012) by the Financial Action Task Force (FATF)
- **Report on New Payment Methods** (2010) by FATF
- **Money Laundering in Cyberspace** (2006) by the World Bank (WB)
- **Mobile Phone Financial Services** (2008) Paper by the WB
- **Risk Management of Remote Deposit Capture** (2009) by the FFIEC
- **Guidance Addressing Risk Management of Remote Deposit Capture Activities** (2009) by FFIEC

The Office of the Comptroller of Currency (OCC) also provides online resources in "OCC Electronic Banking Guidance" including, but not limited to, the following:

- **Handbooks** (e.g., Electronic Banking, Retail Payments, Wholesale Payments, Supervision of Technology Service Providers)
- **Current regulations** (e.g., Final Rule on Electronic Banking)
- **Issuances (OCC Bulletins, alerts, advisory letters)**

- **OCC opinions and letters on permissible electronic banking activities** (e.g., Internet and PC banking, data processing electronic commerce, correspondent banking, electronic payments, sale and production of software, digital certification, excess capacity, Internet access, electronic safekeeping and storage)
- **OCC Research and Analysis**
    - Technological Innovation in Retail Payments: Key Developments and Implications for Banks (2004)
    - Internet Banking: Developments and Prospects, Economics Working Paper (2000, 2002)
    - Internet Banking in the U.S.: Landscape, Prospects, Industry Implications (2001) (Published in Capco Journal of Financial Transformation)
    - Report to the Congress on Review of Regulations Affecting Online Delivery of Financial Products and Services (2001) (jointly issued by the OCC, Federal Reserve, FIDC and OTS)
    - Who Offers Internet Banking? (2000)
    - Banking Over the Internet (1998)
    - Technological Innovation in Banking and Payments (1998)
    - The Report of the Consumer Electronic Payments Task Force (1998)
    - Toward Electronic Money and Banking: The Role of Government Conference Paper – An Introduction to Electronic Money Issues (1996)

Prepaid Access, Stored-Value and E-Cash

1056. What does the term “prepaid access” mean?

FinCEN’s final rule, “Definitions and Other Regulations Relating to Prepaid Access” (Prepaid Access rule) defines “prepaid access” as the following:

- Access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number or personal identification number.

1057. Why did the final rule rename “stored value” as “prepaid access”?

The final rule renamed “stored value” as “prepaid access” because the technology used in the stored-value industry has changed. The final rule provides flexibility so it will not become obsolete as the industry advances to encompass all emerging payment methods, including but not limited to personal identification numbers, electronic serial numbers, cards, tokens, key fobs, mobile phones, etc.

FinCEN stated that prepaid access is not itself a device or vehicle, but that devices or vehicles are means through which prepaid funds are accessed. The two main elements of prepaid access are:

- Funds that have been paid in advance; and
- Those funds that can be retrieved or transferred at some point in the future. FinCEN also clarified that it intended its definition to include the necessary regulatory elasticity to survive future technological advancements.

1058. What are the heightened money laundering and terrorist financing risks of prepaid access?

Transactions may involve funds that have been transferred to or from an unknown party or from a party that wants to engage in illicit transactions or money laundering. Law enforcement has voiced concerns in part due to the ease with which prepaid access can be obtained, the high velocity of money that potentially can be moved with prepaid access and the anonymous use of some prepaid access. However, unlike cash, there are records available for all of the transactions performed for a particular prepaid access device.

Following are examples of types of factors that may increase the risk associated with a prepaid access product:

- Reloadability
- High value/unlimited load amount

- Lack of account relationship with issuer and/or seller of the products
- Lack of identification of purchaser
- Source used to fund product is cash, credit card or another stored-value product
- Ability to conduct cross-border transactions
- Ability to make cash withdrawals

1059. Is the definition of prepaid access limited to cards?

No. The regulatory definition of prepaid access was designed to be applicable to emerging and developing technologies, which may include but are not limited to the following:

- Near field communications (NFC) (set of short-range wireless technologies that establish electromagnetic radio fields that enable devices to communicate with each other when touching or in close proximity)
- Chip technology
- Magnetic strips
- Cellular phones
- Prepaid access through the Internet using PINs/codes
- Prepaid access through fobs, tokens, chips or other technology
- E-cards
- Virtual currency

Prepaid access products encompass a large number of current and most of the emerging growth products, such as open-loop general purpose reloadable (GPR) cards, certain closed-loop cards, mobile phone access, fob or barcode access.

1060. Do all types of prepaid access products pose the same degree of risk?

No. FinCEN has issued guidance that the following types of prepaid access products pose lower risk:

- **Closed-loop prepaid access** - Prepaid access to funds or the value of funds with a maximum dollar threshold of $2,000 that can be used only for goods or services involving a defined merchant or location (or set of locations), such as a specific retailer or retail chain, a college campus, or a subway system;
- Devices that do not permit international use (e.g., use at foreign merchants via the Internet or face to face);
- Non-reloadable devices

1061. What is the difference between a closed-loop and open-loop prepaid access product?

Closed-loop prepaid access products are usable only at a specific merchant, or a group of merchants using the same branding, such as a Starbucks card. They may be in a fixed amount or reloadable. Open-loop prepaid access products may be used at multiple merchants, such as a prepaid card that contains a Visa logo and can be used at any merchant that accepts Visa debit cards. Open-loop cards may also come in fixed or reloadable amounts.

1062. Can a closed-loop prepaid access product be used to launder illicit funds?

As with any type of payment product or service, it is possible for a closed-loop prepaid access product to be misused. Law enforcement has identified instances where drug dealers used illicit funds to purchase closed-loop gift cards, and the cards were then used to purchase retail items. However, there have been very few reported incidents of misuse of either closed- or open-loop prepaid cards in the United States to date, especially for cards issued by a U.S.-based issuer.

1063. What does the term “e-cash” mean?

“E-cash,” also known as e-wallets or e-money, is a digital representation of money that can be stored and retrieved in several forms, including computer-based, mobile telephone-based and prepaid cards.

Computer-based e-cash is usually accessed via a computer or stored in an online repository. Mobile phone e-cash is often accessed through an individual's mobile phone number. Prepaid access and e-cash may be held in a pooled account at a bank. Such accounts may be used to transfer funds between users (e.g., people to people, people to business, business to business), make payments to merchants, allow for cash withdrawals, and many other functionalities.

Additional information on types of e-cash products is available in the FFIEC Information Technology Examination Handbook.

1064. Are banks required to comply with the final rule related to Providers and Sellers of Prepaid Access?

No. The final rule exempts banks and financial institutions regulated by the Securities and Exchange Commission (SEC) and the Commodities Futures Trading Commission (CFTC) from the definition of "provider" of prepaid access.

1065. What are the components of an effective risk management program for prepaid access programs?

On June 28, 2011, the Office of the Comptroller of the Currency (OCC) issued "Risk Management Guidance and Sound Practices" for prepaid programs. As with AML programs, the OCC suggests financial institutions implement a risk-based program to manage the AML, sanctions, fraud and third-party risks of its prepaid access program. An effective risk management program for prepaid access programs should include the following:

- Policies and procedures addressing the following:
    - Risk assessment of prepaid access products including product capabilities, regulatory requirements, competitive factors and other factors of the business model that would impact the risk/reward analysis of the program;
    - Due diligence on purchasers of prepaid access products;
    - Disclosures to purchasers about pricing, fees, transaction limits and credit features; and
    - Due diligence for selecting third-party service providers (TPSP) and oversight of TPSPs, including ongoing monitoring of regulatory obligations, information sharing, business continuity/disaster recovery and termination policy.
- Ongoing audit, self-assessment and compliance functions;
- Comprehensive management reporting to senior management and the board of directors.

1066. What steps can be taken to mitigate the risks associated with prepaid access products?

Following are examples of the types of steps that may be taken to mitigate the risk of prepaid access products:

- Monitor purchases, reloads and withdrawal activities for potential suspicious activity;
- Limit the amount of money that can be loaded over a specified period of time for higher-risk products;
- Limit the number of cards that can be purchased by an individual, or require enhanced due diligence to determine the reason for purchasing a large number of cards (for example, as holiday gifts for teachers or a charity event);
- Limit the dollar amount or location of ATM withdrawals on high-risk products; and
- Obtain identifying information from the purchaser or recipient for higher-risk products.

1067. What due diligence should be conducted on third-party service providers of prepaid access products?

Financial institutions that issue prepaid access products through a third-party service provider (TPSP) should manage risks by monitoring performance, suspicious activities and fraud losses of its third-parties. Financial institutions should also consider their consumer protection obligations when selecting a TPSP and design an effective prepaid access and compliance program.

The OCC suggests the following details be outlined in contracts/agreements with TPSPs:

- Regulatory obligations of each party, including monitoring and reporting of suspicious activity;
- Business continuity/disaster recovery plans for service disruptions and/or security breaches;
- Right of the financial institution to audit and monitor performance of the TPSP (e.g., review the prepaid access program and compliance program);
- Termination parameters (e.g., conditions under which the relationship with the TPSP can be terminated); and
- Process to share information about suspicious activities and fraud losses, and indemnify losses.

Following are examples of the types of due diligence that may be conducted on TPSPs, depending on the risks posed by both the products offered and the third-party itself:

- Review of corporate documentation, licenses, permits, contracts or references;
- Review of financial documentation such as credit reports, financial statements and tax returns;
- Background checks, including running all parties against the OFAC and sanctions lists;
- On-site visits;
- Review of TPSP's compliance program that includes the following:
    - Due diligence on purchasers
    - AML, sanction and fraud policy and procedures
    - Training
    - Independent assessments of program
    - Reports to the board of directors or senior management
- Review of AML audits/reviews of company-prepared self-assessments.

Some financial institutions develop training programs for TPSPs to assist in complying with AML laws and regulations. Some participants of prepaid access programs are now subject to their own AML requirements. For further guidance, please refer to the Providers and Sellers of Prepaid Access section.

1068. Are additional regulations expected for prepaid access?

Yes. The Consumer Financial Protection Bureau (CFPB) held a hearing in May 2012 regarding prepaid access, with a focus on general purpose reloadable (GPR) cards. CFPB is expected to issue additional regulations that may include the following:

- A definition for GPR cards;
- What current consumer protections apply to GPR cards under Regulation E;
- What disclosures will be required regarding fees;
- How to enable consumers to effectively compare various GPR cards;
- Whether consumers should be notified of the existence or lack thereof of FDIC pass-through insurance;
- Costs, benefits and consumer protection issues related to any credit or savings features of GPR cards;
- Efficacy of credit reporting features on GPR cards in enabling consumers to improve or build credit; and
- Regulatory compliance.

1069. What guidance has been issued on prepaid access?

The following are examples of information and guidance that have been issued on prepaid access:

- **"Prepaid Cards/Stored-Value Cards" subsection within Electronic Cash – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 15: New Technologies** (2012) by the Financial Action Task Force (FATF)

- **"E-Banking" and "Emerging Retail Payment Technologies" within the "Retail Payment Systems" sections within the FFIEC Information Technology Examination Handbook** by the FFIEC
- **Report on Money Laundering Using New Payment Methods** (2012) by FATF
- **Payroll Cards: An Innovative Product for Reaching the Unbanked and Underbanked** (2005) by the Office of the Comptroller of Currency (OCC)
- **The 2008 Survey of Consumer Payment Choice** by the Federal Reserve Bank of Boston
- **Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems** (2012) by FATF
- **Consumer Payment Choice: A Central Bank Perspective** by the Consumer Payments Research Center at the Federal Reserve Bank of Boston
- **Prepaid Cards: Vulnerable to Money Laundering?** (2007) by the Federal Reserve Bank of Philadelphia
- **The Laws, Regulations, Guidelines, and Industry Practices That Protect Consumers Who Use Gift Cards** (2008) by the Federal Reserve Bank of Philadelphia
- **Emerging Risk Forum "Cash, Check, or Cell Phone?" Protecting Consumers in a Mobile Finance World** (2010) by the Federal Reserve Bank of Boston
- **New Technologies, New Risks? Innovation and Countering the Financing of Terrorism** (2010) by the World Bank (WB)
- **Survey of Developments in Electronic Money and Internet and Mobile Payments** (2004) by the Bank of International Settlements (BIS)
- **Recommended Practices for Anti-Money Laundering Compliance for U.S.-Based Prepaid Card Programs** (2008) by the Network Branded Prepaid Card Association (NBPCA)
- **Person-to-Person Electronic Funds Transfers: Recent Developments and Policy Issues** (2010) by the Federal Reserve Bank of Boston
- **Understanding Risk Management in Emerging Retail Payments** (2008) the Federal Reserve Bank of New York

Additional organizations providing guidance on stored-value products include, but are not limited to, the following:

- Federal Reserve Bank of Boston Risk and Policy Analysis Unit
- Federal Reserve Bank of Boston Consumer Payments Research Center (CPRC)
- Federal Reserve Bank of Philadelphia Payment Cards Center
- Network Branded Prepaid Card Association (NBPCA)

Trade Finance Activities

1070. What does the term "trade finance" mean?

The term "trade finance" generally refers to the use of short-term financing to facilitate the import and export of goods. Such arrangements can involve payment if documentary requirements are met, such as through the use of a letter of credit, or through a commitment to make payment in the event the original party with the obligations defaults on the terms of the transaction (e.g., through use of a guarantee or a standby letter of credit). In such cases the bank's involvement in the finance activities helps to minimize risk of payment to importers and exporters.

Banks often participate in trade financing by providing pre-export financing, assisting the process of collection, confirming or issuing letters of credit, discounting drafts and acceptances, or offering fee-based services such as providing credit and country information on the buyers. Most trade financing is short term and self liquidating; however, medium-term loans of one to five years, or even longer-term loans, may be used to finance the import and export of capital goods such as machinery or equipment.

The Financial Action Task Force (FATF) defines trade finance to include nondocumentary trade activities (e.g., management of open account trading), whereas the Wolfsberg Group's definition limits trade finance to documentary trade finance activities (i.e., documentary letters of credit, documentary bills of collection).

1071. What are common trade finance instruments?

Common trade finance instruments include, but are not limited to, the following:

- **Letter of credit,** the most widely used trade finance instrument**,** is a formal commitment issued by a bank on behalf of and at the request of a customer, to pay a named beneficiary a stipulated amount of money upon presentation of specified documents set out in the terms and conditions detailed in the letter within a specified time frame. There are two types of letters of credit:
    - The **documentary or commercial letter of credit** is most commonly used to finance a commercial contract for the shipment of goods from seller to buyer by providing for the prompt payment of money to the seller when shipment is made as specified under its terms.
    - The **standby letter of credit** guarantees payment to the beneficiary by the issuing bank in the event of default or nonperformance by the account party (the bank's customer). Although a standby letter of credit may arise from a commercial transaction, it is not linked directly to the shipment of goods from seller to buyer.

  Documentary letters of credit are generally short-term payment instruments for trade finance, while standby letters of credit are written for any maturity or purpose (e.g., credit enhancement, loan guarantees, advance payment bonds, performance bonds).

  An "**irrevocable letter of credit**" is a commitment by the issuing bank to pay, provided the beneficiary complies with the terms and conditions of the letter of credit that cannot be changed unless all parties agree. Conversely, revocable letters of credit can be canceled or amended without notice to the beneficiary.

  A "**confirmed letter of credit**" is a letter of credit guaranteed by a second bank, in addition to the bank originally issuing the credit. The confirming bank agrees to pay or accept drafts against the credit even if the issuer refuses.

  A "**back-to-back letter of credit**" is a letter of credit issued on the strength of another letter of credit involving a related transaction and nearly identical terms.

- **A banker's acceptance** is a time draft drawn on and accepted by a bank that is often used as a short-term discount instrument in international trade. A bank in the importer's country acts on behalf of the exporter for collecting and remitting payments for shipment. The exporter presents the shipping and collecting documents to his or her own bank (in his or her own country), which then sends them to its correspondent bank in the importer's country. The foreign bank (called the presenting bank) hands over the shipping and title documents required for taking delivery of the shipment to the importer in exchange for cash payment (in the case of "documents against payments instructions") or a firm commitment to pay on a fixed date (in case of "documents against acceptance" instructions). The banks involved in the transaction act only in a fiduciary capacity to collect the payment but, unlike a documentary credit, make no guarantees. They are liable only for correctly carrying out the exporter's collection instructions and may, under certain circumstances and where so instructed, sue the non-paying or non-accepting importer on the exporter's behalf. In general, by accepting the draft, a bank makes an unconditional promise to pay the holder of the draft a stated amount at a specified date.
- **Documentary collection** refers to the trade finance instrument in which the exporter entrusts the collection of a payment to the remitting bank (exporter's bank), which sends documents to a collecting bank (importer's bank), along with instructions for payment. Funds are received from the importer and remitted to the exporter through the use of a draft that requires the importer to pay the face amount either on sight (document against payment) or on a specified date in the future (document against acceptance) once the specified terms have been met.
- **Open account trading** describes unsecured trade transactions in which the buyer and seller agree on the terms of the contract. Goods are delivered to the buyer, who then arranges a payment through the financial system. In other words, goods are shipped before payment is due (typically within 30 to 90 days). The majority of trade transactions are executed in this manner as opposed to financing involving prepayments, collections, letters of credit, etc.

1072. Is "trade finance" limited to international commerce?

In its broadest terms, trade finance can include both domestic and international commerce; however, in terms of addressing the risks of trade finance activities, more emphasis has been placed on the financing activities that facilitate international trade.

1073. What are the heightened money laundering and terrorist financing risks of trade finance activities?

The heightened risk of trade finance activities lies in the following:

- Difficulty in conducting adequate due diligence on multiple trade parties, including screening for possible sanctions violations and/or export prohibitions
- Use of shell/front companies to further thwart efforts to conduct due diligence on trade parties
- Trade parties located in jurisdictions with lax AML/CTF laws and regulations
- Susceptibility to documentary fraud due to complex, documentary-based transactions
- Diverse and complex financing arrangements
- Lack of transparency in complex transactions
- Increased frequency of international transactions
- Potential involvement with high-risk goods (e.g., weapons, nuclear materials or equipment, sensitive technical data, precious gems, crude oil)
- Difficulty in sharing trade information across international borders
- Among employees responsible for executing and monitoring trade finance transactions, lack of required specialized knowledge to determine effectively if a trade transaction is potentially suspicious for all types of goods

More recently, transactions related to the potential breach of sanctions, including the proliferation of weapons of mass destruction, has underscored the need to scrutinize trade finance activities for potentially suspicious activity.

1074. How is the term “trade-based money laundering” defined?

Trade-based money laundering (TBML) refers to the process of disguising the proceeds of illegal activity and moving value through the use of trade transactions so that they appear to come from legitimate sources or activities. Examples of TBML include the Black Market Peso Exchange (BMPE) and reintegro schemes.

Generally, the BMPE is an intricate money laundering system in which Colombian cartels sell drug-related U.S.-based currency to black market peso brokers in Colombia who, in turn, place the currency into U.S. bank accounts. The brokers then sell monetary instruments drawn on their bank accounts to Colombian importers who use them to purchase foreign goods, or they pay for goods directly on behalf of the importers with reimbursement upon delivery of the goods in Colombia. Although the BMPE in Colombia is one of the more widely known locations for such activities, BMPEs operate in other parts of the world, too.

“Reintegro” refers to a trade-based, reverse-BMPE laundering scheme that hinges on trade document manipulation and often includes the corruption of a bank employee or customs official. Unlike traditional BMPE activities that operate with goods (not funds) crossing the border, in reintegro transactions, peso exchange brokers repatriate drug proceeds by disguising them as payments for nonexistent or overvalued goods using purchased export papers, similar to letters of credit, to make the payments appear legitimate. This is known as “reintegro” or “reintegrate papers.”

1075. What is the International Chamber of Commerce?

The International Chamber of Commerce (ICC), established in 1919 with members in more than 130 countries, is a world business organization with a mission to promote trade and investment across frontiers and help business corporations meet the challenges and opportunities of globalization by establishing rules and policies to facilitate international trade and facilitating arbitration.

The ICC has issued standard rules and practices to facilitate international trade (e.g., The Uniform Customs and Practice for Documentary Letters of Credit (2007 Revision), ICC Publication No. 600; and The Uniform Rules for Collections, ICC Publication No. 522). These standard rules and practices assist financial institutions in establishing controls to mitigate the risks of trade finance without hindering business.

The ICC has also established the Commercial Crime Services (CCS) and Business Action to Stop Counterfeiting and Piracy (BASCAP) to assist in combating maritime piracy, financial fraud and counterfeiting.

1076. Who are the typical participants in a trade transaction?

The complex nature of trade activities requires the active involvement of multiple parties on both sides of the transaction. Participants typically include the following:

- **Trader** refers to anyone who facilitates the exchange of goods and related services across national borders, international boundaries or territories. Importers/exporters are businesses specifically organized to facilitate international trade; however, the term is commonly used to describe any business that conducts international trade transactions.
- **Trade Finance Parties** refers to the institutions that facilitate the financial component of a trade transaction (e.g., the financial institutions of the importer and exporter, intermediary financial institutions and nonfinancial institutions that provide conduits and services to expedite the payment flows and delivery of underlying documents associated with trade transactions).
- **Shipping Agents/Couriers** refers to the companies who prepare shipping documents, arrange shipping space and insurance, and deal with customs requirements.
- **Insurers** refers to the companies who provide insurance to protect against loss or damage of shipments. Many financial institutions require insurance to provide select trade financing services (e.g., letter of credit).
- **Trade/Customs Authorities** refers to the authorities who are responsible for collecting, analyzing or storing trade data. Trade data refers to information collected from import-export forms or supporting documentation (e.g., description of the goods being imported or exported, quantity, value, weight, customs or tariff code number, the mode of transportation by which the goods are being imported or exported, name and address of the exporter, importer, shipping company, financial or banking data). It is important to note that the collection, use and sharing of trade data is subject to international agreements between two or more countries.
- **Investigative Authorities** refers to the authorities who are responsible for investigating money laundering, terrorist financing and/or the underlying predicate offense (e.g., customs fraud, smuggling, narcotics trafficking). In some cases, customs authorities will not have the responsibility or authority to conduct such investigations.

1077. What roles can banks play in trade finance transactions?

According to the FFIEC BSA/AML Examination Manual, banks can play the following roles:

- **Issuing Bank**. The bank that issues the letter of credit on behalf of the Applicant (e.g., buyer, importer) and advises it to the Beneficiary (e.g., buyer, exporter) either directly or through an Advising Bank. The Applicant is the Issuing Bank's customer.
- **Confirming Bank**. Typically in the home country of the Beneficiary, at the request of the Issuing Bank, the bank that adds its commitment to honor draws made by the Beneficiary, provided the terms and conditions of the letter of credit are met.
- **Advising Bank**. The bank that advises the credit at the request of the Issuing Bank. The Issuing Bank sends the original credit to the Advising Bank for forwarding to the Beneficiary. The Advising Bank authenticates the credit and advises it to the Beneficiary. There may be more than one Advising Bank in a letter of credit transaction. The Advising Bank may also be a Confirming Bank.
- **Negotiation**. The purchase by the nominated bank of drafts (drawn on a bank other than the nominated bank) or documents under a complying presentation, by advancing or agreeing to advance funds to the beneficiary on or before the banking day on which reimbursement is due to the nominated bank.
- **Nominated Bank**. The bank with which the credit is available or any bank in the case of a credit available with any bank.
- **Accepting Bank**. The bank that accepts a draft, providing a draft is called for by the credit. Drafts are drawn on the Accepting Bank that dates and signs the instrument.
- **Discounting Bank**. The bank that discounts a draft for the Beneficiary after it has been accepted by an Accepting Bank. The Discounting Bank is often the Accepting Bank.
- **Reimbursing Bank**. The bank authorized by the Issuing Bank to reimburse the Paying Bank submitting claims under the letter of credit.
- **Paying Bank**. The bank that makes payment to the Beneficiary of the letter of credit.

1078. What is the role of correspondent banking in trade finance transactions?

From a business perspective, financial institutions should ensure that collection and penalty procedures stipulated in contracts are enforceable in foreign countries in which business is conducted. In addition, many financial institutions rely on the local expertise and knowledge of their foreign correspondent banking relationships to assist in mitigating the associated risks and executing trade finance transactions. For further guidance on correspondent banking, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts and Correspondent Banking.

1079. What are "free trade zones"?

Free trade zones are designated areas within countries that offer a free trade environment with minimal regulation. According to the Financial Action Task Force (FATF), free trade zones are now located in more than 130 countries. Financial institutions may consider conducting enhanced due diligence on parties and transactions associated with free trade zones. The FATF issued guidance on the vulnerabilities of free trade zones in its publication, *The Money Laundering Vulnerabilities of Free Trade Zones*. For additional guidance on geographic considerations, please refer to the High Risk Geographies section.

1080. What consideration should financial institutions give to sanctions, export prohibitions and licensing requirements?

To assist in mitigating the risks associated with trade finance activities, financial institutions should consider the sanctions, export prohibitions and licensing requirements of each jurisdiction in which they conduct business.

For example, in the United States, the following government agencies have primary responsibility for sanctions and export prohibitions and licensing:

- All U.S. persons are required to comply with Office of Foreign Assets Control (OFAC) regulations. The purpose of OFAC is to promulgate, administer and enforce economic and trade sanctions against certain individuals, entities and foreign government agencies and countries whose interests are considered to be at odds with U.S. policy. Sanctions programs target, for example, terrorists and terrorist nations, drug traffickers and those engaged in the proliferation of weapons of mass destruction.
- The U.S. Bureau of Industry and Security (BIS) publishes the Denied Persons List (DPL), which includes individuals who/entities that have been denied export privileges. BIS is an agency of the U.S. Department of Commerce. The mission of BIS is to advance U.S. national security, foreign policy and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership. BIS achieves this by controlling the dissemination of dual-use products and technology to destinations and end users throughout the world. BIS expertise includes engineering and product knowledge used for product classification.
- The Commerce Control List (CCL), administered by the Commerce Department, is used to regulate the export and re-export of items that have commercial uses but also have possible military applications ("dual-use" items).
- The U.S. Munitions List (USML), administered by the State Department, is used to control the export of defense articles, services and related technologies.
- The U.S. Department of Defense (DoD) is actively involved in the inter-agency review of those items controlled on both the CCL and the USML. The agencies work together when there is a question about whether a proposed export is controlled on the CCL or the USML.
- The Energy Department controls nuclear technology and technical data for nuclear power.
- The Bureau of Export Administration (BXA) – U.S. exporters, and third parties in general, are prohibited from dealing with denied parties in transactions involving U.S. items. BXA also maintains an Entities List, comprising foreign end-users engaged in proliferation activities. Since these entities pose proliferation concerns, exports to them are usually prohibited without a license. However, since the BXA guidelines are administered under a case-by-case basis, there are some listed entities that can still receive low-level technology without an export license. The Debarred Parties List is maintained by the State Department. It lists the names of individuals denied export privileges under the International Traffic in Arms Regulations (ITAR).

For further guidance on sanctions lists, please refer to the following sections: Specially Designated Nationals and Blocked Persons List, Country- and Regime-Based Sanctions Programs, Non-Specially Designated Nationals Palestinian Council List, and Other U.S. and International Government Sanctions Programs. For further guidance on licensing, please refer to the Licensing section.

1081. What are examples of standard documentation in letter of credit transactions?

According to the "OCC Handbook: Trade Finance," standard documentation in letter of credit transactions generally falls into four primary categories: transfer, insurance, commercial and other.

- **Transfer documents** are issued by a transportation company when moving merchandise from the seller to the buyer.
    - The **bill of lading**, the most common transfer document, is a receipt given by the freight company to the shipper. A bill of lading serves as a document of title and specifies who is to receive the merchandise at the designated port (as specified by the exporter). It can be in nonnegotiable form (straight bill of lading) or in negotiable form (order bill of lading).
        - In a **straight bill of lading**, the seller (exporter) consigns the goods directly to the buyer (importer). Because it allows the buyer to obtain possession of the merchandise without regard to any bank agreement for repayment, a straight bill of lading may be more suitable for prepaid or open account transactions as opposed to a letter of credit transaction.
        - With an **order bill of lading**, the shipper can consign the goods to the bank, which retains title until the importer acknowledges liability to pay. This method is preferred in documentary or letter of credit transactions since the bank maintains control of the merchandise until the buyer completes all the required documentation. After the bank releases the order bill of lading to the buyer, the buyer presents it to the shipping company to gain possession of the merchandise.
- **Insurance documents**, normally an insurance certificate, cover the merchandise being shipped against damage or loss. The terms of the merchandise contract may dictate that either the seller or the buyer obtain insurance. Open policies may cover all shipments and provide for certificates on specific shipments.
- The **commercial documents**, principally the invoice, are the seller's description of the goods shipped and the means by which the buyer gains assurances that the goods shipped are the same as those ordered. Among the most important commercial documents are the invoice and the draft or bill of exchange.
    - Through the **invoice**, the seller presents to the buyer a statement describing what has been sold, the price and other pertinent details.
    - The **draft** or **bill of exchange** is a negotiable instrument that supplements the invoice as the means by which the seller charges the buyer for the merchandise and demands payment from the buyer, the buyer's bank or some other bank. The customary parties to a draft are the drawer (usually the exporter), the drawee (the importer or a bank), and the payee (usually the exporter), who is also the endorser.
        - A draft can be "clean" (an order to pay) or "documentary" (with shipping documents attached).
        - In a letter of credit, the draft is drawn by the seller, usually on the issuing, confirming or paying bank, for the amount of money due under the terms of the letter of credit.
        - In a collection, this demand for payment is drawn on the buyer.
- **Other** documentation includes official documents that may be required by governments to regulate and control the passage of goods through their borders (e.g., inspection certificates, consular invoices, certificates of origin).

Financial institutions should review available trade documentation to assist in identifying potentially suspicious activity including, but not limited to, invoices and copies of official U.S. or foreign government import and export forms to assess the reliability of documentation provided (e.g., U.S. Customs and Border Protection Form 7501 (Entry Summary), U.S. Department of Commerce Form 7525-V (Shipper's Export Declaration)).

1082. How can trade finance activities be monitored for potentially suspicious activity?

Due to the complex and fragmented nature of trade finance, financial institutions often do not have access to the necessary information to monitor trade transactions effectively for potentially suspicious activity. For example, trade data may not be publicly available or current, or the particulars of a specific business arrangement may not be apparent (e.g., legitimate discounts, bartering deals). If credit services are not provided, financial institutions may only facilitate the transmission of funds with no knowledge of the purpose of the payment. Financial institutions should conduct appropriate due diligence prior to the inception of the customer relationship, and conduct ongoing monitoring of trade transactions that may pose risks. "The Wolfsberg Trade Finance Principles," from the Wolfsberg Group, provides guidance on due diligence specific to letters of credit and bills for collection. The "OCC Handbook: Trade Finance" provides common errors in letter of credit documentation (e.g., bills of lading, invoices, insurance documents, drafts).

To the extent feasible, financial institutions should review trade documentation, not only for compliance with the terms of the trade and/or financial agreement (e.g., letter of credit), but also for red flags that could indicate unusual or suspicious activity. Examples of potentially suspicious activity include obvious under- or over-invoicing, lack of government licenses (when required), and discrepancies in the description of goods on various documents.

Cooperation among the multiple financial institutions involved in each trade finance transaction, as well as other participants involved in the trade transaction, can facilitate the identifying of potentially suspicious activity effectively. A strong correspondent banking due diligence program is instrumental in mitigating the risks associated with trade finance.

For further examples of red flags of potentially suspicious activity, please refer to the following sections: Suspicious Activity Red Flags and Trade Finance Red Flags. For further guidance on correspondent banking, please refer to the following sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts and Correspondent Banking.

1083. In circumstances where a Suspicious Activity Report is warranted, are financial institutions expected to stop trade or discontinue processing the transaction(s)?

Unless there is a potential OFAC violation that may require the blocking or rejecting of one or more transactions, generally, in circumstances where a SAR is warranted, financial institutions are not required to stop trade or discontinue processing the transactions. However, financial institutions proceed at their own risk when continuing to allow suspect transactions to occur.

Whenever violations require immediate attention, such as when a reportable transaction is ongoing, including but not limited to ongoing money laundering schemes or detection of terrorist financing, financial institutions should immediately notify law enforcement, even before the SAR is filed.

Additionally, FinCEN has established a hotline, 1.866.556.3974, for financial institutions to report voluntarily to law enforcement suspicious transactions that may relate to recent terrorist activity against the United States.

1084. What guidance has been issued on trade finance?

The following key guidance has been issued on trade finance and TBML/FT:

- **Trade Finance Activities – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Trade-Based Money Laundering** (2012) by the Financial Action Task Force (FATF)
- **Money Laundering Vulnerabilities of Free Trade Zones** (2010) by FATF
- **Best Practices Paper on Trade-Based Money Laundering** (2008) by FATF
- **The Wolfsberg Trade Finance Principles** (2008) by the Wolfsberg Group
- **Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering** (2010) by the Financial Crime Enforcement Network (FinCEN)
- **Application of a Section 311 Special Measure to Payments under a Stand-By Letter of Credit** (2009) by FinCEN
- **Black Market Peso Exchange Update** (2002) by FinCEN
- **Guidance to Financial Institutions on the Repatriation of Currency Smuggled into Mexico from the United States** (2006) by FinCEN
- **Comptroller's Handbook: Trade Finance** (1998) by the Office of the Comptroller of Currency (OCC)
- **Comptroller's Handbook: Banker's Acceptances** (1999) by the OCC

The following key OFAC guidance has been issued for importers and exporters:

- **Foreign Assets Control Regulations for Exporters & Importers** (2012) by OFAC
- **Frequently Asked Questions for Importers and Exporters** (2012) by OFAC
- **Frequently Asked Questions on Licensing** (2012) by OFAC

- **Ask the TIC: Guide to Export Controls** (2000) by the Trade Information Center (TIC)
- **Letter of Credit Update: OFAC Regulations: The Countries Aren't Enough!** (2002) by OFAC
- **Notice to Mariners** (2006) by the National Geospatial-Intelligence Agency (NGA)
- **Part 1 and Part 2 - Export Controls Compliance: Don't Neglect OFAC** (1999) by the Society for International Affairs, Inc.

Additional organizations providing guidance on trade transactions, trade finance and TBML include, but are not limited to, the following:

- **The U.S. Customs and Border Protection (CBP)** agency is one of the Department of Homeland Security's largest divisions responsible for securing the borders of the United States while simultaneously facilitating the flow of legitimate trade and travel.
- **Trade Transparency Units (TTUs)** were established by the U.S. Immigration and Crime Enforcement (ICE) agency. TTUs conduct financial, money laundering and trade fraud investigations, and have access to customs information on cargo movements, trade data and financial information collected by financial intelligence units (FIU) of participating jurisdictions.
- **The Trade Information Center (TIC)** is operated by the International Trade Administration of the U.S. Department of Commerce for the 20 federal agencies comprising the Trade Promotion Coordinating Committee.
- **The International Chamber of Commerce (ICC)**, established in 1919 with members in more than 130 countries, is a world business organization with a mission to promote trade and investment across frontiers and help business corporations meet the challenges and opportunities of globalization by establishing rules and policies to facilitate international trade and facilitating arbitration. The ICC has established the Commercial Crime Services and Business Action to Stop Counterfeiting and Piracy to assist in combating maritime piracy, financial fraud and counterfeiting.
- **The World Trade Organisation (WTO)**, established in 1995, is an international body with more than 150 member countries that deals with the rules of trade between nations, ranging from liberalizing trade to negotiating trade agreements to settling trade disputes.
- **The World Customs Organisation (WCO)** (formerly the Customs Co-operation Council), established officially in 1952, is an intergovernmental organization with more than 170 member countries. It focuses exclusively on customs matters such as the development of global standards, the simplification and harmonization of customs procedures, trade supply chain security, the facilitation of international trade, the enhancement of customs enforcement and compliance activities, anti-counterfeiting and piracy initiatives, public-private partnerships, integrity promotion, and sustainable global customs capacity building programs. The WCO also maintains the international Harmonized System goods nomenclature, and administers the technical aspects of the WTO Agreements on Customs Valuation and Rules of Origin as well as the Customs Enforcement Network (CEN), a central depository for enforcement-related information to assist the customs enforcement community in producing and exchanging intelligence.
- **The Global Trade Finance Program (GTFP)** was established by the International Finance Corporation, a private arm of the World Bank. The GTFP extends and complements the capacity of banks to deliver trade financing by providing risk mitigation in new or challenging markets where trade lines may be constrained.

Lending Activities

1085. What types of lending activities have been identified as having heightened money laundering and terrorist financing risks?

Lending activities identified as higher risk exhibit one or more of the following: complexity (e.g., the involvement of multiple parties: guarantors, signatories, principals, or loan participants who may manipulate the transaction[s]), payments made in cash or by third parties, high frequency of international transactions, and/or historical susceptibility to abuse by criminals. Examples include, but are not limited to, the following:

- Credit cards; consumer, commercial and agricultural loans collateralized with cash; certificates of deposit (CDs); or assets owned by third parties and/or located in foreign jurisdictions
- Commercial and residential real estate
- Trade finance

- Online lending activities
- Disposition of foreclosed properties

Recently, there has been a rise in mortgage fraud, generally defined as any material misstatement, misrepresentation or omission relied upon by an underwriter or lender to fund, purchase or insure a loan. For additional guidance on mortgage fraud, please refer to the Mortgage Fraud section.

1086. What are some examples of due diligence that should be conducted on customers of the aforementioned lending products?

Historically, although more information was collected on lending customers than deposit customers, the due diligence included a review of credit risks but failed to evaluate money laundering and terrorist financing risks. Financial institutions should consider conducting the following due diligence on lending customers:

- Review source of funds used for collateral and/or payments
- Determine if transaction activity is consistent with the nature of the customer's business and the stated purpose of the loan

1087. How can lending activities be monitored for potentially suspicious activity?

Financial institutions should examine lending activities for suspicious activity by monitoring for common red flags such as:

- Early repayment of a loan in currency or monetary instruments (particularly for problem loans)
- Unexpected payments to cure past due status
- Structured payments of loans in currency or monetary instruments
- Disbursement of loan proceeds via structured currency withdrawals or monetary instruments
- Disbursement of loan proceeds to a third party
- Third-party payment of a loan
- Unwillingness to provide information about the purpose of the loan and/or source of repayment and/or collateral

For additional guidance on red flags, please refer to the sections: Lending Red Flags, Mortgage and Real Estate Red Flags, Credit Card Red Flags, and Trade Finance Red Flags.

1088. What due diligence should financial services companies consider when they provide services to other lenders?

For providers of lending products, the following due diligence should be conducted:

- Limiting business to service providers with an established relationship with the financial institution or other trusted entity
- Conducting background checks on service providers, including a review of all services offered, methods of soliciting new clients, applicable licensing, regulatory obligations and reputation
- Restricting services for certain high-risk customer types, such as nonresident aliens (NRAs) or politically exposed persons (PEPs), or customers located in high-risk jurisdictions
- Evaluating whether the service provider's AML/OFAC Compliance Program is adequate and consistent with the policies of the financial institution

1089. Are there specific AML requirements for nonbank lenders and/or other participants in the lending process?

The USA PATRIOT Act expanded the definition of "financial institutions" subject to AML requirements to include persons involved in real estate settlements and closings. Although the regulation has not been issued yet, under the proposed rule, involved persons include, but are not limited to, the following:

- Real estate brokers

- Attorney(s) representing a buyer/seller
- Financing entities (e.g., banks, mortgage brokers)
- Title insurance companies
- Escrow agents
- Real estate appraisers

Some of the above are considered "professional service providers" who/that act as an intermediary between a client and a third-party financial institution who/that may conduct or arrange for financial dealings and services on their client's behalf (e.g., management of client finances, settlement of real estate transactions, asset transfers, investment services, trust arrangements). For additional guidance on the AML requirements of the aforementioned service providers, please refer to the sections: Persons Involved in Real Estate Settlements and Closings, Nonbank Mortgage Lenders and Originators, Housing Government Sponsored Enterprise and Professional Service Providers.

1090. What AML guidance has been issued on lending activities?

Examples of key guidance on lending activities include the following:

- **Lending Activities – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **An OFAC Primer for the Real Estate Settlement and Title Insurance Industry** (2003) by the Office of Foreign Assets Control (OFAC)
- **RBA Guidance for Real Estate Agents** (2008) by the Financial Action Task Force (FATF)
- **Money Laundering and Terrorist Financing Through the Real Estate Sector** (2007) by FATF
- **Money Laundering in the Commercial Real Estate Industry: An Assessment Based Upon Suspicious Activity Report Filing Analysis** (2008) by the Financial Crimes Enforcement Network (FinCEN)

Nondeposit Investment Products

1091. What does the term "nondeposit investment product" mean?

Nondeposit investment products (NDIPs) include various types of investment products (e.g., securities, bonds, fixed or variable annuities, mutual funds) that may be offered by a financial institution directly through proprietary programs with subsidiaries or affiliates, or indirectly through third-party networking arrangements. Third-party networking arrangements may include relationships with third-party financial services corporations (e.g., investment firms, securities brokers/dealers, insurance companies) to offer NDIP on the premises of the financial institution. These may include co-branded products and dual-employee arrangements where products are co-sponsored by the financial institution and a third-party institution, or third-party arrangements where a third-party institution leases space from the financial institution to offer its NDIPs independent of the hosting financial institution.

1092. What are the heightened money laundering and terrorist financing risks of NDIPs?

The heightened risk of NDIPs lies in the following:

- Reliance on third parties to conduct adequate due diligence and monitoring for potentially suspicious activity in third-party networking arrangements
- Use of front/shell companies to obscure the beneficial owner
- Large volume of transactions
- Potentially rapid movement of funds

1093. Do all NDIPs pose the same degree of risk?

Third-party networking arrangements pose a greater money laundering and terrorist financing risk than proprietary programs. Additionally, NDIP portfolios managed and controlled directly by customers pose a greater risk than those managed by the financial institution or financial services provider(s).

1094. What steps can a financial institution take to mitigate the risk associated with NDIPs?

To mitigate the risk of NDIPs provided through third-party networking arrangements, financial institutions may consider executing the following at the inception of the relationship and on an ongoing basis:

- Limiting business to financial services corporations with an established relationship with the financial institution or other trusted entity
- Conducting background checks on the financial services corporation and its management team/owners, including a review of all services offered, methods of soliciting new clients, applicable licensing, regulatory obligations, reputation, and history of consumer complaints
- Evaluating whether the service provider's AML/OFAC Compliance Program, when required, is adequate and consistent with the policies of the financial institution

For all NDIPs, financial institutions may consider restricting offerings for certain high-risk products, such as private investment companies (PICs) or other special purpose vehicles (SPVs) located in high-risk jurisdictions and offshore hedge funds, and/or providing high-risk products only to established customers.

1095. Who is responsible for conducting due diligence and monitoring for potentially suspicious activities of NDIPs?

The manner in which the NDIP relationship is structured affects the AML responsibilities:

- **Co-Branded Arrangements**: AML responsibilities for completing Customer Identification Program (CIP), customer due diligence (CDD), and suspicious activity monitoring and reporting can vary. Financial institutions should clearly outline each party's contractual responsibilities and ensure compliance by all parties.
- **Dual-Employee Arrangements**: When the dual employee is providing investment products and services, the third-party financial services corporation (e.g., investment firm, securities broker/dealer, insurance company) is responsible for monitoring the registered representative's compliance with applicable securities laws and AML regulations. When the dual employee is providing products or services from the financial institution, responsibility for monitoring the employee's performance and compliance with AML requirements falls on the financial institution.
- **Third-Party Networking Arrangement**: All AML responsibilities are assumed by the third-party financial services corporation.
- **Proprietary NDIPs**: All AML responsibilities are assumed by the financial institution offering the proprietary NDIPs.

1096. How should NDIPs be monitored for suspicious activity?

Financial institutions should examine NDIPs for suspicious activity by monitoring for common red flags such as:

- An account shows an unexplained high level of funds transfer activity with a very low level of securities transactions
- Client deposits or attempts to deposit cash at a financial institution that does not routinely accept cash
- Client takes both a short and a long position in a security or contract for similar amounts and similar expiration dates with no apparent business purpose
- Customer appears to be acting as an agent for an undisclosed third party, but declines or is reluctant to provide information relating to the third party
- Customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer the proceeds out of the account
- Early termination of investment contracts

For a list of red flags related to account activity and transaction executions, please refer to the section Suspicious Activity Red Flags.

1097. Are there specific AML requirements for financial service corporations offering NDIPs?

The USA PATRIOT Act expanded the definition of "financial institutions" subject to AML requirements to include:

- Broker-dealers
- Mutual funds
- Insurance companies

For additional guidance on the AML requirements of broker-dealers, mutual funds and insurance companies, please refer to sections Broker-Dealers, Mutual Funds and Insurance Companies.

Insurance Products

1098. What types of insurance products have been identified as having increased money laundering and terrorist financing risks?

The following insurance products have been identified as higher risk because they exhibit one or more of the following: complexity (e.g., the involvement of multiple parties: guarantors, signatories, beneficiaries, or professional service providers who may manipulate the transaction[s]), ability to transfer value without the knowledge of the issuer, payments made in cash or by third parties, high frequency of international transactions, and/or historical susceptibility to abuse by criminals:

- Permanent life insurance policies, other than group life insurance policies
- Annuity contracts, other than group annuity contracts
- Any other insurance products that have cash value or investment features

1099. Are there specific AML requirements for financial services companies offering these types of insurance products?

The USA PATRIOT Act expanded the definition of "financial institutions" subject to AML requirements to include insurance companies offering the aforementioned covered products. The definition of insurance company currently excludes group insurance products, term (including credit), life, title, health, and many property and casualty insurers. It also excludes products offered by charitable organizations (e.g., charitable annuities), as well as reinsurance and retrocession contracts. It also excludes entities that offer annuities or other covered products as an incidental part of their business.

For additional guidance on the AML requirements of insurance companies, please refer to the Insurance Companies section.

1100. Who is responsible for conducting due diligence and monitoring for potentially suspicious activities of insurance products?

Insurance products are typically sold to bank customers through networking arrangements with an affiliate, an operating subsidiary, or other third-party insurance providers. Often, banks play the role of third-party agent selling covered insurance products.

The manner in which the insurance products are offered, however, affects the AML responsibilities.

- **Co-Branded Arrangements** – AML responsibilities for completing Customer Identification Program (CIP), customer due diligence (CDD), and suspicious activity monitoring and reporting can vary. Financial institutions should clearly outline each party's contractual responsibilities and ensure compliance by all parties.
- **Dual-Employee Arrangements** – When the dual employee is providing investment products and services, the insurance company is responsible for monitoring the registered representative's compliance with applicable securities laws and AML regulations. When the dual employee is providing products or services from the financial institution, responsibility for monitoring the employee's performance and compliance with AML requirements falls on the financial institution.
- **Third-Party Networking Arrangement** – The insurance company assumes all AML responsibilities.

- **Proprietary Insurance Products** – The financial institution offering the proprietary insurance products assumes all AML responsibilities.

1101. How can these insurance products be monitored for potentially suspicious activity?

Financial institutions should examine insurance products for potentially suspicious activity by monitoring for common red flags such as:

- Customer's lack of concern with the cost of the policy
- Customer's lack of concern with the performance of an insurance product
- Customer's lack of concern with the penalties/fees
- Large single-payment premiums for life and annuity policies
- Unusual methods of payment, particularly cash or cash equivalents

For additional guidance, please refer to the sections: Suspicious Activity Red Flags and Insurance Products Red Flags.

1102. What guidance has been issued on insurance companies and covered products?

The following are examples of key guidance that has been issued:

- **Insurance – Overview within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual** by the Federal Financial Institutions Examination Council (FFIEC)
- **Frequently Asked Questions: Customer Identification Programs and Banks Serving as Insurance Agents** (2006) by FinCEN
- **Insurance Industry Suspicious Activity Reporting: An Assessment of Suspicious Activity Report Filings** (2010) by the Financial Crimes Enforcement Network (FinCEN)
- **Frequently Asked Questions from the Insurance Industry** (2012) by the Office of Foreign Assets Control (OFAC)
- **Risk-Based Approach for the Life Insurance Sector** (2009) by the Financial Action Task Force (FATF)
- **Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism** (2004) by the International Association of Insurance Supervisors (IAIS)
- **Anti-Money Laundering Guidance Notes** (2003) by the IAIS

Administration of Customer Risk Assessment

1103. How often should a financial institution's customer risk assessment methodology be re-evaluated?

The customer risk assessment methodology should be re-evaluated when new products or services are introduced, with each merger/acquisition, and when new markets are targeted (e.g., type of customer, country of domicile of customer).

1104. How often should customer risk ratings be re-evaluated by a financial institution?

Financial institutions should, on a regular basis, re-evaluate their customers. In addition, re-evaluations should take place shortly after new information about a customer becomes known to the financial institution. For example, when:

- A customer relationship manager becomes aware an individual is starting a new business in a high-risk activity or jurisdiction
- A customer begins using high-risk products or services
- A customer relationship manager notices significant changes in the number or amount of a customer's transactions

- A customer relationship manager reads an article about a customer recently indicted for illicit activities (e.g., drug offenses)
- The financial institution receives a grand jury subpoena naming the customer

1105. Can a financial institution customize or modify results of a customer risk assessment?

Yes. Usually the ability to modify an assigned risk score rests with Compliance. Changes to the score should be clearly documented. Some financial institutions limit reducing risk scores to customers who have maintained relationships with the financial institution for a minimum of one year.

1106. How can a financial institution validate the outcome of its customer risk assessment model?

A financial institution can validate its customer risk assessment model by running existing customer information through the model to ensure the results are consistent with the perceived risk of the customer.

1107. How can a financial institution test its customer risk assessment model and methodology?

The financial institution can test its customer risk assessment model and methodology by determining:

- Data sources are properly fed
- Algorithms are properly functioning
- Risk ratings are logical, based on experience of compliance personnel
- Customer risk assessment results are used according to policies and procedures

1108. What are the most common gaps with customer risk assessments?

The most common gaps with customer risk assessments include, but are not limited to, the following:

- The methodology does not identify and/or quantify, in whole or partially, all inherent risk factors
- The same methodology is applied to different customer types (e.g., individual, business, financial institution)
- Not all customers are assessed
- The assessment is not executed in a timely manner, initially or ongoing
- The results of the methodology are not used to determine the extent of due diligence for each customer (e.g., requiring provision of additional information, site visits, senior management approvals, reviews of profiles) and the scope and frequency of monitoring.
- Only the results, and not the methodology itself, are documented
- The classifications of high, moderate and/or low risk are inconsistent with leading practice
- The methodology is not current
- There is a lack of or inadequate controls on the ability to modify results of assessments

Office of Foreign Assets Control Risk Assessment

1109. What is an Office of Foreign Assets Control (OFAC) risk assessment?

An OFAC risk assessment attempts to identify an organization's level of vulnerability to noncompliance with economic sanctions administered by OFAC or any sanction program as required by the financial institution's policy. This is accomplished by evaluating, among other factors, the inherent risk of products and services, customer types, the geographic origin and destination of transactions, and the strength of the controls mitigating those risks.

For further guidance on OFAC and other sanction requirements, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

1110. Are financial institutions required to implement an OFAC risk assessment?

There is no requirement per se that institutions conduct OFAC risk assessments. However, banking regulators, in particular, expect financial institutions to conduct an OFAC risk assessment. Best practice suggests all financial institutions should conduct an assessment to understand their level of vulnerability to noncompliance with OFAC.

1111. How often should an OFAC risk assessment be conducted?

At a minimum, the OFAC risk assessment should be conducted annually.

1112. How often should an OFAC risk assessment methodology be re-evaluated?

An OFAC risk assessment methodology should be re-evaluated when new products or services are introduced, with each merger/acquisition, and when new markets are targeted (e.g., type of customer, country of domicile of customer).

1113. How should an OFAC risk assessment be conducted?

The method used to conduct the OFAC risk assessment will depend on the complexity of the financial institution and the technology support available to the organization. A combination of methods (e.g., questionnaires, internally or externally developed databases, web-based applications) is often used to collect the product/process information effectively and enable Compliance to review and validate the risk assessment results.

1114. Which customers pose a higher OFAC risk?

Per the FFIEC BSA/AML Examination Manual, customers posing a higher OFAC risk include, but are not limited to:

- Nonresident aliens (NRAs)
- Foreign customers
- Customers with foreign operations or a foreign customer base

1115. What types of products and services pose a higher OFAC risk?

Per the FFIEC BSA/AML Examination Manual, products posing a higher OFAC risk include, but are not limited to:

- International funds transfers
- Cross-border automated clearing house (ACH) transactions
- Commercial letters of credit
- Transactional electronic banking
- Foreign correspondent services
- Management of sovereign debt
- Payable through accounts (PTAs)
- Products or services provided to entities or individuals without accounts at the financial institution (e.g., monetary instruments, wires)
- Online activities

1116. What guidance has been provided on OFAC risk assessments?

The FFIEC BSA/AML Examination Manual provides guidance with respect to the identification of specific risk categories, the level of detail of the analysis of specific risk categories, the impact of the risk assessment on the organization's OFAC program, the recommended frequency for which the assessment should be conducted, and the circumstances prompting an organization to update its risk assessments, but specifically avoids providing guidance on the form risk assessments should take.

1117. What are the most common gaps with OFAC risk assessments?

The most common gaps with OFAC risk assessments include, but are not limited to, the following:

- The methodology does not identify and/or quantify, in whole or partially, all inherent risk factors
- The methodology does not identify and/or assess, in whole or partially, all controls/control environments
- The methodology does not calculate residual risk
- A consistent methodology is not used by each business line
- The classifications of high, moderate and/or low risk are inconsistent with leading practice
- Only the results, and not the methodology itself, are documented
- The results of the executed methodology are not used to drive strategic changes in the OFAC/Sanctions Compliance Program
- The results are not current
- The methodology is not current
- Lack of or inadequate training on the purpose of the assessment and the meaning of the results with Compliance, business line management and senior management
- Over-reliance on a third party to develop and execute the assessment

TRANSACTION MONITORING, INVESTIGATIONS AND RED FLAGS

Monitoring Process

1118. Should all transactions be monitored?

Yes. All transactions should be subject to monitoring, but the extent, nature and frequency of monitoring should be risk-based. Financial institutions should periodically take an inventory of all products and services offered by the institution and determine how each of the products is monitored to identify unusual or potentially suspicious activity. In addition, the financial institution should have a mechanism in place to ensure newly added products and services are incorporated into the monitoring process; this usually is accomplished through compliance representatives participating in new product development committees.

1119. Should all transactions be monitored in a similar fashion?

No. A “one-size-fits-all” approach is usually insufficient when trying to identify unusual or potentially suspicious activity. Financial institutions should, when identifying all of the products and services offered (as outlined above), also identify where the transaction activity and customer profile information are stored. This exercise should identify the format, location, content and quality (e.g., level of detail, completeness, usefulness) of the electronically stored data. This exercise also should include identification of non-electronic sources of information (e.g., customer files maintained by relationship managers, letters of credit files). The factors identified during this exercise will impact the way in which the transactions can be monitored (e.g., through automated monitoring systems, through manual reports, with support from customer information).

1120. On what level should transactions be monitored (e.g., account, customer)?

Transactions should be monitored on a customer level in order to follow properly the money trail when conducting an investigation. Monitoring rules/parameters can be applied on different “levels” to detect potentially suspicious activity:

- Transaction level (typically driven by type/code [e.g., cash, wire] and date[s] and amount[s] of the transaction)
- Account level (typically driven by account type, such as checking, savings or loan)
- Customer level (typically driven by aggregate transactions/profiling on a taxpayer identification number [TIN] level or other number used to uniquely identify a customer)
- Household level (similar to customer level, but on a household level)
- Geographic level (typically driven by higher-risk geographic locations or unusual patterns of activity in particular locations)

A strong monitoring program may include monitoring on a combination of levels. Factors that may determine the level of monitoring include available customer information and specific capabilities of the transaction monitoring software utilized by the financial institution.

1121. How is the term “household” defined?

A household is generally defined as an entity consisting of two or more distinct customers who share a common factor such as an address, phone number or business owner.

1122. How can technology be used to support a financial institution's AML monitoring program?

Much has been written about the use of AML technology to support a financial institution's AML monitoring efforts. Technology can be used, for example, to support:

- Monitoring for suspicious transactions and facilitating SAR filings
- Storage of customer information (e.g., CIP, due diligence [DD], enhanced due diligence [EDD])
- Calculation of customer risk ratings
- Searching against special lists of prohibited and/or high-risk individuals/entities (e.g., Office of Foreign Assets Control [OFAC], 314(a), subpoenas, media searches, internal "deny" lists, politically exposed persons [PEPs]) for customers and transactions
- Case management

For further guidance on AML technology, please refer to the sections: Suspicious Transaction Monitoring and Suspicious Activity Report Filing Software, Case Management Software, Customer Information Database and Customer Risk Assessment Software, List Providers, Interdiction Software.

1123. What protocols should a financial institution establish when developing its monitoring program?

A financial institution's monitoring process is often dictated by its suspicious activity monitoring software solution. Once a technology solution has been implemented, financial institutions should establish the following monitoring protocols:

- Assignment of alerts (e.g., by manager, by risk score, by self-assignment, etc.)
- Time frames for conducting reviews (e.g., review automated alerts within 30 days of generation, filing of SARs within 30 days from the date of detection, etc.), and appropriate tracking and reporting procedures to detect any backlogs
- Prioritization and escalation of cases
- Documentation standards (e.g., supported reasoning for cleared alerts, appropriate use of a case management system, effective use of the Internet, etc.) that cover the "Five W's":
    - Who conducted the activity?
    - What instruments were used?
    - Where did the activity occur?
    - When did the activity occur?
    - Why is the activity suspicious or not suspicious?
- Quality assurance procedures (e.g., secondary review of select alerts, cases and SARs filed, etc.)

1124. How can financial institutions develop profiles to help identify unusual or potentially suspicious activity?

Many financial institutions, during the account opening process, ask for the customer's expected activity (e.g., products, geographic locations, frequency, dollar volume). The financial institution should, however, review this expected transaction profile for appropriateness (e.g., comparison against expectations for customer's occupation and salary/business and revenue). When developing profiles for existing customers, many financial institutions use historical data once they have determined that this data is indeed reasonable and appropriate for the customer. As mentioned earlier, the financial institution should review the profile created using historical data with the institution's expectations for the customer.

1125. How can a financial institution utilize a risk-based approach to its transaction monitoring?

Many financial institutions utilize the results of their business line and customer risk assessments as factors in determining the appropriateness of their transaction monitoring. For example, some financial institutions assign more resources (e.g., staff, monitoring reports, monitoring system enhancements) to higher-risk products, geographies and

business lines (as assigned during the financial institution's business line risk assessment process). In addition, many financial institutions adjust monitoring thresholds based upon a customer's risk level (as assigned during the financial institution's customer risk assessment process) to place more scrutiny on higher-risk customers.

Some suspicious activity monitoring software solutions also include a feature that allows financial institutions to risk rate, or prioritize, alerts to enable prioritization (e.g., assignment of high risk or more complex alerts to more seasoned investigators, etc.).

1126. How is transaction monitoring conducted in institutions that do not have AML monitoring software?

Institutions that do not have automated systems and/or that need to supplement their automated systems often use reports from various internal systems that may be generated for other purposes. For example, reports on loan prepayments, currency activity, funds transfers, nonsufficient funds, large items, significant balance changes, monetary instruments and closed deposit accounts are commonly generated by institutions for management reporting and business development purposes, and reports on off-market transactions are produced to monitor trading activity. The information included within these reports also could be invaluable for AML monitoring.

Though institutions should maximize the efficiency of transaction monitoring by utilizing existing reports, additional reports and review procedures may be required to ensure all of an institution's transactions are being captured in its monitoring efforts. Periodic transaction-monitoring reports may include, but are not limited to, cash and wire transactions that exceed a predetermined amount, check transactions, loan payments and prepayments, and closed deposit accounts. Employees in high-risk areas, such as trade finance and correspondent banking, should receive in-depth and customized training on the identification of potentially suspicious activity and red flags because, to a large extent, these areas involve real-time manual monitoring by those employees.

1127. What are some common reasons for creating manual monitoring reports?

As sophisticated as technology has become, it often does not provide all the monitoring necessary to cover all customer types and products, services and transactions offered by a financial institution. Reasons for creating manual reports generally include data issues or a need for more enhanced methods of detection. Common examples include, but are not limited to, the following:

- Certain customer types (e.g., trusts) or transaction processing (e.g., loan payments) are processed on different platforms
- Products with red flags cannot be monitored by an automated system (e.g., trade finance)
- Omnibus accounts require more drill-down than single customer accounts
- Activities, such as human trafficking, require data analytics and not just traditional monitoring

Roles and Responsibilities

1128. Who should perform transaction monitoring?

Individuals who either deal directly with customers or process customer transactions are in the best position to perform effective transaction monitoring on a real-time basis. Within an organization, these individuals tend to know the most about the customers and their typical pattern of transaction activity. In addition, many financial institutions have developed centralized investigative units, which are responsible for reviewing alerts generated by the monitoring program in place.

1129. Who should investigate unusual or potentially suspicious activity once it is identified?

Once unusual or potentially suspicious activity has been identified by either a business unit or through manual or automated monitoring, many financial institutions require the activity to be referred to a central investigative unit. The central investigative unit can either be a stand-alone department or be housed within the compliance department or a security department. Centralized investigations help to ensure that standards are applied uniformly, that confidentiality is maintained, and that there is consistency of documentation. Centralization also may aid in the detection of larger-scale money laundering problems that span more than one business unit. Since this unit does not generally have in-depth knowledge of a particular customer and its transaction profile, business units must be involved, at a minimum, to provide insight and explanation.

1130. Should one investigator be assigned to a case from the initiation to the conclusion of an investigation?

Financial institutions with small investigation teams are more likely to take a “cradle-to-grave” approach in which one analyst selects an alert, investigates it and sees it through to resolution.

Other, particularly larger, institutions may take more of a triage approach, such as the following:

- Analysts perform the initial review of alerts to determine whether an activity may be potentially unusual and a case should be opened
- Investigators perform a detailed review of customer activity and recommend whether a case should be closed or a SAR filed
- Managers perform final review and make a decision to file or not file a SAR

The triage approach potentially allows better alignment of responsibilities with people’s skills and experience, but in either case, there can be a process or at least an understanding that the more complex alerts should go to the most experienced people.

1131. Who should make the decision to file/not file a SAR?

Investigators, at the conclusion of an investigation, generally submit the findings to a member of management (e.g., AML compliance officer), who would then (a) agree with the decision to close the investigation without a Suspicious Activity Report (SAR) filing, (b) request additional investigation and/or clarification, or (c) agree with the decision to file a SAR. Financial institutions have varying levels of review regarding investigations warranting a SAR filing. Some financial institutions allow the AML compliance officer, or his or her delegate, to make the final decision whether or not to file a SAR; others require approval from the chief compliance officer and/or general counsel. Whatever the quality control process, the financial institution should ensure it submits high-quality SARs in a timely manner.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

1132. When selecting personnel to staff the investigative unit, what skills should be required by the financial institution?

There are a number of different skills and experiences that are useful for AML monitoring, including, but not limited to, the following:

- Relevant industry/product knowledge
- Understanding of applicable AML risks
- Fraud and forensic training/healthy dose of skepticism
- Skilled at using the Internet to develop information
- Ability to work effectively with the business lines to gather information
- Experience with suspicious transaction monitoring software, including an understanding of system functionality and detection logic
- Ability to identify patterns and spot anomalies
- Ability to draw and support conclusions and summarize them in a logically organized report

Investigation Process

1133. In addition to alerts produced through monitoring, how else might a financial institution become aware of suspicious activity?

An institution may become aware of suspicious activity through internal referrals from business units performing real-time transaction monitoring or with direct customer contact, 314(a)/(b) requests, subpoenas, National Security Letters (NSLs), the media (e.g., radio, television, newspaper), regulatory updates released by FinCEN or other applicable agencies, and reports from third parties such as credit reporting agencies or negative database operators (e.g., check fraudsters, charge-offs).

1134. What is the difference between an alert and an investigation?

An alert is a potential indicator of unusual or potentially suspicious activity based on various factors, such as expected activity thresholds, account history, customer types, product types and geography in an automated monitoring system. An alert also can be generated outside of a transaction monitoring system via internal referrals, subpoenas and 314(a)/(b) matches. Regardless of its source, an alert is not necessarily an automatic indicator of suspicious activity. An investigation is the review of transactions/conduct in order to classify the alert as a "false positive" or a "true positive," which will require further analysis and could result in the filing of a SAR.

1135. How can a financial institution incorporate the use of the media into its monitoring system?

Many AML departments subscribe to news services offered by some of the major search engines and list providers and/or designate personnel to screen local and national news sources on a continual basis for information that may link customers to money laundering and terrorist financing, and to conduct investigations for any matches.

1136. What are some keys to an effective investigation process?

Keys to an effective investigation process include, but are not limited to:

- Maintaining an investigation file with adequate documentation to allow an uninvolved party to understand how the decision to file or not file a SAR was reached.
- Performing sufficient due diligence on the customer or suspect – This would involve obtaining occupation or nature of business if not already contained in the financial institution's customer due diligence (CDD)/enhanced due diligence (EDD) documentation, gaining a basic understanding of the purpose of the account or transactions in question, and performing research on adverse media/news information.
- Investigating not only the transaction(s) in question, but also conducting a historical review of the nature of the account activities and, where appropriate, related accounts over a reasonable period of time – Some common review periods include the previous six months or previous year, with some review periods starting from the date of account opening.
- Performing research on the entire customer relationship, including related accounts and related parties.

1137. How can a financial institution evaluate the effectiveness of its monitoring program?

When assessing overall effectiveness, the evaluation should not be limited to AML technology, but should also include the overall suspicious activity monitoring program, including systems, personnel, procedures and training. Some indicators and areas to assess include, but are not limited to, the following:

- **Alert-to-Case Ratio:** Financial institutions should review system rules that have low alert-to-case ratios to identify parameters that could be adjusted to reduce the volume of "false positives" (alerts cleared without escalation). Another indicator of ineffective monitoring is if a high percentage of recurring alerts were previously investigated and deemed not suspicious.
- **Case-to-SAR Filing Ratio:** Similar to alert-to-case ratios, analyzing cases that lead to SAR filings may assist financial institutions in refining controls to better detect potentially suspicious activity by identifying high-risk products, services, customers or geographies that may require specific system rules or a separate manual monitoring process. In circumstances with low case-to-SAR filing ratios, the financial institution may need to revisit existing parameters, data feeds and staff training to reduce the number of false positives.
- **Non-System Sourced Cases/SAR Filings:** Repeat cases and SAR filings from non-system sources may provide insight into the development of new or enhanced monitoring rules (e.g., law enforcement inquiries, 314(a) and 314(b) information requests, etc.). However, if more SARs are filed on non-system sourced referrals than from automated alerts, existing monitoring rules need to be reviewed for effectiveness.
- **Lack of Alerts Generated for a Certain Product or Transaction Type:** This may indicate that a product or transaction type is not covered in the suspicious activity monitoring software, or that the existing rules and thresholds are ineffective in monitoring for potentially suspicious activity. In some instances, a manual monitoring process may need to be implemented to cover a particular product or transaction type (e.g., trade finance, etc.).
- **Few Alerts Generated for High-Risk Customers:** This may indicate an ineffective customer risk assessment methodology, ineffective incorporation of risk into suspicious activity monitoring software, or both.

- **Wide-Ranging Rates of Clearing Alerts by Investigative Personnel:** Developing a process in which more complex alerts and cases are assigned to seasoned personnel may improve the overall efficiency of the monitoring and investigation process. Additionally, to ensure alerts are properly reviewed, quality control reviews of cleared alerts by more experienced staff can be conducted. For additional guidance on conducting investigations, please refer to the Transaction Monitoring, Investigations and Red Flags section.
- **Alert Assignment and Case Management:** In many cases, different system rules may generate alerts on the same activity; therefore, a comprehensive alert and case management system that assigns alerts based on customer and account relationships is critical to overcome any inefficiencies in reviewing the same transaction(s) flagged by multiple monitoring rules. A proper case management system should also incorporate non-system sourced cases (e.g., law enforcement inquiries, etc.).
- **Usefulness of Individual Rules/Scenarios:** Looking at how many alerts are generated from individual rules and the extent to which these alerts ultimately result in SARs being filed may yield results that can be used to modify or delete certain rules.
- **High Volume of Repeat SAR Filings on the Same Subject(s):** This may indicate an ineffective customer termination policy.
- **Backlogs or Late SAR Filings:** This may indicate ineffective use of monitoring software, lack of required personnel commensurate to the volume of alerts, inadequate knowledge and experience of monitoring and investigation personnel and/or a lack of appropriate management reporting to track and aid in understanding and promptly addressing any growing backlogs.
- **Auditors/Regulators Identify Suspicious Activity Unreported on SARs Filed by the Financial Institution or Question the Quality and Completeness of Investigation Files:** This may indicate that the monitoring and investigation team lack: relevant industry/product knowledge; an understanding of applicable AML risks; fraud and forensic training/healthy dose of skepticism; the ability to work effectively with business lines to gather and document pertinent information; or an understanding of system functionality or detection logic.

Financial institutions should continuously review published typologies to identify emerging risks or controls to assist them in enhancing their suspicious activity monitoring program.

Overall, each component of a financial institution's monitoring program (including individual system rules and resulting alerts) should be analyzed individually and collectively for overall effectiveness. Potential root causes for ineffective or deficient monitoring programs generally can be traced to the following:

- The number and qualifications of assigned individuals to the monitoring and investigation team(s)
- Adequacy and communication of training on policies and procedures
- Use (or misuse) of technology

For additional guidance on suspicious activity monitoring software, please refer to the AML Technology section.

1138. What documentation should be maintained for investigations not warranting a SAR filing?

Financial institutions should maintain the same level of detailed investigative support for investigations not resulting in a SAR as they do for SAR filings. The financial institution should have enough support to justify its decision to both file a SAR and close an investigation without a SAR filing. This support should include a synopsis of both the customer and other suspects identified, a summary of the activity reviewed, and a clear determination as to why the situation did or did not warrant a SAR filing. The utilization of a case management system that serves as a central repository for all investigations will assist financial institutions with the organization and maintenance of the documentation.

Suspicious Activity Red Flags

1139. What are examples of suspicious activity?

The following is a sample list of red flags that may be applicable to different types of transaction activities and businesses. This is not an exhaustive list. It is essential that financial institutions consider these red flags as guidance and exercise judgment in identifying other transactions that may be unusual or indicate potential money laundering or terrorist financing.

Also, it is important to note that customers are not necessarily doing something illegal just because their activities mirror one or more of these red flags; however, such activities generally warrant further review and, if a satisfactory justification is not obtained, a more thorough investigation should be conducted to determine whether a SAR should be filed.

Further examples of potentially suspicious activity can be found in the SAR Bulletin issued periodically by FinCEN, the FATF's annual report on Money Laundering Typologies, the FIU's "In Action" report produced by the Egmont Group and the FFIEC Examination Manual.

Account Opening Red Flags

- Customer is unwilling to provide the required account opening information and/or documentation
- Customer uses unusual or suspicious identification documents that cannot be readily verified
- Customer exhibits unusual concern for secrecy, particularly with respect to identity, type of business, assets or dealings with other entities
- Customer has difficulty describing its business, the stated purpose of the account and the expected transactions in the account
- Customer lacks a general knowledge of its industry
- Customer's financial statements reflect concentrations of closely held companies or businesses that lack audited financial statements to support their value
- Customer is reluctant to provide information on controlling parties and underlying beneficiaries
- Customer questions reporting/recordkeeping requirements
- Customer requests that documentation standards be waived
- Customer provides forms of identification for CIP purposes with conflicting information
- Customer makes frequent or large transactions and has no record of past or present employment experience
- Customer has no apparent reason for using the institution's services (e.g., customer is not located in close proximity)
- Customer has multiple accounts under single or multiple names for no apparent business purpose
- Customer, or a person/entity publicly associated with the customer, has a questionable background, including prior criminal, civil or regulatory convictions
- Upon request, customer refuses to identify or fails to indicate a legitimate source of its funds and other assets
- Customer has a defensive stance to questions
- Customer uses same address(es) for multiple customers that have no apparent relationship
- Customer provides disconnected telephone number(s)
- Customer provides identification documents that are expired or appear false
- Customer provides inconsistent information when questioned

Account Activity and Transaction Execution Red Flags

- Transactions with no logical economic purpose
- Lack of concern exhibited by the customer regarding risks, commissions or other transaction costs
- Sudden high volume of unexplained activity
- Transactions that involve higher-risk businesses
- Transactions involving senior political figures, both foreign and domestic
- Round-sum transactions (e.g., $10,000.00, $50,000.00, $500,000.00)

- Layering (e.g., transfers between bank accounts of related entities or charities for no apparent reason)
- Customer opens a number of accounts under one or more names, and makes numerous cash deposits just under 10,000, or deposits containing bank checks or traveler's checks
- Customer makes numerous deposits under $10,000 in an account in short periods of time, thereby avoiding the requirement to file a Currency Transaction Report; this includes deposits made at an automatic teller machine
- Customer makes large deposits and maintains large balances with little or no apparent justification
- Transaction not in line with customer's stated purpose of the account and/or nature of business
- Deposit/withdrawal transactions just below reporting thresholds, indicating possible structuring or avoidance of tax reporting requirements (e.g., $2,999, $9,990)
- Frequent transactions at daily maximums (e.g., cash withdrawals from an ATM)
- Customer conducts multiple transactions several times in one day or over a short period of time (possibly using different tellers), indicating structuring
- Customer maintains multiple accounts at a bank or at different banks for no apparent legitimate reason; accounts may be in the same names or in different names with different signature authorities; inter-account transfers evidence common control
- Customer attempts to bribe or threaten an employee in order to circumvent reporting requirements
- Frequent disbursements to/from apparently unrelated third parties
- Accumulation of large balances that are inconsistent with the customer's business, and the subsequent transfer of such balances to another jurisdiction
- High volume of transaction activity with low balances and/or account is frequently overdrawn
- Transactions are frequently changed at the teller, particularly upon notification of identification and/or reporting requirements
- Uncharacteristic nonpayment for services, which may indicate a loss of funds or access to funds

Currency Red Flags

- Deposits of currency just below the reportable threshold conducted with multiple branches, tellers, ATMs, accounts and/or on different days
- Deposits of currency by multiple individuals into the same account
- Deposits of currency wrapped in currency straps that have been stamped by other financial institutions
- Frequent exchanges of small dollar denominations for large dollar denominations
- High volume of currency deposits and/or withdrawals inconsistent with the profile of the customer
- Multiple deposits occurring in various out-of-state locations
- Frequent cash deposits or withdrawals with no apparent/known business source
- Customer requests cash shipment or transfer to another account almost immediately after making numerous cash deposits
- Sudden increase in cash activity
- Lack of withdrawal of currency for businesses that generally require significant amounts of currency (e.g., retail, check cashers, owners of automated teller machines), possibly indicating another source of currency

Privately Owned ATM Red Flags

- Automated teller machine (ATM) activity levels are high in comparison with other privately owned or bank-owned ATMs in comparable geographic and demographic locations.

- Sources of currency for the ATM cannot be identified or confirmed through withdrawals from account, armored car contracts, lending arrangements, or other appropriate documentation.

Bulk Shipments of Currency Red Flags

- An increase in the sale of large denomination U.S. bank notes to foreign financial institutions by U.S. banks
- Small denomination U.S. bank notes smuggled into Mexico being exchanged for large denomination U.S. bank notes possessed by Mexican financial institutions
- Large volumes of small denomination U.S. bank notes being sent from Mexican *casas de cambio* to their accounts in the United States via armored transport, or sold directly to U.S. banks
- Multiple wire transfers initiated by *casas de cambio* that direct U.S. financial institutions to remit funds to jurisdictions outside of Mexico that bear no apparent business relationship with that *casa de cambio* (recipients include individuals, businesses, and other entities in free trade zones and other locations associated with Black Market Peso Exchange-type activities)
- The exchange of small denomination U.S. bank notes for large denomination U.S. bank notes that may be sent to jurisdictions outside of Mexico, including jurisdictions associated with Black Market Peso Exchange-type activities, such as Mexico, Guatemala, Argentina, Brazil, Paraguay, Uruguay, and Venezuela.
- Deposits by *casas de cambio* to their accounts at U.S. financial institutions that include third-party items (including sequentially numbered monetary instruments and checks)
- Deposits of currency and third-party items by Mexican *casas de cambio* to their accounts at Mexican financial institutions and thereafter, direct wire transfers to the *casas de cambio* accounts at U.S. financial institutions
- Frequent requests for cash letter instruments

Branch and Vault Shipments Red Flags

- Significant exchanges of small-denomination bills for large-denomination bills
- Significant changes in currency shipment patterns between vaults, branches and/or correspondent banks
- Rapid increase in the size and frequency of cash deposits with no corresponding increase in noncash deposits
- Unusually large currency shipments to and from remote locations
- International cash shipments funded by multiple monetary instruments
- Frequent use of cash shipments of customers in non-cash intensive businesses
- Cash shipments with instructions inconsistent with normal cash shipment practices
- Branches whose large bill requirements are significantly greater than the average or branches that suddenly stop shipping large bills

Monetary Instrument Red Flags

- Purchase or deposit of structured monetary instruments, often in round dollar amounts, sequentially numbered, just below reporting threshold (e.g., $2,999, $9,990) for currency
- Purchase of multiple sequentially numbered monetary instruments for the same payee
- Use of one or more monetary instruments to purchase another monetary instrument(s)
- Purchase of cashier's checks, money orders, and so forth, with large amounts of cash
- Missing/illegible information (e.g., blank payee)
- Lack of signature
- Frequent payments to same payee(s)

- Deposit or use of multiple monetary instruments purchased on the same date from different banks or different issuers
- Numerous deposits of small monetary instruments, followed by a request for a large outgoing wire to another institution or country
- Customer purchases multiple money orders with no apparent reason

U.S. Dollar Draft Red Flags

- Significant variance in expected/historical activity versus actual activity in terms of volume of U.S. dollar draft activity
- Dollar amounts that appear to be designed to evade reporting requirements (i.e., under $3,000 or $10,000) or are purchased in round amounts
- Multiple sequentially numbered U.S. dollar drafts
- High volume of U.S. dollar drafts to the same payee or from the same remitter
- Drafts issued by *casas de cambio*
- Third-party endorsed drafts
- No payee named on the draft (typically from Mexico)
- Large volume of activity through correspondent master accounts opened by foreign banks

Wire Transfer Red Flags

- Apparently unnecessary and/or frequent changes to standard wire payment instructions
- Changes made to spelling of names and addresses of originators/beneficiaries (e.g., deliberate misspellings, reordering of names, incomplete addresses)
- Wire transfers to and from bank secrecy haven countries and countries known for or linked to terrorist activities, drug trafficking, illegal arms sales or other illegal activity
- Wires to other countries without changing the form of the currency (e.g., USD)
- Intentional circumvention of approval authorities or reporting limits by splitting transactions
- A large deposit followed by numerous, smaller wire transactions
- Numerous smaller wire transactions from an account that maintains a low balance
- Several deposits, particularly in currency or monetary instruments, followed by international wire transactions
- Unexplained or sudden, extensive wire activity, especially in accounts that had little or no previous activity
- Outgoing wire transactions requested by non-account holders, particularly for cash under $10,000 designed to evade Currency Transaction Reporting
- Large number of wire transfers to/from unrelated third parties
- Large number of wire transfers for large round dollar amounts
- Indications of frequent overrides of established approval authority and other internal controls
- Wiring of funds without normal identifying information or in a manner that indicates an attempt to hide the identity of the sender or recipient
- Wire transactions designed to evade the $3,000 identification/recordkeeping requirement
- Wire transactions sent or received from the same individual to or from different accounts
- Transactions sent by or to noncustomers, also known as “Payable Upon Proper Identification” (PUPID)

Certificate of Deposit Red Flags

- Early redemption of certificates of deposit without regard to penalties
- Used as collateral for loans
- Disbursement of certificates of deposit by multiple bank checks or to unrelated third parties

Safe Deposit Box Red Flags

- Frequent visits to safe deposit boxes by one or more customers
- Visits to safe deposit boxes after withdrawals of large amounts of currency/purchases of monetary instruments
- Multiple safe deposit boxes rented by the same customer
- Safe deposit box opened by an individual who does not reside or work in the area
- Signatories have no apparent business or personal relationship

Lending Red Flags

- Early repayment of a loan in currency or monetary instruments (particularly for problem loans)
- Structured payments of loan in currency or monetary instruments
- Disbursement of loan proceeds via structured currency withdrawals or monetary instruments
- Disbursement of loan proceeds to a third party
- Third-party payment of a loan
- Unwillingness to provide information about the purpose of the loan and/or source of repayment and/or collateral
- Loan collateralized with a currency deposit, certificate of deposit, funds from an offshore account or in the name of a third party
- Loan proceeds are transferred offshore without apparent reason
- Attempts to sever any paper trail connecting a loan with the collateral for that loan
- Early pay-down or pay-off of a large loan, with no evidence of refinancing or other explanation

Mortgage and Real Estate Red Flags

- Borrower arrives at a real estate closing with a significant amount of cash
- Borrower purchases property in the name of a nominee, such as an associate or a relative
- Borrower negotiates a purchase for market value or above asking price, but records a lower value on documents, paying the difference “under the table”
- Borrower sells property below market value with an additional “under the table” payment
- Borrower or agent of the borrower purchases property without much knowledge about the property inspection or does not appear sufficiently knowledgeable about the purpose or use of the real estate being purchased
- Borrower purchases multiple properties in a short period of time or appears to be buying and selling the same piece of real estate for no apparent legitimate purpose
- Seller requests that proceeds be sent to a high-risk jurisdiction or offshore bank
- Borrower makes payments with funds from a high-risk jurisdiction or offshore bank

Credit Card Red Flags

- Prepayment of credit card, particularly when refund checks will be issued to the customer

- Payment of credit card from high-risk jurisdiction or offshore bank
- Payment of credit card with cash or currency
- Payment of credit card by unrelated third parties
- Multiple payments within a billing cycle
- Prepayments followed by cash advances/purchases of convenience checks
- Payment of private label credit cards via gift card from the merchant
- Credit card refunds from merchants without offsetting transactions

Trade Finance Red Flags

- Items shipped that are inconsistent with the nature of the customer's stated line of business
- Obvious over- or under-pricing of goods and services
- Transactions involving high-risk goods (e.g., weapons, ammunition, chemicals, sensitive technical data, nuclear materials, precious gems, crude oil)
- Goods are transshipped through one or more jurisdictions for no apparent economic reason
- Missing trade documentation information (e.g., name and address of applicant/beneficiary, name and address of issuing/advising banks, specified or determinable amount and type of currency, sight or time draft to be drawn, expiry date, general description of merchandise, types and numbers of documents that must accompany the credit)
- Unwillingness to provide documents to prove the shipment of goods
- Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction
- Documentation showing a higher or lower value or cost of merchandise than that which was declared to customs or paid by the importer
- Documentary fraud
- Changes in payment instructions
- Excessively amended letters of credit
- Presentations of letters of credit or documents where the financial institution has no record of the credit's existence
- Letter of credit that includes a condition for a "switch bill of lading"
- Bill of lading describing containerized cargo, but without container numbers or with sequential numbers
- Invoice showing miscellaneous charges (e.g., handling charges greater than 40 percent of total invoice value)
- Transaction(s) involving front/shell companies

Capital Market Products Red Flags

- An account shows an unexplained high level of funds transfer activity with a very low level of securities transactions
- Client deposits or attempts to deposit cash at a financial institution that does not routinely accept cash
- Client takes both a short and a long position in a security or contract for similar amounts and similar expiration dates with no apparent business purpose
- Customer appears to be acting as an agent for an undisclosed third party, but declines or is reluctant to provide information relating to the third party
- Customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer the proceeds out of the account

- Customer funds an account with funding sources such as traveler's checks, third-party checks, checks made out to cash, etc.
- Transactions originating from/destined to high-risk jurisdictions that were not included as expected transactions in the account profile and/or are otherwise unexpected
- Transactions where the beneficiary name is not the account holder, or where the wire instruction is not the standard wire instruction provided at account opening
- Large trades/purchases performed in accounts with small balances
- Transactions/trades that consistently result in large losses

Insurance Products Red Flags

- Customer's lack of concern with the cost of the policy
- Customer's lack of concern with the performance of an insurance product
- Customer's lack of concern with the penalties/fees
- Purchase of a product that appears outside the customer's normal range of wealth or estate planning needs
- Large single-payment premiums for life and annuity policies
- Unusual methods of payment, particularly cash or cash equivalents
- Multiple currency equivalents from different banks and money services businesses used to make payments
- Beneficiaries that are unidentified or located in high-risk jurisdictions
- Policy repayments that are inconsistent with the customer's source of funds and/or income
- Premium payments that are made by apparently unrelated third parties
- Policy assigned to a third party soon after it is purchased
- Early policy cancellation (particularly during the free-look period of annuity contracts)
- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge

Casino Red Flags

- Gaming transactions that do not correspond with the customer's profile (e.g., stated business, income/salary)
- Structuring of cash transactions in an attempt to evade currency transaction reporting requirements (e.g., $9,900)
- An initial deposit of funds with the casino is either cashed out or transferred to a bank account with minimal or no gaming activity
- Customer betting with unusual characteristics (e.g., betting both sides of an even bet)
- Customer transfers chips to other individuals to cash out
- Customer redeems chips for casino checks that amount to significantly more than the amount of funds deposited with no apparent winnings to account for the additional amount

Retail Red Flags

- Purchase of luxury items in cash or monetary instruments
- Return of high-value items paid for in cash or monetary instruments to obtain a check refund
- Purchase of prepaid access/gift cards with cash or monetary instruments
- Structuring of cash transactions in an attempt to evade Form 8300 reporting requirements by making purchases at different point-of-sale (POS) terminals or various branches

- Refusal to provide personal information for purposes of filing Form 8300 or other recordkeeping and reporting requirements
- Transactions on behalf of individuals/corporations located in jurisdictions with little or no AML regulation; countries with known drug, criminal or terrorist links; and offshore entities in tax havens
- Transactions made by high-risk customers, such as senior foreign political figures, if known
- Purchases that are inconsistent with past purchasing trends
- Third-party payments for luxury items
- Willingness to trade or exchange items for less than retail value
- Purchases of large quantities of precious metals and stones (e.g., gold, diamonds), fine art and other valuable items (e.g., stamps)
- Purchases of items in bulk that are small in size and high in value
- Purchases of items in bulk that are easy to resell online (e.g., baby formula, razors)

Consumer Products Red Flags

- Cross-border sales to transfer funds and/or goods across jurisdictions
- Profit margin on equipment/goods appears unrealistically high, indicating the possible sale of stolen equipment/goods
- Payment of proceeds to/by an unrelated third party

Human Trafficking

- Customer with an excessive number of individual accounts
- A common mobile number, address and/or employment references that are used to open multiple accounts under different names
- Customer's telephone numbers linked to personal advertisements verified through public sources
- Customer's address linked to residence and/or hotel with suspected ties to trafficking (e.g., named in previous investigations and busts, offer hourly rates)
- Households with an unusually high number of residents who also appear unrelated
- Accounts opened in the name of unqualified minors
- Accounts reported for identity theft
- Accounts opened with fraudulent or missing/incomplete documentation
- Repeat payments to advertisers that promote the sex industry (e.g., websites, newspapers, escort services)
- Bill payments using money orders as opposed to paying with personal checks
- Cash deposits into one account from multiple locations throughout all states
- Frequent use of cash couriers
- High number of cash deposits structured to avoid reporting requirements
- Frequent deposits and withdrawals from multiple ATMs
- Frequent transfers utilizing money transmitters to common recipients often in high-risk countries
- Frequent transfers or checks payable to casinos
- Frequent payments for rent, hotels, airline tickets or other travel-related accommodations
- Frequent small-dollar international funds transfers for "repayment of debt"
- High volume of payments for multiple mobile phones

- High volume of deposits of government benefits for multiple beneficiaries followed immediately by cash withdrawals
- Accounts lacking commercial activity or activity inconsistent with the stated nature of business/expected activity;
- Purchases of luxury items or assets in high-risk countries
- Account activity beyond the living standard of the account holder

Elder Financial Abuse

- **Changes in transaction activity** – The elder's spending pattern may change, including:
    - Decreased spending on essential items (e.g., food, medication, utilities, etc.)
    - Increased spending and purchases of unnecessary items or items he/she can't use
    - Numerous withdrawals, including the maximum ATM withdrawal
    - Checks may be written out of sequence
    - Large wires to third-party beneficiaries with unclear relationships with the elder
- **Unexplained activity** – The activity may not make logical sense, given known details about the customer:
    - ATM withdrawals, when the elder is homebound
    - The sudden presence of overdrafts, when previously there had been limited to no insufficient funds activity
    - Numerous unpaid bills, when someone has been designated to pay them
    - An appearance of checks or signed documents, when the elder cannot write or lacks the capacity to understand what he/she is signing, or the signature on checks and documents may not resemble the elder's signature
- **Changes in account features** – The elder may request the addition of account features or changes to existing features, including:
    - A request for the issuance of a credit or debit card for the first time
    - Seeking to enroll in online banking
    - Changing the account beneficiary
    - Requesting that statements be sent to an address besides his/her own
- **Uncharacteristic requests** – The elder may seek to undertake a non-routine transaction, including:
    - Refinancing a mortgage
    - Closing a certificate of deposit without regard to penalties for early withdrawal
    - Requesting to wire a large sum for no apparent purpose

Informal Value Transfer System (IVTS) Red Flags

- Structured currency deposits to individual checking accounts, often well below the typical levels for reporting, with multiple daily deposits to multiple accounts at different branches of the same bank on the same day
- Consumer checking accounts used for a period of time and then becoming dormant, and in some cases, overdrawn
- Personal checking accounts opened by foreign nationals who come to the bank together
- Multiple accounts opened on the same day or held by the same foreign nationals at various banks
- Frequent structured cash purchases of monetary instruments, including money orders or bank checks made payable to the same individuals or entities
- Lack of payee/payer information on the monetary instruments

Terrorist Financing Red Flags

- An account for which several persons have signature authority, yet these persons appear to have no relation to each other
- An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organization
- Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g., student, unemployed, self-employed)
- Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (e.g., countries designated by national authorities)
- Transactions to/from nonprofit or charitable organization for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction

Employee Red Flags

- Employee has lavish lifestyle inconsistent with his or her salary
- Employee continuously overrides internal controls
- Employee is reluctant to take long vacations
- Significant personal credit problems
- Behavioral changes indicating possible drug, alcohol, gambling addiction or fear of losing job
- High employee turnover, especially in areas vulnerable to fraud
- Refusal to take vacation or leave
- Lack of segregation of duties

AML TECHNOLOGY

Overview

1140. How can technology be used to support a financial institution's AML program?

Much has been written about the use of technology to support a financial institution's AML compliance efforts. Technology can be used, for example, to support:

- Monitoring for suspicious transactions and facilitating SAR filings
- Monitoring for large currency transactions and facilitating CTR filings
- Verification of customer information (e.g., Customer Identification Program [CIP])
- Storage of customer information (e.g., CIP, customer due diligence [CDD], enhanced due diligence [EDD])
- Calculation of customer risk ratings
- Searching against special lists of prohibited and/or high-risk individuals/entities (e.g., Office of Foreign Assets Control [OFAC], 314(a), subpoenas, media searches, internal "deny" lists, politically exposed persons [PEPs]) for customers and transactions
- AML training
- Case management

1141. Can one system support multiple aspects of an AML program?

Some vendors offer modules that support various compliance needs; other vendors have alliances with other companies to offer an institution a wider range of services.

Since customer bases and levels of transaction activity vary across institutions, each institution needs to consider the software package(s) that best meets its requirements, requiring minimal add-on services.

1142. What are the benefits of implementing AML software on an enterprise-wide basis rather than on a local basis?

An increasing number of large financial institutions are selecting and implementing AML software on an enterprise-wide basis, as this can be cost-effective and can enhance efficiency and consistency throughout an organization.

1143. What are some of the important considerations that should go into a decision to purchase AML technology?

When selecting a technology solution, financial institutions should address vendor qualifications and capabilities, technical factors, functionality, customer support and cost. Some of the key characteristics to consider include, but are not limited to, the following:

Vendor

- How long has the software vendor been in the market? Is the vendor viable?
- What experiences have other financial institutions had with the vendor and software?
- Is the vendor knowledgeable of regulatory requirements?
- For international financial institutions, is the vendor able to provide services on a global basis (e.g., multilingual capabilities)?
- Is the system an enterprise-wide solution across business lines (e.g., bank, broker-dealer, insurance)?

Technical Factors

- Is the system scalable in terms of transactions/customers?
- What security features does the system have (e.g., controls)?
- Does the solution provide a detailed audit trail?
- Will the installation require significant customization (e.g., data feeds, parameters)? To what extent? How will the extent of customization impact the implementation and costs of the system?
- How are upgrades delivered to the financial institution?
- Is the software compatible with the institution's existing hardware or will additional hardware need to be purchased?

Customer Support

- Is the software user-friendly (e.g., does it have a graphical user interface [GUI])?
- How are upgrades implemented?
- Does the vendor provide training (initial and ongoing)?
- Does the vendor assist financial institutions with customizing the system?

Cost

- What pricing model (e.g., per user, site license, transaction volume) is offered by the vendor?
- Is the implementation included in the cost of the system?
- Is ongoing customer support included in the cost of the system?
- Are upgrades included in the cost of the system?

Disaster Recovery/Business Continuity

- Are the vendor's disaster recovery/business resumption plans adequate to avoid unacceptable disruption to the compliance program?

1144. Should a financial institution have a dedicated information technology (IT) resource to support its AML program?

As with any type of technology, a financial institution should ensure it has the appropriate personnel to support its AML technology. As the reliance on AML technology increases, financial institutions should frequently assess personnel needs to ensure business processes are adequately supported. The financial institution should review its personnel complement to ensure the technology and compliance staff can work efficiently together and that they understand both AML regulatory and industry requirements and how these requirements translate into technical specifications.

1145. What documentation should be maintained regarding systems used to support the AML compliance function?

Regulators expect institutions to have a complete set of documentation surrounding the design, implementation, testing and usage of the system(s). Any changes to the system(s) should be formally approved and documented.

1146. What are some challenges in selecting, implementing and maintaining an AML technology solution?

Some challenges include:

- Assuming more expensive or feature-rich sophisticated AML technology solutions are appropriate based on the size of the institution (e.g., not considering types of customers, products, services, geographies or risk)
- Underutilization of the features of implemented AML technology solutions
- Rushing to implement technology without considering process changes to maximize the utility of the technology
- Selection of an enterprise-wide solution that may not address local needs (e.g., inability to monitor products offered by all the divisions or branches of the institution, inability to adjust rules and parameters for different locations)
- Lack of understanding transaction data, including source and data feeds (e.g., unaware of missing transaction data due to disparate systems)
- Overreliance on vendors to tailor the AML technology solution to the needs of the institution
- Overreliance on system manuals; lack of development of tailored user manuals for all AML-related systems (e.g., functionality, rationale for system criteria/thresholds, etc.)
- Insufficient reporting of key metrics related to AML technology solutions to assist with improving the efficiency and effectiveness of implemented solutions (e.g., number of customers, transactions, alerts, investigations, etc.)
- Lack of conducting cost-benefit analysis when selecting a new solution or considering upgrades
- Insufficient incorporation of risk assessment methodologies in determining monitoring priorities and system criteria/thresholds
- Insufficient internal controls and processes for system changes (e.g., use or nonuse of specific features, changing of thresholds/parameters, upgrades and ongoing maintenance to systems, etc.)
- Incompatibility with or difficulty in integrating with core systems
- Costs and/or willingness of the vendor to support customization

Suspicious Transaction Monitoring and Suspicious Activity Report Filing Software

1147. Is there a requirement that a financial institution use automated AML software?

Certain jurisdictions require the use of automated systems. For example, in 2003, Switzerland set a precedent by becoming the first country to issue rules requiring banks and securities houses to use automated AML transaction monitoring software. In 2005, the Philippines mandated the use of automated monitoring systems, and in 2007, India's finance ministry asked all banks to install automated software.

Although there are no regulations requiring U.S. financial institutions to use automated software for AML monitoring, regulators have encouraged financial institutions to adopt such software, and in some cases, have required the implementation of software under the terms of enforcement actions.

1148. What types of suspicious transaction monitoring software are currently available?

Several different types of suspicious transaction monitoring software are currently available. Some of the most commonly used AML technologies include rules-based software, profiling software and artificial intelligence (AI) software or predictive analysis.

Rules-based software flags any transaction or activity that violates a business rule. For example, a common rule is to flag any transaction involving particular countries that are designated as high risk by the institution. Rules-based software can be customized over time through the addition and/or refinement of rules. Rules-based software is suitable for known patterns of suspicious activity (e.g., four cash transactions aggregating to less than $10,000 within a 30-day period).

Profiling software uses a combination of predictive profiles developed from a customer's identification and customer due diligence (CDD)/enhanced due diligence (EDD) information, as well as historical transactions. Profiling software is designed to flag transactions that are out of profile by utilizing means, standard deviations and thresholds. Profiling software is suitable for both known and unknown patterns of suspicious activity.

AI software offers the most complex technology solutions, using neural networks and other intelligent technologies; it continually updates customer profiles based on cumulative transactions. AI technologies can identify transaction patterns between accounts, compare transaction activity to established money laundering methods, and assess and score transactions for suspicious activity. AI technology should be built on specific business rules, enabling the system to identify suspicious activity based on patterns and sophisticated algorithms. This technology is usually more sophisticated than rules-based software, making the detection of unusual or suspicious activity more efficient.

1149. What are some of the important considerations that should go into the decision to purchase suspicious transaction monitoring software?

There are many important considerations that should go into this decision, including, but not limited to, the following:

- What type(s) of monitoring does the system perform (e.g., AI, rules-based, profiling, outlier detection)?
- Can the system incorporate the financial institution's customer risk assessment results (i.e., establish conditional thresholds based on the results of the customer risk assessment)?
- Does the system have comprehensive monitoring reports, such as:
    - Profiling – the comparison of actual activity against average or expected activity
    - Outlier detection – the identification of activity that significantly deviates from the norm
    - Text mining/keyword searches
    - Transaction/product-specific alerts (e.g., cash, wires, loans, aggregate activity)
- Does the system enable customization of alert criteria?
- How does the system output alerts (e.g., one report per alert criteria, consolidated reports by customer, on-screen only)?
- Does the system include a case management feature for tracking and documenting investigations?
- Does the system facilitate the electronic filing of SARs?
- Does the system provide flexible reporting (e.g., alerts generated, alerts cleared, alerts resulting in a SAR, SARs filed)?
- Is the system scalable?

The reasons and rationale for choosing a particular monitoring system should be well documented. The documentation should be able to articulate how the monitoring system's functionality will meet the financial institution's risk profile and needs.

1150. If cost is not a factor, should a financial institution select the most sophisticated transaction monitoring system available?

No. A financial institution should choose the transaction monitoring system that appropriately addresses its needs. Vendors offer a wide array of products and services; the most sophisticated solution may not be appropriate. Highly complex systems require significant implementation time and training. The investment may not be worth the return if the same objectives can be achieved with a different solution.

1151. What can institutions expect when the transaction monitoring system is implemented?

Upon initial implementation of the monitoring software, the number of alerts generated can be overwhelming. This can result when the criteria for generating alerts has not been fully customized to the size and customer profile of the

financial institution, when there is insufficient historical data within the system, when overly conservative variance parameters have been set, or a combination of these factors.

Financial institutions must recognize that adjustments and fine-tuning will be necessary before an automated system is effective. A significant amount of time should be allocated to this fine-tuning in the initial implementation phase. In addition, financial institutions may need to adjust the organizational structure and number of AML compliance staff to ensure alerts generated are reviewed properly and in a timely manner.

The reasons for changes made to the system parameters following the initial implementation, which can be based on risk appetite, statistical analysis and regulatory guidance, should be well documented.

1152. What are the main factors that influence the cost associated with implementing automated AML monitoring software?

Key cost drivers of the implementation of AML monitoring software include, but are not limited to, the following:

- Complexity of current system environment (e.g., number of transactional systems, data center locations)
- Customization requirements of AML monitoring software functionality and reports
- Transactional data quality
- Conversion of current transactional data

1153. What types of controls need to be in place to protect the integrity of an automated transaction monitoring system?

A system administrator or IT team should be responsible for protecting the integrity of an automated AML system by developing and ensuring compliance with detailed policies and procedures regarding the following:

- Validation of data integrity from the source data (e.g., the financial institution's posting system) to the data warehouse of the automated AML system
- Validation of programming methodology used by the automated AML system
- Customization of thresholds and documentation of all changes approved by the compliance department
- Additions/deletions of products/services and business units
- Updating of government and other high-risk lists utilized in the system (e.g., OFAC)
- Maintenance of a control list of end users with read, write and/or author access

The authority to establish or change expected activity profiles should be clearly defined and should generally require the approval of the AML compliance officer and/or senior management. Controls should ensure limited access to the monitoring system.

Management should document and be able to explain filtering criteria, thresholds used, and how both are appropriate for the financial institution's risks.

1154. To what extent can financial institutions rely on suspicious transaction monitoring software?

Even though highly sophisticated suspicious transaction monitoring software is currently available, software is only a tool and one component of an effective suspicious activity monitoring program. Equally, if not more, important are the experience levels and knowledge of personnel charged with reviewing and interpreting alerts. Financial institution employees who deal directly with customers are in the best position to know and understand their customers' transactions. Those employees should be aware of AML requirements and risks, and should be trained to identify unusual or potentially suspicious transactions.

Additionally, a financial institution's suspicious transaction monitoring software may not be capable of monitoring all types of customers, products and/or transactions. For example, trade finance and select correspondent banking activity may require manual procedures for potentially suspicious activities. Current events that may impact a financial institution's customer base also need to be considered when monitoring transactions.

Ultimately, it is the financial institution's responsibility to identify a suspicious transaction. An element of judgment inevitably is involved in identifying potentially suspicious transactions, and an automated system cannot replace this degree of judgment.

The best defense for a financial institution is to have a strong AML program that includes controls and procedures for transaction monitoring and employee training, with emphasis on the employee's responsibility with respect to monitoring. A financial institution that utilizes suspicious transaction monitoring software should have procedures in place to review, modify and further customize the criteria of the automated monitoring software to generate meaningful alerts on an ongoing basis.

1155. Should the financial institution rely upon the software vendor's predetermined screening criteria?

There is no "one-size-fits-all" approach that works equally for all financial institutions. Predetermined screening criteria may be helpful for establishing a benchmark; however, each financial institution is unique and requires a customized solution, based on the products/services, industry, and size and profile of its customer base. The responsibility for implementing an effective AML program ultimately falls on the financial institution, not on third-party software vendors.

1156. What inputs should a financial institution consider to establish rules and scenarios in its suspicious activity monitoring software?

Financial institutions should consider the following inputs when establishing rules and scenarios in its suspicious activity monitoring software:

- **Regulatory requirements** - Some parameters are dictated by regulatory requirements (e.g., cash transactions greater than $10,000, potentially suspicious activities greater than $5,000 (or $2,000 in the case of money services businesses (MSB), monetary instruments between $3,000 and $10,000). Establishing parameters to aid in the detection of customers attempting to evade BSA reporting requirements is one starting point.
- **Suspicious Activity Red Flags** – The FFIEC BSA/AML Examination Manual provides common red flags for potentially suspicious activity for multiple customer products and transactions as well as account and customer-level behaviors, many of which can be used to create monitoring rules or establish parameters.
- **Software vendor** – Predetermined criteria can be helpful in establishing benchmarks.
- **Affiliates and peers** – Leveraging the experience of affiliates and peers with similar customer base, product offerings and risk profile can aid in establishing monitoring rules and parameters.
- **Previous monitoring reports, investigations and suspicious activity report (SAR) filings** – Reviewing the results of previous monitoring reports (e.g., manual, automated reports based on previous suspicious activity monitoring software) can assist financial institutions in identifying rules and parameters that were the most effective in identifying potentially suspicious activity.
- **Results of risk assessments** - Management can use AML risk assessments to establish priorities for monitoring, as well as the features the monitoring system will need to incorporate for the organization's unique risk profile (i.e., the financial institution's customers, products, services and geographies). The results from customer risk assessments can be utilized to establish risk-based thresholds.
- **Customer expected activity** – Expected activity can be obtained directly from each customer during the account opening process or developed independently by the financial institution based on historical transaction history for segments of its customer population or from other information. This information can be used to establish custom profiles in suspicious activity monitoring software and help financial institutions determine whether transaction activity is normal or potentially suspicious.

For additional guidance on risk assessments, please refer to the sections: Enterprise-wide Risk Assessment, Business Line Risk Assessment and Customer Risk Assessment.

1157. How can a financial institution determine “normal” expected activity for each of its customers for the purposes of establishing custom suspicious activity monitoring profiles?

Some financial institutions ask for the following information directly from their customers during the account opening process:

- Deposits/credits per month (number and volume)
- Withdrawals/debits per month (number and volume)
- Cash transactions (number and volume)
- Wire transfer transactions (number and volume)
- Purpose of account
- Origination/destination country(ies) of incoming/outgoing wire transfers or other types of payments

To facilitate the account opening process, some financial institutions provide ranges of activity with triggers to ask for additional information if specified dollar thresholds are met or higher risk activities are identified. It is important to note that although customers may answer these questions to the best of their ability, their responses are often guesstimates and may need to be reviewed and revised throughout the duration of the relationship.

Financial institutions can also establish custom profiles by analyzing underlying transaction activity based on defined segments, including, but not limited to, the following:

- Customer type (e.g., business, individual)
- Geography (e.g., home address, place of business)
- Nature of business/occupation
- Account type (e.g., savings, checking, certificate of deposit, loan, etc.)
- Account balance
- Transaction volume

For example, some financial institutions have opted to segment their customer population by customer type, geography (foreign/domestic) and class based on volume of transaction activity and balances held in their accounts to establish custom profiles in their suspicious activity monitoring software.

1158. Does implementing automated transaction monitoring software eliminate the need for all manual monitoring?

No. There are other potential “triggers” for potentially suspicious activity that exist outside of an automated monitoring system, such as notification of suspicious activity by employees, 314(a) requests, subpoenas and the media. For example, the names of individuals and/or companies involved in or potentially involved in money laundering schemes often are disclosed in the press. Financial institutions need to be aware of this so that they can identify whether any of the named individuals and/or companies are customers of the financial institution.

Additionally, an automated system may not capture all products (e.g., letters of credit, loans, pouch activity, capital markets transactions). In such instances, manual monitoring may be necessary.

1159. How often should suspicious transaction monitoring software be reviewed and updated?

To ensure a suspicious activity monitoring program remains efficient and effective, financial institutions should review their suspicious activity monitoring software annually, at minimum. Additionally, software should be reassessed when new products or services are introduced, with each merger/acquisition, when new markets are targeted (e.g., type of customer, country of domicile of customer) or when there are significant upgrades to the software.

Documentation to explain adjusted filtering criteria, thresholds used, and how both are appropriate for the financial institution’s risks should also be brought current when updates to software are made.

1160. How can a financial institution evaluate the effectiveness of its suspicious activity monitoring program?

When assessing overall effectiveness, the evaluation should not be limited to AML technology, but should include the overall suspicious activity monitoring program, including systems, personnel, procedures and training. Some indicators and areas to assess include, but are not limited to, the following:

- **Alert-to-Case Ratio:** Financial institutions should review system rules that have low alert-to-case ratios to identify parameters that could be adjusted to reduce the volume of "false positives" (alerts cleared without escalation). Another indicator of ineffective monitoring is if a high percentage of recurring alerts were previously investigated and deemed not suspicious.
- **Case-to-SAR Filing Ratio:** Similar to alert-to-case ratios, analyzing cases that lead to SAR filings may assist financial institutions in refining controls to better detect potentially suspicious activity by identifying high-risk products, services, customers or geographies that may require specific system rules or a separate manual monitoring process. In circumstances with low case-to-SAR filing ratios, the financial institution may need to revisit existing parameters, data feeds and staff training to reduce the number of false positives.
- **Non-System Sourced Cases/SAR Filings:** Repeat cases and SAR filings from non-system sources may provide insight into the development of new or enhanced monitoring rules (e.g., law enforcement inquiries, 314(a) and 314(b) information requests, etc.). However, if more SARs are filed on non-system sourced referrals than from automated alerts, existing monitoring rules need to be reviewed for effectiveness.
- **Lack of Alerts Generated for a Certain Product or Transaction Type:** This may indicate that a product or transaction type is not covered in the suspicious activity monitoring software, or that the existing rules and thresholds are ineffective in monitoring for potentially suspicious activity. In some instances, a manual monitoring process may need to be implemented to cover a particular product or transaction type (e.g., trade finance, etc.).
- **Few Alerts Generated for High-Risk Customers:** This may indicate an ineffective customer risk assessment methodology, ineffective incorporation of risk into suspicious activity monitoring software, or both.
- **Wide-Ranging Rates of Clearing Alerts by Investigative Personnel:** Developing a process in which more complex alerts and cases are assigned to seasoned personnel may improve the overall efficiency of the monitoring and investigation process. Additionally, to ensure alerts are properly reviewed, quality control reviews of cleared alerts by more experienced staff can be conducted. For additional guidance on conducting investigations, please refer to the Transaction Monitoring, Investigations and Red Flags section.
- **Alert Assignment and Case Management:** In many cases, different system rules may generate alerts on the same activity; therefore, a comprehensive alert and case management system that assigns alerts based on customer and account relationships is critical to overcome any inefficiencies in reviewing the same transaction(s) flagged by multiple monitoring rules. A proper case management system should also incorporate non-system sourced cases (e.g., law enforcement inquiries, etc.).
- **Usefulness of Individual Rules/Scenarios:** Looking at how many alerts are generated from individual rules and the extent to which these alerts ultimately result in SARs being filed may yield results that can be used to modify or delete certain rules.
- **High Volume of Repeat SAR Filings on the Same Subject(s):** This may indicate an ineffective customer termination policy.
- **Backlogs or Late SAR Filings:** This may indicate ineffective use of monitoring software, lack of required personnel commensurate to the volume of alerts, inadequate knowledge and experience of monitoring and investigation personnel, and/or lack of appropriate management reporting to track and aid in understanding and promptly addressing any growing backlogs.
- **Auditors/Regulators Identify Suspicious Activity Unreported on SARs Filed by the Financial Institution or Question the Quality and Completeness of Investigation Files:** This may indicate that the monitoring and investigation team lack: relevant industry/product knowledge; an understanding of applicable AML risks; fraud and forensic training/healthy dose of skepticism; the ability to work effectively with business lines to gather and document pertinent information; or an understanding of system functionality or detection logic.

Financial institutions should continuously review published typologies to identify emerging risks or controls to assist them in enhancing their suspicious activity monitoring program.

Overall, each component of a financial institution's monitoring program (including individual system rules and resulting alerts) should be analyzed individually and collectively for overall effectiveness. Potential root causes for ineffective or deficient monitoring programs generally can be traced to the following:

- The number and qualifications of individuals assigned to the monitoring and investigation team(s)
- Adequacy and communication of training on policies and procedures
- Use (or misuse) of technology

1161. How should a financial institution utilize its AML risk assessment to implement its suspicious activity monitoring program?

A financial institution's AML Business Line Risk Assessment (BLRA) identifies monitoring priorities on an enterprise or macro level. BLRA results can be used to identify overall system and personnel needs.

A financial institution's customer risk assessment assesses money laundering and terrorist financing risk on a customer level and can be used as a direct input into its suspicious activity monitoring system.

Although these risk assessments drive the monitoring program, the process is cyclical. Trends observed from alerts, cases and SARs from the AML monitoring program should be considered when updating the financial institution's BLRA and customer risk assessment methodologies.

For additional guidance on risk assessments, please refer to the Business Line Risk Assessment and Customer Risk Assessment sections.

Case Management Software

1162. What types of case management systems are currently available?

Vendors have developed an array of case management systems covering the majority of tasks assigned to the AML compliance department. For example, case management systems can be used not only to facilitate the handling of alerts generated from an automated transaction monitoring system, but also to facilitate the Currency Transaction Report (CTR) filing and exemption process, the following up on customer acceptance exceptions, and the review and regular update of customer risk ratings and profiles.

1163. What are some of the important considerations that should go into a decision to purchase a case management tool?

There are many important considerations that should go into this decision, including, but not limited to, the following:

- Does the system have the ability to import data from multiple sources (e.g., transaction monitoring alerts, internal referrals)?
- Does the system have workflow management capabilities (e.g., assignment of cases, multi-user-level hierarchy)?
- Does the system have the ability to upload attachments (e.g., internal e-mails; research, such as Internet; correspondence with customer; customer identification information)?
- Does the system have the ability to export summaries of investigation out of the system?
- Does the system have record retention abilities to retain cases for future investigations, examinations and audits?

For further guidance on general considerations for AML technology providers relating to technical factors, customer support, cost and disaster recovery, please refer to the Overview section.

Large Currency Transaction Monitoring and Currency Transaction Report Filing Software

1164. What types of currency transaction monitoring and CTR filing solutions are currently available?

Available CTR filing solutions range from stand-alone systems that function only in the back office to fully integrated solutions that provide real-time aggregation to the front office. Additionally, some systems include functionality to monitor for suspicious currency activity and manage the financial institution's Currency Transaction Report (CTR) exemption process.

1165. What are some of the important considerations that should go into a decision to purchase a currency transaction monitoring and CTR filing solution?

There are many important considerations that should go into this decision, including, but not limited to, the following:

- Does the system have real-time aggregation?
- Does the system handle aggregation for foreign customers and/or foreign currencies?
- Does the system link related customers?
- Are noncustomer transactions captured?
- Does the system include all currency transactions (e.g., ATMs)?
- Can the system integrate with a customer information platform (i.e., automatically upload from a customer information platform or manually enter information)?
- Does the system have an intrinsic case management feature (e.g., assign cases to multiple users, document reason for not filing CTR)?
- Does the system facilitate the electronic filing of CTRs, the CTR amendment process and/or the CTR exemption process?
- Does the system include a reporting/trending capability for historical CTR filings?
- Does the system have record retention capabilities to comply with recordkeeping requirements for CTRs?

For further guidance on general considerations for AML technology providers relating to technical factors, customer support, cost and disaster recovery, please refer to the Overview section.

Customer Information Database and Customer Risk Assessment Software

1166. What types of customer information databases are currently available?

Financial institutions can benefit from housing all customer information (e.g., name, address, salary/revenue, occupation/industry, transaction profile, customer risk assessment score) in one central location. Many, however, heavily weigh the benefit of housing all customer information in one place against the cost of doing so. Legacy core system enhancements typically require significant effort (e.g., time, resources) and may even disrupt normal business processes. As a result, vendors are providing financial institutions with a number of options, including developing "add-on" databases and systems to the institution's core legacy systems, and developing a graphical user interface (GUI) that portrays, on the user's screen, all relevant data, as if it were housed in one central system.

1167. What are some important considerations that should go into a decision to purchase a customer information database solution?

There are many important considerations that should go into this decision, including, but not limited to, the following:

- Does the system have the flexibility to add custom fields/questions for various customer types (e.g., individual, business, trust, NAIC code)?
- Does the system have controls and rules to ensure required fields are triggered and completed during the account opening process?
- In what format is the information maintained (e.g., tables, scanned images)?
- Does the system have the ability to upload documentation obtained from customers?
- Does the system have a tickler system to track exceptions in the quality control process and the ability to notify account officers of exceptions?

1168. What types of customer risk assessment software are currently available?

Automated customer risk assessment solutions range from systems that are incorporated into account-opening platforms to transaction monitoring systems. Wherever the financial institution houses its automated customer risk assessment solution, the financial institution should incorporate the results of the customer risk assessment methodology into its due diligence and enhanced due diligence (EDD) processes.

1169. What are some of the important considerations that should go into a decision to purchase a customer risk assessment solution?

There are many important considerations that should go into this decision, including, but not limited to, the following:

- Does the system allow for custom methodologies for various customer types (e.g., individual, business, trust)?
- Can factors, weights, scores (individual and overall) and bands (e.g., high, moderate, low) be customized?
- Can risk scores be recalculated on a periodic basis?

For further guidance on general considerations for AML technology providers relating to technical factors, customer support, cost and disaster recovery, please refer to the Overview section.

Customer Verification Software

1170. What types of customer verification software are currently available?

Many of the available customer verification software packages utilize a positive verification approach (e.g., comparison against a credit reporting database). Others utilize a negative verification approach (e.g., comparison against a database of customers who have written bad checks), a logical verification approach (e.g., the address provided by the customer is located in the correct city/ZIP code/area code), or a combination of the three.

Software packages also range from full integration with the customer information database of the financial institution to complete outsourcing.

1171. What are some of the important considerations that should go into a decision to purchase customer verification software?

There are many important considerations that should go into this decision, including, but not limited to, the following:

- What is the method of verification: positive, negative or logical?
- Does the system support verification for individuals and businesses?
- Does the system support verification for domestic and foreign customers?
- Is the verification process conducted in real time or in batch?
- Can the system be integrated with the customer information database?

For further guidance on general considerations for AML technology providers relating to technical factors, customer support, cost and disaster recovery, please refer to the Overview section.

1172. What is the difference between verification and authentication software?

Verification software confirms that the information provided by a customer is valid (e.g., an individual with the provided name, address and TIN matches with an independent source, such as a credit reporting database).

Authentication software attempts to ensure that the individual providing the information (or accessing the account[s]) is the person he or she is claiming to be. Authentication is accomplished by requesting information that is not necessarily "found in a wallet" (e.g., previous address, previous employer). Often, once an individual has been verified, financial institutions will ask customers to create custom security questions (e.g., mother's maiden name, favorite movie, pet's name) that serve to authenticate customers.

List Providers

1173. What types of list providers are currently available?

Various vendors provide lists or databases that can include sanctioned individuals and entities (e.g., SDN), politically exposed persons (PEPs) and subjects of negative media. Credit bureaus are an example of a list provider. Lists can be accessed through the Internet by conducting ad hoc searches or incorporated into an automated screening solution, either independently or as part of an institution's account opening or transaction monitoring software.

1174. How does a financial institution determine which lists should be used when screening its customer base?

Many vendors, when promoting their products, provide the institution with the sources they use when populating their databases of heightened-risk individuals/businesses. Financial institutions should discuss the vendor's sources with their legal department, peers in the industry or other external advisers, as appropriate, to determine which are required and/or appropriate.

1175. Can a financial institution modify the vendor's database to include/exclude other individuals or entities?

Vendors have begun to provide financial institutions with the ability to add individuals and entities they feel should be monitored beyond lists provided by the vendor. Such individuals and entities can include those the financial institution chooses not to do business with anymore and those identified in a 314(a) request. In addition, lists can be modified to exclude individuals or entities from monitoring. The development of these "white lists" can reduce the number of false positive alerts that institutions have to review for customers they are familiar with and know are not a high risk for money laundering or terrorist financing.

1176. What are some of the important considerations that should go into a decision to select a list provider?

There are many important considerations that should go into the decision to select a list provider, including, but not limited to, the following:

- Is the definition/criteria comprehensive and in alignment with internal policy?
- Are the updates (e.g., additions, deletions, enhancements) to lists timely (e.g., real time, daily)?
- Is notification of updates provided to end users?
- Is supplemental information provided with name of individual/entity on the list (e.g., name only, address, aliases, public information)?

For further guidance on general considerations for AML technology providers relating to technical factors, customer support, cost and disaster recovery, please refer to the Overview section.

Interdiction Software

1177. What is interdiction software?

Interdiction software, also known as filtering or screening software, is a tool that facilitates the comparison of separate sets of data (e.g., a customer database, list of individuals/businesses linked to illicit activity) for possible matches. Some vendors provide detailed background information for the individuals/entities, while others provide limited information (e.g., name, address).

Interdiction software can involve screening customers, as well as transactions (e.g., wires, ACHs).

1178. How can interdiction software be used to support an AML/OFAC Compliance Program?

Interdiction software is most commonly used to screen for sanctions violations as part of an institution's AML/OFAC Compliance Program; however, it increasingly is being used to screen for politically exposed persons (PEPs), 314(a), custom internal lists (e.g., terminated customers) and other negative-information databases.

1179. What are the different types of logic used by interdiction software to screen customers and transactions?

Phonetic name matches and fuzzy logic are the two most common logics used by interdiction software to screen customers and transactions.

- **Phonetic matching** is based on the pronunciation of a name as opposed to the spelling.
- **Fuzzy logic** uses an algorithm to calculate the confidence that the two names are the same.
- The more sophisticated interdiction products are designed to recognize vowel and diacritic representations, nonstandard word splitting and concatenation, glottal stops, double letters, and consonants not present in Latin-based alphabets.

1180. What have been some challenges with the utilization of interdiction software?

Institutions have experienced challenges in the utilization of interdiction software, including, but not limited to:

- Limitations in screening algorithms that do not adequately account for misspellings, line breaks or foreign names
- Inconsistent implementation of confidence levels (e.g., 100 percent match) across all products, transactions, customer types and departments
- Lack of understanding and over-reliance on vendors on how the interdiction software works
- Inappropriate use of "exclusion lists" that suppress potential matches

1181. What are some of the important considerations that should go into a decision to purchase interdiction software?

There are many important considerations that should go into this decision, including, but not limited to, the following:

- Does the system include the source lists (e.g., OFAC, other international sanctions programs, custom lists) in addition to the interdiction software?
- Does the system handle screening of customers and all required transaction types (e.g., wires, ACHs)?
- What type of information is maintained by the vendor (e.g., names and addresses of entities/individuals, background information)?
- What is the matching algorithm (e.g., character by character, fuzzy logic, phonetic, Soundex) used by the system?
- Can end users customize the sensitivity level (e.g., 100 percent match, 90 percent match)?
- Does the system have the ability/methodology to suppress repeat false positives?

For further guidance on general considerations for AML technology providers relating to technical factors, customer support, cost and disaster recovery, please refer to the Overview section.

Training Software

1182. What types of training software are currently available?

Some of the most commonly used training solutions include Internet-, intranet- and computer-based training modules.

1183. What are some of the important considerations that should go into a decision to purchase a training solution?

There are many important considerations that should go into this decision, including, but not limited to, the following:

- Is the content comprehensive and current?
- What is the method of delivery (e.g., Internet, intranet, computer-based)?
- What is the method of ensuring comprehension (e.g., quiz, e-mail acknowledgement)?
- Are questions randomized in multiple quiz attempts or is the same quiz used?
- Can end users customize the content and quizzes?
- What are the administrative (e.g., assigning required courses to employees, tracking and retention of scores) and flexible reporting (e.g., number of employees who passed/failed, statistics on frequently missed questions) features?

For further guidance on general considerations for AML technology providers relating to technical factors, customer support, cost and disaster recovery, please refer to the Overview section.

NONBANK FINANCIAL INSTITUTIONS AND NONFINANCIAL BUSINESSES

Nonbank Financial Institutions

1184. What is meant by the term “nonbank financial institution” (NBFI)?

For purposes of our discussion, NBFIs include all entities, excluding depository institutions, that are considered financial institutions under the USA PATRIOT Act. These include, but are not limited to, the following:

- Money services businesses (MSBs)
- Broker-dealers
- Futures commission merchants (FCMs) and introducing brokers (IBs)
- Commodity trade advisers (CTAs)
- Commodity pool operators (CPOs)
- Mutual funds
- Insurance companies
- Casinos and card clubs
- Trust companies
- Operators of credit card systems
- Dealers in precious metals, stones or jewels
- Persons involved in real estate settlements and closings
- Investment advisers
- Unregistered investment companies
- Loan or finance companies
- Nonbank residential mortgage lenders and originators (RMLOs)
- Housing government-sponsored enterprises (GSEs)
- Businesses engaged in vehicle sales, including automobile, airplane and boat sales
- Travel agencies
- Pawnbrokers
- Telegraph companies

For additional guidance on how requirements apply to the types of companies listed above, please refer to the respective questions below.

1185. Some of the companies identified as NBFIs are not “financial institutions” in the traditional sense. Why are they included as “financial institutions”?

Just as is the case with traditional financial institutions, the companies included under the definition of “financial institution” may provide opportunities to money launderers and terrorist financiers (e.g., because they are cash-intensive and/or because they facilitate the conversion of funds into goods that can be used or resold).

1186. Do NBFIs have to comply with all the same provisions of the BSA and USA PATRIOT Act as traditional financial institutions?

Not all provisions of the BSA and USA PATRIOT Act apply to all NBFIs. Additionally, NBFIs that are subsidiaries of bank holding companies (BHC) are typically included in the enterprise-wide AML Compliance Program and subject to organizational requirements to establish an AML program. Some of the differences in application are highlighted in the questions below.

For additional guidance on the various AML requirements common to many of the NBFIs, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections.

1187. With which provisions of the BSA and USA PATRIOT Act should an institution that is in multiple businesses (e.g., banking, broker-dealer, insurance) comply?

At a minimum, individual financial institutions that are subject to issued AML regulations must comply with the specific requirements applicable to their industry. In addition, many diversified organizations with subsidiaries that are subject to AML regulations issued by multiple agencies have chosen to implement enterprise-wide AML standards that apply to all entities within the organization. Of course, some or all of the entities within the organization may need to implement more detailed policies and/or procedures to implement requirements specific to their industries.

It is also worth noting that federal banking regulators have indicated that nonbank subsidiaries and affiliates of insured banks should have effective Customer Identification Programs (CIPs) in place, even though CIP requirements may not apply to these entities by regulation.

It is important to note that some NBFIs are subject to state AML laws and regulations that may impose more stringent requirements on the NBFI (e.g., recordkeeping and suspicious activity reporting requirements for lower transaction thresholds than the federal requirement, record retention periods that are longer than the federal requirement).

1188. Are NBFIs required to comply with OFAC and other sanction regulations?

Yes. OFAC and other sanction requirements apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. In addition, under limited circumstances, sanction requirements apply to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

1189. What are the heightened money laundering and terrorist financing risks of NBFIs?

The following characteristics, which may apply in varying degrees, heighten the money laundering and terrorist financing risks of NBFIs:

- Cash-intensiveness
- High volume of transactions
- High-risk nature of customer base (e.g., high net worth; geographically dispersed; financially sophisticated; increased use of corporate structures, such as offshore private investment companies; lack of ongoing relationships with customers, such as money services businesses [MSBs] and casinos)
- High-risk product offerings (e.g., ability to transfer funds domestically and internationally, particularly to jurisdictions with weak AML requirements; stored-value cards; transportability of merchandise; high-value merchandise; merchandise that is difficult to trace, such as precious stones)
- Ability to transfer value (e.g., conversion to precious gems, immediate or deferred income through insurance and other investment products, real estate)

- Access to funds held in foreign financial institutions or access by foreigners to funds held in domestic financial institutions
- Historically less regulated or less stringently regulated than traditional financial institutions, such as depository institutions
- Potentially weaker controls than traditional financial institutions due to fewer regulatory pressures and/or the private ownership structures
- Difficulty in monitoring for suspicious activity due to complex nature of transactions (e.g., involvement of multiple third parties, therefore decreasing transparency of transaction details)
- Possibility of operating without proper registration or licensing (e.g., MSBs)
- History of abuse by money launderers and terrorists

Money Services Businesses

Definition

1190. What is a money services business (MSB)?

FinCEN's final rule "Definitions and Other Regulations Relating to Money Services Businesses" defines an MSB as "a person wherever located doing business, whether or not on a regular basis or as an organized or licensed concern, wholly or in substantial part within the United States, in one or more capacities" listed below:

- Issuer or seller of money orders or traveler's checks
- Check casher
- Dealer in foreign exchange
- Providers or sellers of prepaid access
- Money transmission (domestic or international)

1191. Which types of MSBs are required to comply with AML laws and regulations?

Any MSB that conducts more than $1,000 in money services business activity with the same person (in an aggregate amount in one type of MSB activity) on the same day or provides money transfer services of any amount must comply with AML laws and regulations. For example, an entity that cashes checks, in aggregate, of more than $1,000 for any person in a single day in one or more transactions is covered and must comply with AML requirements.

Specific AML laws and regulations for an MSB vary based on the activities that it is involved in, as well as whether it is performing as the agent or as the principal MSB.

1192. Are foreign-located entities engaged in MSB activities within the United States subject to AML laws and regulations?

Yes. FinCEN clarified that all entities engaged in MSB activities within the United States, regardless of the physical location of its agents, agencies, branches or offices, are required to comply with AML laws and regulations. Examples include foreign entities with U.S. customers and foreign entities transmitting funds to or from U.S. recipients via the Internet.

Foreign-located entities engaged in MSB activities are also required to designate a person who resides in the United States to function as an agent to accept service of legal process.

1193. Are there plans to modify the definitional threshold of $1,000 for MSB activity?

While FinCEN considered modifying the definitional threshold for MSBs, it has clarified in its recent rulings that the existing threshold will remain at $1,000 (other than a money transmitter that has no definitional threshold).

1194. Are there exemptions to the definition of an MSB?

Yes. The following entities are not included in the definition of an MSB:

- A bank or foreign bank;
- A person registered with and functionally regulated or examined by the U.S. Securities and Exchange Commission (SEC) or the Commodities and Futures Trading Commission (CFTC);
- A foreign financial agency that engages in financial activities that, if conducted in the United States, would require the foreign financial agency to be registered with the SEC or CFTC; or
- A natural person who engages in covered MSB activities on an infrequent basis and not for gain or profit.

1195. Does licensing affect whether an MSB is subject to AML laws and regulations?

A business that engages in covered MSB activity in the United States is subject to AML laws and regulations whether or not it is licensed or required to be licensed. For further guidance, please refer to the Informal Value Transfer Systems section.

Issuers and Sellers of Money Orders and Traveler's Checks

1196. How is the term "issuer and seller of money orders and traveler's checks" defined for MSBs?

An issuer is defined as "a person that issues money orders or traveler's checks that are sold in an amount greater than $1,000 to any person on any day in one or more transactions."

A seller is defined as "a person that sells money orders or traveler's checks in an amount greater than $1,000 to any person on any day in one or more transactions."

1197. What is the difference between an issuer and a redeemer of money orders and traveler's checks?

An issuer of a money order or traveler's check is the business ultimately responsible for the payment of the money order or traveler's check.

A redeemer, or seller, is a business that exchanges money orders and traveler's checks for currency, monetary or other negotiable instruments. The acceptance of a money order or traveler's check as a payment for goods and services is not considered redemption.

Check Cashers

1198. What is a check casher?

A check casher is defined as an entity that provides a customer with money orders, or a combination of currency and money orders, in exchange for a check, in an amount greater than $1,000 on any day in one or more transactions. An entity providing check-cashing services for less than $1,000 is not subject to AML laws and regulations.

1199. Are there exemptions to the definition of a check casher?

Yes. The following entities are not included in the definition of a check casher:

- A person who sells prepaid access in exchange for a check, monetary instrument or other instrument;
- A person who solely accepts monetary instruments as payment for goods or services other than check cashing services;
- A person who engages in check cashing for the verified maker of the check who is a customer otherwise buying goods and services;
- A person who redeems his/her own checks; or
- A person who only holds a customer's check as collateral for repayment by the customer of a loan.

Dealer in Foreign Exchange

1200. What is a dealer in foreign exchange?

A dealer in foreign exchange is defined as "a person that accepts the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more countries in exchange for the currency, or other monetary instruments, funds or other instruments denominated in the currency, of one or more countries in an amount greater than $1,000 for any other person on any day in one or more transactions, whether or not for same-day delivery."

1201. What is a "casa de cambio"?

A "*casa de cambio*," the Spanish term for currency exchange, money exchange, or bureau de change, is a business whose customers exchange one currency for another.

Providers or Sellers of Prepaid Access

1202. How is the term "prepaid access" defined?

The final rule which was issued July 29, 2011, "Definitions and Other Regulations Relating to Prepaid Access" (Prepaid Access rule) imposes regulatory requirements on certain providers and sellers of prepaid access. The rule defines "prepaid access" as the following:

- Access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number or personal identification number. Prepaid access applies to a very broad range of prepaid services, including but not limited to open-loop prepaid access, closed-loop prepaid access, prepaid access given for the return of merchandise, many prefunded employee programs such as a Health Savings Account, etc.

1203. How is the term "provider and seller of prepaid access" defined?

The Prepaid Access rule defines the terms "provider" and "seller" of prepaid access as the following:

- **Providers of prepaid access** – The participant within a prepaid program that agrees to serve as the principal conduit for access to information from its fellow program participants. The participants in each prepaid access program (which may be one or more) must determine a single participant within the prepaid program to serve as the provider of prepaid access ("provider"). The provider also will be the primary contact and source of information for FinCEN, law enforcement and regulators for the particular prepaid program.
- **Sellers of prepaid access** – Any person who receives funds or the value of funds in exchange for an initial or subsequent loading of prepaid access if:
    - That person either sells prepaid access offered under a prepaid program that can be used before the customer's identity can be captured (including name, address, date of birth and identification number) and verified; or
    - That person sells prepaid access (including closed-loop prepaid access) to funds that exceeds $10,000 to any person or entity (there is a limited exception for bulk sales) on any one day and has not implemented policies and procedures to reasonably prevent such sales.

1204. Why did the rule rename "stored value" as "prepaid access"?

The Prepaid Access rule renamed "stored value" as "prepaid access" because the technology used in the stored-value industry has changed. The final rule provides flexibility so it will not become obsolete as the industry advances to encompass all emerging payment methods, including but not limited to personal identification numbers, electronic serial numbers, cards, tokens, key fobs, mobile phones, etc.

FinCEN stated that prepaid access is not itself a device or vehicle, but that devices and vehicles are the means through which prepaid funds are accessed. The two main elements of prepaid access are:

- Funds that have been paid in advance; and
- Those funds that can be retrieved or transferred at some point in the future. FinCEN also clarified that it intended its definition to include the necessary regulatory elasticity to survive future technological advancements.

1205. How does the Prepaid Access final rule amend the regulatory requirements for MSBs?

In addition to updating the definition of "stored value" to "prepaid access," MSBs that qualify as "providers or sellers of prepaid access" are now required to file suspicious activity reports, register with FinCEN and take a number of other actions. Remaining regulations for MSBs remain unaffected by the Prepaid Access rule.

For additional guidance, please refer to the Providers and Sellers of Prepaid Access section.

Money Transmitters

1206. What is a money transmitter?

A money transmitter is defined as the following:

- Any person engaged in the transfer of funds
- A person who provides money transmission services

Money transmission services is defined as "the acceptance of currency, funds or other value that substitutes currency from one person and the transmission of currency, funds or other value that substitutes for currency to another location or person by any means."

"By any means" includes money transmission through the following:

- A financial agency or institution;
- A Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System or both;
- An electronic funds transfer network; or
- An informal value transfer system.

1207. Are there exemptions to the definition of a money transmitter?

Yes. The term "money transmitter" does not include a person who only:

- Provides the delivery, communication or network access services used by a money transmitter to support money transmission services;
- Acts as a payment processor to facilitate the purchase of, or payment of a bill for a good or service through a clearance and settlement system by agreement with the creditor or seller;
- Operates a clearance and settlement system or otherwise acts as an intermediary solely between BSA-regulated institutions, including but not limited to, the following:
    - Fedwire system
    - Electronic funds transfer networks
    - Certain registered clearing agencies regulated by the SEC and derivatives clearing organizations
    - Other clearinghouse arrangements established by a financial agency or institution
- Physically transports currency, other monetary instruments, other commercial paper or other value that substitutes for currency as a person primarily engaged in such business (e.g., armored car) from one person to the same person at another location or to an account belonging to the same person at a financial institution, provided that the person engaged in physical transportation has no more than a custodial interest in the currency, other monetary instruments, other commercial paper or other value at any point during the transportation;
- Provides prepaid access;
- Accepts and transmits funds only integral to the sale of goods or provision of services, by the person who is accepting and transmitting the funds.

Guidance on the Applicability of the Definition of Money Services Businesses

FinCEN has issued considerable guidance on the applicability of the definition of money services businesses to various business types that can be found at www.fincen.gov/statutes_regs/guidance. Several of these sets of guidelines are summarized below.

1208. Is a business that cashes payroll checks for its employees included in the definition of a check casher?

No. According to FinCEN Ruling FIN-2006-G005, a business that cashes payroll checks for its employees does not meet the regulatory definition of a check casher.

1209. Is a payday lender included in the definition of a check casher?

Yes. A payday loan is a short-term loan that is intended to cover a borrower's expenses until his or her next payday. According to FinCEN Ruling 2002-2, a business that provides "payday loans" by providing cash to customers in return for a postdated personal check meets the regulatory definition of a check casher.

1210. Is a "merchant payment processor" included in the definition of a money transmitter?

No. According to FinCEN Ruling 2003-8, merchant payment processors, also known as third-party payment processors, process payments from consumers as an agent of the merchant to which the consumers owe money, rather than on behalf of the consumers themselves; they therefore do not meet the regulatory definition of a money transmitter. The role of the merchant payment processor in these transactions is to provide merchants with a portal to a financial institution that has access to the payment system (e.g., ACH, etc.); it is not to transmit funds on behalf of third parties.

1211. Is a "member-sponsored merchant and/or retail operator of automated teller machines (ATMs) that participates in a third-party prepaid card reload program" included in the definition of an issuer of stored value?

No. According to FinCEN's Ruling FIN-2008-R005, member-sponsored merchants and retail operators of ATMs that participate in a third-party prepaid card reload program serve only as (1) the physical point in the reload process where a card is presented to transmit data to a member of the prepaid card reload program and (2) the point where the customer presents funds for collection. The merchant and retail operator of ATMs do not control nor conduct the actual transaction that results in the adding of value to the reloadable card and therefore do not meet the regulatory definition of an issuer of stored value.

Additionally, regulations also provide that "the acceptance and transmission of funds as an integral part of the execution and settlement of a transaction other than the funds transmission itself will not cause [the merchant and/or ATM retail operator] to be a money transmitter" either. In other words, the act of collecting funds from the customer that is then forwarded to the member for eventual credit to a prepaid card is not considered a funds transfer; therefore the merchant or ATM retail operator is not a money transmitter.

1212. Is a "company that offers a loan acceleration product for consumer financing" included in the definition of a money transmitter?

No. A loan acceleration product is a service that assists borrowers in paying off consumer loans faster, utilizing various methods (e.g., bi-weekly payments). According to FinCEN Ruling FIN-2008-R009, a company that offers a loan acceleration product for consumer financing does not meet the regulatory definition of a money transmitter. Generally, the acceptance and transmission of funds as an integral part of a transaction other than the funds transmission itself (e.g., in connection with a sale of securities or service [loan acceleration]) will not cause a person to be a money transmitter.

1213. Is a "foreign exchange dealer" included in the definition of a dealer in foreign exchange or money transmitter?

Yes. According to FinCEN's Ruling FIN-2008-R002, a foreign exchange dealer is included in the definition of a dealer in foreign exchange as currency from one country is exchanged for currency from another country.

A foreign exchange dealer may also be a money transmitter if it does not limit its business activity to accepting and transmitting funds for the purpose of executing and settling foreign exchange transactions with its unaffiliated

business customers, but also settles transactions by moving funds between its customers and their third-party foreign counterparts through its own accounts.

1214. Is a "foreign exchange broker or consultant" included in the definition of a dealer in foreign exchange or money transmitter?

No. According to FinCEN's Ruling FIN-2008-R004, an "intermediate foreign exchange broker and consultant" is engaged in obtaining interbank prices for the foreign currency transactions of its clients. Because the foreign exchange consultant does not exchange foreign currency in the course of providing its services to its clients, it does not meet the regulatory definition of currency dealer or exchanger.

Additionally, regulations also provide that "the acceptance and transmission of funds as an integral part of the execution and settlement of a transaction other than the funds transmission itself will not cause [the foreign exchange consultant] to be a money transmitter" either. In other words, the forwarding of client funds to another financial institution by the foreign exchange consultant for subsequent exchange by the third-party financial institution is not considered a funds transfer; therefore, the foreign exchange consultant is not a money transmitter.

1215. Is a "person who is engaged in the business of foreign exchange risk management" included in the definition of a dealer in foreign exchange and/or a money transmitter?

Yes. According to FinCEN's Ruling FIN-2008-R003, a person who is engaged in the business of foreign exchange risk management is included in both the definitions of a dealer in foreign exchange and a money transmitter, and thereby is subject to applicable AML requirements.

A foreign exchange risk management company "manages exchange rate risk for Internet seller clients operating in currency A who (1) offer products for purchase by customers who operate in currency B ("sale transactions"), and (2) purchase supplies offered by suppliers who operate in currency C ("supply transactions") by conducting foreign exchange or 'hedging' transactions in the relevant currency for the client." Additionally, the foreign exchange management company settles sale and supply transactions by the following methods:

- Settling Sale Transactions: "Submitting the bank card information of a client's customer, which it has received from the client, to the card processor for authorization and payment. This payment is made into the company's own account, and the company ultimately remits those funds to the client."
- Settling Supply Transactions: "Moving funds from its clients to its clients' suppliers through their own accounts."

The method of managing exchange rate risk falls under the definition of currency dealing and exchanging, as currency from one country is exchanged for currency from another country.

The method of settling supply transactions ("moving funds from its clients to its clients' suppliers through their own accounts") is considered a funds transfer; therefore a person who is engaged in the business of foreign exchange risk management, as defined above, falls under the definition of money transmitter.

Key AML and Sanction Requirements

1216. With which key AML and sanctions requirements are MSBs required to comply?

MSBs must comply with the following key AML and sanctions requirements:

- Establishment of an AML program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program and conducts an independent review of the AML program
- Filing of CTRs
- Filing of SARs (although stored-value providers and check cashers are currently exempt)
- Filing of Reports of Foreign Bank and Financial Accounts (FBAR)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIR)
- Recordkeeping and retention (e.g., Funds Transfer Rule, Travel Rule, Purchase and Sale of Monetary Instruments)
- Information-sharing (i.e., Section 314(a), in some cases, mandatory; Section 314(b), optional)

- Registration with FinCEN (exemption for agents of other MSBs that are MSBs solely because they offer products or services of the other MSBs)
- OFAC and other sanction requirements

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections.

1217. Since MSBs do not have "customers with accounts" in the traditional sense, do they have CIP obligations?

MSBs are not subject to the CIP requirement. However, if an MSB establishes a relationship with a party (e.g., through the issuance of ID cards, stored-value cards, web-based transfer services), additional verification procedures, including the adoption of a KYC program, would be appropriate. Gathering information up front will assist the MSB with its monitoring and, as necessary, reporting of CTRs and SARs.

1218. Are MSBs required to file CTRs?

Yes, MSBs are required to file CTRs. For a listing of financial institutions required to file CTRs at the time of this publication, please refer to the Currency Transaction Reports section.

1219. Can MSBs grant CTR exemptions?

No. Only depository institutions (banks, savings associations, thrift institutions or credit unions) can grant exemptions, and then only for their U.S. customers.

1220. Should an MSB with multiple agents aggregate cash transactions across agents for CTR filing purposes?

FinCEN has indicated that multiple currency transactions occurring across multiple agents must be aggregated for CTR reporting when the MSB has knowledge that they are by or on behalf of the same person, and meet the CTR reporting threshold.

For example, an MSB has two agents, Agent A and Agent B. A customer goes to Agent A and sends $7,000 to an individual and, on the same day, goes to Agent B and sends an additional $7,000 to the same (or another) individual. Both transactions are conducted in cash, and neither agent is aware of the other transaction. In this case, the MSB must file a CTR if it knows that multiple currency transactions aggregating to more than $10,000 have been conducted by the same person on the same day. Financial institutions need to take care to understand whether they will be deemed to have such knowledge, as some financial institutions that have failed to aggregate appropriately have been fined.

1221. Is the SAR filed by MSBs unique?

Beginning March 29, 2012, FinCEN replaced industry-specific SAR forms with a single form that must be submitted electronically. However, FinCEN will continue to accept legacy versions of the new SAR via electronic means until March 31, 2013. If an MSB decides to continue to submit legacy reports, it is required to file the Suspicious Activity Report by Money Services Businesses (SAR-MSB) for suspicious transactions of $2,000 (or aggregating to $2,000) or more, except for transactions relating to clearance records or other similar records of money orders or traveler's checks, in which case suspicious transactions that involve or aggregate to $5,000 or more are to be reported. MSBs also can voluntarily file on suspicious transactions that are less than $2,000.

1222. What types of activities require a SAR to be filed for MSBs?

MSBs should file a SAR upon detection of the following activities:

- **Transactions aggregating to $2,000 (except where detailed below) or more that involve potential money laundering or violations of the Bank Secrecy Act (BSA)** – Any transaction(s) totaling or aggregating to at least $2,000 (except where detailed below) conducted by a suspect through the MSB, where the MSB knows, suspects or has reason to suspect that the transaction either: involved illicit funds or is intended or conducted to hide or disguise funds or assets derived from illegal activities (including, but not limited to, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any law or regulation or avoid any transaction reporting requirement under federal law; or is designed to evade any BSA regulations.
- **Transactions relating to clearance records aggregating to $5,000 or more that involve potential money laundering or violations of the BSA** – An MSB should file a SAR whenever it detects any known or suspected

federal criminal violations or pattern of violations have been committed or attempted through it or against it involving clearance records or other similar records of money orders or traveler's checks that have been sold or processed.

- **Evasion** – A SAR should be filed in any instance where the MSB detects that the transaction was designed to evade any BSA regulations, whether through structuring or other means.
- **No business or apparent lawful purpose** – The transaction has no business or apparent lawful purpose, and there is no known reasonable explanation for the transaction after examination of available facts, including the background and possible purpose of the transaction.
- **Facilitate criminal activity** – The transaction involves the use of the MSB to facilitate criminal activity.

For red flags that assist in identifying suspicious activity as outlined above, please refer to the Suspicious Activity Red Flags section.

1223. Are there exemptions to the suspicious activity reporting requirement of MSBs?

The SAR requirement currently does not apply to MSBs engaged solely in check cashing.

Therefore, if an MSB provides, for example, wire transfers and check cashing, its SAR filing requirements would apply only to its wire transfer activities. MSBs can, however, voluntarily file SARs on check cashing.

1224. Should MSBs file SARs on behalf of their agents?

Yes. An MSB must file SARs on any covered suspicious activity that is transferred or transacted through it, or is attempted, including suspicious activities at its agent locations.

1225. Are there red flags for detecting potentially suspicious activity for MSBs?

Yes. A comprehensive list of red flags for detecting potentially suspicious activity relating to transaction execution and high-risk products/services/transactions (e.g., cash, wires, monetary instruments) has been provided in this publication. Common red flags include, but are not limited to, the following:

- For monetary instruments:
    - Monetary instruments purchased on the same or consecutive days at different locations, and/or are numbered consecutively in amounts designed to evade reporting requirements (i.e., under $3,000 or $10,000), or are purchased in round amounts
    - Blank payee lines
    - Instruments which contain the same stamp symbol or initials
- For funds transfers:
    - Frequent, large, round dollar wire transactions
    - Wire transfers to and from bank secrecy haven countries and countries known for or linked to terrorist activities, drug trafficking, illegal arms sales or other illegal activity

For further guidance on red flags, please refer to the sections: Suspicious Activity Red Flags, Currency Red Flags, Monetary Instrument Red Flags and Informal Value Transfer System (IVTS) Red Flags.

1226. Must an MSB maintain its AML program in English?

There is no prohibition against an MSB maintaining its AML program in a language other than English. In fact, where English is not the first language of the business's owners, employees or customers, maintaining an AML program in the language(s) most commonly used may be particularly helpful. However, FinCEN requires that, upon request, an English language translation be available within a reasonable period of time. Businesses, therefore, would be well-advised to maintain English translations of key documents, such as policies and procedures, to ensure that they can meet the "reasonable" time frame required by FinCEN.

1227. Are MSBs required to hire a certified public accountant (CPA) or outside consulting company to perform the independent review of the AML program?

No. In implementing the independent testing requirement, FinCEN stated that MSBs are not required to hire a CPA or an outside consultant to conduct a review of their programs. The review may be conducted by an officer, employee or

group of employees so long as the reviewer is not the designated compliance officer of the MSB and does not report directly to the compliance officer, nor have other responsibilities for AML compliance. For additional guidance on independent testing, please refer to the Independent Testing section.

1228. What type of information should an MSB be prepared to provide to a financial institution when establishing an account relationship?

MSBs should be prepared to provide the following information to a financial institution when establishing an account relationship:

- Basic identifying information about the MSB, its owners and principal officers, and a history of its operations
- Products and services offered
- List of branches and agents, including the jurisdictions in which they operate
- FinCEN registration, if required
- Proof of compliance with state or local licensing requirements, if applicable
- Anticipated account activity (e.g., volume and type of transaction activity, seasonal fluctuations)
- Purpose of the account(s) (e.g., domestic remittances, remittances to foreign-based agents)
- Results of the independent testing of the AML program (unless subject to attorney-client or work product privilege or other confidentiality obligation)
- Written AML policy
- Written agent management, termination and employment screening practices

Financial institutions may choose to require additional information from an MSB either at account opening or at a later date.

1229. What are the key recordkeeping requirements of the BSA for MSBs?

The BSA requires the retention of all BSA reports (e.g., SARs, CTRs, FBARs, CMIRs). Additionally, other required documentation must be retained by dealers in foreign exchange, such as the following:

- When required, a taxpayer identification number (TIN) (or passport number or description of a government-issued identification for nonresident aliens) of each person for whom a transaction account is opened or a line of credit is extended and for each person who has a financial interest in the account
- List of names, addresses and account or credit line numbers of those persons from whom the dealer in foreign exchange was unable to obtain the above information
- Statements of accounts from banks, including paid checks, deposit slips, charges or other debit and credit entry memoranda, representing the entries reflected on such statements
- Records of each exchange of currency involving transactions in excess of $1,000, including the name, address, TIN or passport number; date and amount of transaction; currency name; and total amount for each foreign currency
- Signature cards or other documents evidencing signature authority over each deposit or security account containing the name of the depositor, address, TIN or passport number, and signature of the depositor or authorized signer
- Each item, including checks, drafts or transfers of credit, of more than $10,000 remitted or transferred to a person, account or place outside of the United States
- A record of each receipt of currency, other monetary instruments, investment securities and checks, and of each transfer of funds or credit of more than $10,000 received on any one occasion directly and not through a domestic financial institution, from any person, account or place outside of the United States
- Records prepared or received by a dealer in the ordinary course of business, which would be needed to reconstruct an account and trace a check in excess of $100 deposited in such account through its internal recordkeeping system to its depository institution or to supply a description of a deposited check in excess of $100

- A record maintaining the name, address, TIN or passport number of any person presenting a certificate of deposit for payment, as well as a description of the instrument and date of transaction
- A system of books and records that will enable the dealer in foreign exchange to prepare an accurate balance sheet and income statement

The above applies to currency dealers or exchangers. The BSA outlines additional requirements for other types of financial institutions (e.g., depository institutions, broker-dealers, casinos) as well. For further guidance, please refer to the Recordkeeping Requirements, Broker-Dealers and Casinos or Card Clubs sections.

1230. Are check cashers subject to additional recordkeeping requirements of the BSA for MSBs?

No. Check cashers are not required to maintain additional records under the recordkeeping requirements of the BSA for MSBs specific to their check cashing activity as with money transmitters, issuers of monetary instruments, and currency dealers (e.g., Funds Transfer Recordkeeping Requirement and Travel Rule, Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments). However, if they provide money services other than check cashing, they are required to maintain records as detailed above. For additional guidance on recordkeeping requirements, please refer to sections: Funds Transfer Recordkeeping Requirement and Travel Rule and Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments.

1231. Are MSBs required to conduct AML and OFAC risk assessments?

AML regulations do not require that MSBs conduct written AML risk assessments; however, MSBs are expected to develop and maintain risk-based compliance programs. This requires that they conduct AML risk assessments. The AML risk assessments developed by MSBs should address such factors as geographic risk, product risk (e.g., limits, in-person or Internet services) and risks associated with the agents and other business partners of an MSB.

The same reasoning applies to conducting OFAC risk assessments. For additional guidance on AML and OFAC risk assessments, please refer to the Risk Assessments section.

1232. Are MSBs required to conduct customer risk assessments?

As previously indicated, MSBs often do not have “customers” per se. However, in instances where MSBs do have “customers” or collect sufficient information on parties involved in transactions to be able to profile these parties, they should conduct customer risk assessments and tailor their AML Compliance Programs, particularly monitoring, to the risk.

1233. As customers, should all MSBs unilaterally be considered high risk?

No. The risks of each MSB should be assessed based on a variety of factors (e.g., product/service offerings, nature and geography of customer base, size and geography of operations, and nature of services. Evaluating the risks of MSBs in this manner will result in different risk ratings (e.g., low, moderate, high). However, as a practical matter given the nature of the business, most MSBs are likely to have high or moderate (not low) inherent risk.

1234. Are MSBs required to maintain separate checking accounts for their check cashing and money transmissions lines of business?

No. According to FinCEN Ruling FIN-2008-R012, MSBs are not required to maintain separate checking accounts for their check cashing and money transmission lines of business. In some instances, however, as a requirement to establish an account at a bank, MSBs may be required to establish separate accounts for their various lines of business in accordance with the bank’s internal policy.

1235. Who is responsible for examining MSBs for compliance with AML requirements?

The responsibility for examining MSBs is delegated to the IRS by FinCEN. Many states also examine MSBs and their agents for compliance with AML and other federal and state requirements.

Registration

1236. What is the registration requirement for MSBs?

MSBs are required to register by filing the Registration of Money Services Business (RMSB) report with FinCEN.

1237. What is the purpose of the registration requirement for MSBs?

The purpose of the registration requirement is to identify MSBs that are operating so they may be monitored for compliance with AML laws and regulations.

1238. Are all MSBs required to register with FinCEN?

All MSBs must register with FinCEN, except the following:

- An MSB that solely serves as an agent of another MSB
- U.S. Postal Service
- Government agencies

1239. Should each branch of an MSB register separately with FinCEN?

No. An MSB should not register each branch separately with FinCEN.

1240. How should MSBs submit RMSBs to FinCEN?

While it is not currently mandatory, MSBs should submit RMSBs to FinCEN via the BSA E-Filing System, an Internet-based e-filing system developed by FinCEN to enable financial institutions to file BSA reports electronically. Paper filings will be accepted.

1241. What should an MSB do if an error was found on an RMSB?

An MSB should do the following:

- Complete Part I of a new registration form in its entirety and only those other entries that are being added or changed
- Include a copy of the prior report (or the acknowledgement from FinCEN if received) with the corrected report
- Resubmit the updated registration form and prior report to FinCEN

1242. What information does an MSB have to include with respect to its agents on its RMSB?

An MSB needs to provide the following information on its agents:

- Number of agents authorized to conduct each money services activity (e.g., money order sales, check cashing, currency exchange) on behalf of the MSB
- Jurisdictions in which it is conducting business that include jurisdictions in which it has agents

1243. What information must a provider of prepaid access provide when registering with FinCEN?

In addition to a complete and accurate RMSB form, a prepaid access provider is, among other things, required to provide a complete list of the prepaid programs for which it serves as a provider.

1244. What supporting information is an MSB required to maintain as it relates to its RMSBs?

An MSB is required to maintain the following supporting documentation:

- Copy of its registration form
- An annual estimate of the volume of the registrant's business in the coming year
- The name and address of owner(s) or individual(s) who control the business (i.e., any shareholder holding more than 5 percent of the registrant's stock, any general partner, any trustee, any director, any officer)
- An agent list

1245. Should an MSB send this supporting information to FinCEN along with its RMSB?

No. The supporting documentation detailed above should not be sent to FinCEN but should be maintained at a location within the United States for five years.

1246. Are MSBs required to reregister after the initial registration with FinCEN?

Registrations must be renewed every two years. FinCEN provides an MSB Registration Renewal Calculator to assist in determining the appropriate renewal deadline.

Reregistration also is required when one of the following events occurs:

- A change in ownership or control of the MSB requiring reregistration under state registration law
- More than 10 percent of voting power or equity interest of the MSB is transferred (except certain publicly traded companies)
- A 50 percent or more increase in the number of agents

The reregistration form must be filed within 180 calendar days after such a change occurs.

1247. What are the consequences of not registering?

MSBs that fail to register or to renew their registrations may be subject to civil and criminal penalties.

1248. Is registration the same as licensing?

No. Registration is administered by FinCEN. Licensing is administered by each state and imposes separate requirements on MSBs. Operating an unlicensed MSB where licensing is required is illegal. For additional details on unlicensed MSBs, please refer to the Informal Value Transfer Systems section.

1249. Do MSBs need to indicate on the RMSB all states in which they originate transactions or only states in which the MSB maintains a physical presence?

When filing FinCEN's Registration of Money Services Business form, MSBs should only indicate states in which the MSB, its agents or branches have a physical presence.

1250. Will FinCEN continue to administer the monthly MSB Registration List?

No. The monthly MSB Registration List has been replaced by the MSB Registration Website. The MSB Registration Website will be updated weekly. New RMSBs will be added to the MSB Registration Website within approximately two weeks of electronic filings and 60 days for paper filings.

1251. Is inclusion on the MSB Registration Website a recommendation or endorsement from FinCEN?

No. Inclusion on the MSB Registration Website is not a recommendation or endorsement of the MSB from FinCEN or any other government agency. The MSB Registration Website is intended only as general reference for the public.

1252. Does inclusion on the MSB Registration Website serve as evidence of an MSB's registration with FinCEN?

Yes. Since the implementation of the MSB Registration Website, FinCEN will no longer be sending registration acknowledgement letters. The MSB Registration Website will provide MSB Registration Numbers, as well as the name of the registrant, states where the registrant engages in MSB activities and the types of MSB activities provided.

1253. Can unlicensed MSBs register with FinCEN?

Yes. Unlicensed MSBs can be registered with FinCEN. MSB registration is required for all covered MSBs, regardless of whether the business is subject to state licensure. However, most licensed MSBs are covered MSBs and, thus, are required to register.

Agents

1254. How is the term "agent" defined for MSBs?

The term "agent" is a separate business entity from the MSB that the MSB authorizes, through written agreement or otherwise, to sell its MSB services (e.g., monetary instruments, funds transfers). MSB agents engaging in covered

activities are MSBs, too, and are subject to the AML requirements. Agents may include businesses such as grocery stores, convenience stores, travel agencies and gas stations.

1255. Is an employee of an MSB considered an agent?

No. A person who is solely an employee of the MSB is not an agent of that MSB.

1256. What are the heightened money laundering and terrorist financing risks of agents?

Agents pose similar if not more heightened risks than do principal MSBs, due to the same factors that heighten the risks of MSBs relative to other types of financial institutions (e.g., banks, broker-dealers, etc.). These factors include, but are not limited to, the lack of traditional relationships with "customers," the lack of compliance-related experience of owners/management, the lack of sophisticated internal controls and high employee turnover. Further, for many though not all agents, their MSB business is secondary to their primary business and may not, therefore, be subject to the same focus on compliance that principal MSBs exhibit.

1257. What information is an MSB required to maintain about its agents?

Each MSB that is required to register must prepare and maintain a list of its agents. The agent list is not filed with the registration form but must be maintained at a location in the United States. The list must include the following specific information:

- Agent name
- Agent address
- Agent telephone number
- The type of service(s) provided by each agent on behalf of the MSB
- Identification of the months in the immediately preceding 12 months in which the gross transaction amount of each agent with respect to financial products/services issued by the MSB exceeds $100,000
- The name and address of any depository institution at which an agent maintains a transaction account for part or all of the funds conducted by the agent on behalf of the MSB
- The year in which each agent first became an agent of the MSB
- The number of branches or subagents that each agent has

The list should be updated annually and retained for a period of five years. Upon request, the MSB should make the agent list available to FinCEN, the IRS and appropriate law enforcement agencies. Requests for such information should be coordinated through FinCEN. An MSB's regulators and auditors also may request such information.

1258. What due diligence should MSBs conduct when acquiring and maintaining agents?

Based upon risk, MSBs should conduct due diligence and enhanced due diligence (EDD) when acquiring and maintaining agents, including, but not limited to, the following:

- Performing adequate due diligence to ensure that the business is in good standing
- Performing background checks and credit checks on the primary owners of the agent
- Performing due diligence necessary to understand the agent's operations, customer base and services (e.g., periodic onsite visits, maintaining and updating agent due diligence on a regular basis)
- Obtaining letters of reference
- Ensuring that the agent has an effective AML program in place or that the agent agrees to adopt the MSB's AML program
- Requiring that the agent agrees to share relevant information upon request of the MSB

1259. What is mystery shopping and are MSBs required to mystery shop their agent locations?

Mystery shopping is a process that involves mystery shoppers visiting an MSB and posing as customers and providing detailed evaluations of their experience (both good and bad) using written reports or questionnaires. Mystery shopping may have multiple objectives (e.g., ensuring employees are adhering to applicable laws and

regulations and following the company's internal policies and procedures, evaluating customer service, and/or assessing how well employees are meeting company sales goals).

Agent mystery shopping is not a regulatory requirement. However, mystery shopping has become a growing industry practice used to identify and mitigate risks associated with agent relationships.

1260. What is a foreign agent or foreign counterpart of an MSB, and what are the heightened money laundering and terrorist financing risks of foreign agents?

A foreign agent or counterpart of an MSB is a business outside of the United States that the MSB authorizes, through written agreement or otherwise, to sell its instruments or, in the case of funds transmission, to receive or pay its funds transfers or facilitate other flow of funds into and out of the United States. MSBs utilize relationships with foreign agents and counterparties to facilitate the movement of funds into or out of the United States, similar to correspondent banking relationships. The movement of money through wire transfers to or from foreign establishments may place MSBs at higher risk of facilitating the flow of illicit funds or legitimate funds used for illicit purposes.

1261. Has any guidance been issued relating to an MSB's obligations with respect to foreign agents and foreign counterparts?

FinCEN issued interpretive guidance requiring that an MSB's AML program be capable of detecting the abuse of products and services offered through foreign agents or counterparties by establishing procedures for:

- Conducting due diligence on foreign agents and counterparties, including, but not limited to, identification of the owners and evaluation of their operations and policies, procedures and controls to determine whether they are reasonably designed to help ensure they are not subject to abuse
- Performing risk-based monitoring on foreign agents and foreign counterparts
- Taking corrective action or terminating relationships, as appropriate

Informal Value Transfer Systems

Definition

1262. What is an informal value transfer system (IVTS)?

IVTS refers to any system, mechanism or network of people that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, regardless of whether it is in the same form. They are networks that facilitate the transfer of value (e.g., cash, commodities) domestically or internationally outside the conventional financial systems. IVTS activities often do not involve traditional banking transactions or services, such as deposit or lending products, although they may sometimes use banking systems. IVTSs are also known as informal money transfer systems (IMTSs), underground banking systems and alternative remittance systems.

A few of the more common examples include hawala, hundi, fei-ch'ien and the Black Market Peso Exchange (BMPE).

Hawala is an Arabic word that means "a bill of exchange or promissory note." Hundi, a word that originated in India, means "trust" and "reference." Fei-ch'ien, a Mandarin word, translates into "flying money" or "fast money." In addition, several studies have identified other IVTSs, including, but not limited to, phoe kuan (Thai), hui k'uan (Mandarin), ch'iao hui (Mandarin), nging sing kek (Cantonese), hui kuan (Vietnamese), stash house (South American) and chit house (British).

1263. What characteristics of an IVTS make it a preferred method of transferring funds by criminals?

The following characteristics of an IVTS make this system a preferred method of transferring funds for illicit purposes:

- Many transactions do not involve the physical or electronic transfers of funds but instead are an exchange of debt
- There are no official receipts of deposit funds and very limited or no paperwork

- Due to the complex variations that can be used to conduct these transactions, they can be very difficult to detect

1264. How do IVTSs work?

The various informal money transfer systems often provide paperless banking transactions and enable individuals to transfer large sums of cash from one country to another without the funds ever crossing borders or being recorded. The IVTS makes minimal use of any sort of negotiable instrument; the system is simply based on trust and "recordless" systems of transactions.

Transfers of money take place based on communications between members of a network of dealers. For example, when an individual wishes to send money to relatives in another country, he or she may contact local IVTS agents, who communicate payment instructions to their counterparts in the relatives' country. The counterparts complete the transaction(s) and balance their accounts with future payments in the opposite direction. In some cases, IVTS agents utilize the traditional banking system and wire payments or funds transfers or other financial transactions on behalf of their customers. It is this latter type of IVTS that can be detected by a financial institution as an unlicensed money transmitter.

1265. Are IVTSs used only to transfer money?

No. Commodities can be transferred through this system as well.

1266. Are IVTSs illegal?

Yes. IVTSs are unlicensed money transmitters. Operating an unlicensed MSB, unless otherwise exempt from licensure by law, is deemed to be engaging in money laundering.

1267. Are IVTS operators required to comply with AML requirements?

All money transmitters, licensed or not, are required to comply with applicable AML requirements. As a practical matter, however, an unlicensed money transmitter is unlikely to be in compliance with AML requirements.

1268. What actions should a financial institution take if a customer is suspected of being an IVTS operator?

A financial institution that suspects or knows a customer is operating as an illegal money transmitter should file a SAR with FinCEN and then determine if it should close the account(s).

1269. Are there any penalties for unlicensed money transmitters/IVTS operators?

Yes. Penalties for operating an illegal money transmitting business include civil and criminal fines, imprisonment, or both.

Black Market Peso Exchange

1270. What is the Black Market Peso Exchange (BMPE)?

A well-known IVTS is the BMPE. Generally, the BMPE is an intricate money laundering system in which Colombian cartels sell drug-related U.S.-based currency to black market peso brokers in Colombia who, in turn, place the currency into U.S. bank accounts. The brokers then sell monetary instruments drawn on their bank accounts to Colombian importers who use them to purchase foreign goods, or they pay for goods directly on behalf of the importers with reimbursement upon delivery of the goods in Colombia. Although the BMPE in Colombia is one of the more widely known IVTSs, BMPEs operate in other parts of the world, too.

1271. How can financial institutions incorporate the detection of the BMPE within their suspicious activity monitoring programs?

Detecting BMPE activity is very difficult due not only to the complexity of the scheme but the lack of any one participant having access to all of the underlying transaction details necessary to detect such activity. Whether a broker, a *casa de cambio* or a bank, it is the responsibility of each participant to conduct adequate due diligence into the source and purpose of funds. Common red flags include, but are not limited to, the following:

- Structured currency deposits to individual checking accounts, often well below the typical levels for reporting, with multiple daily deposits to multiple accounts at different branches of the same bank on the same day

- Consumer checking accounts used for a period of time and then becoming dormant, and in some cases, overdrawn
- Personal checking accounts opened by foreign nationals who come to the bank together
- Multiple accounts opened on the same day or held by the same foreign nationals at various banks
- Frequent structured cash purchases of monetary instruments, including money orders or bank checks made payable to the same individuals or entities

For additional guidance on how to detect BMPE activity, please refer to sections: Informal Value Transfer System (IVTS) Red Flags and Trade Finance Red Flags.

Reintegro

1272. What does the term "reintegro" mean?

"Reintegro" refers to a trade-based, reverse-BMPE laundering scheme that hinges on trade document manipulation and often includes the corruption of a bank employee or customs official. Unlike traditional BMPE activities that operate with goods (not funds) crossing the border, in reintegro transactions, peso exchange brokers repatriate drug proceeds by disguising them as payments for nonexistent or overvalued goods using purchased export papers, similar to letters of credit, to make the payments appear legitimate. This is known as "reintegro" or "reintegrate papers."

1273. What is an example of a reintegro scheme?

The following is an example of a reintegro scheme:

A Colombia-based peso broker purchases legitimate export forms from a corrupt bank employee and establishes a shell company, National Fruit. The Colombian peso broker's U.S.-based partner also establishes a shell company, Worldwide Fruit. Both companies share the same names with legitimate fruit companies as detailed on the purchased export forms. Both open business accounts at financial institutions in their respective countries. Cash derived from the selling of drugs in the United States is then structured/smurfed into Worldwide Fruit's business account. The Colombia-based broker, under the pretense of shipping fruit to the United States, presents the purchased export forms to his financial institution to create the appearance that National Fruit has a legitimate reason to receive funds from Worldwide Fruit (i.e., payment for shipment of fruit). The funds are sent to National Fruit and deposited at the official exchange rate, which is more profitable than the traditional BMPE, where peso brokers sell pesos to Colombian businesses at a discounted rate.

1274. How many times can export papers be used to "reintegrate" illicit funds?

In the United States, these purchased export papers or reintegro papers can remain valid for up to one year, so criminals are able to sell their use multiple times within that year.

Providers and Sellers of Prepaid Access

Definitions

1275. What are the key features of FinCEN's final rule, "Definitions and Other Regulations Relating to Prepaid Access"?

The final rule which was issued July 29, 2011, "Definitions and Other Regulations Relating to Prepaid Access" (Prepaid Access rule) imposes regulatory requirements under the Bank Secrecy Act to entities involved in the provision or sale of prepaid access of virtually all types (open- or closed-loop) through nearly any means (card, code, fob, smart phone, etc.).

Certain providers and sellers of prepaid access are subject to numerous AML and information capture and retention requirements. Non-bank financial institutions, retailers, merchants and others who offer or sell such products are subject to portions of the Prepaid Access rule.

There are two separate prongs of the rule:

- Whether a prepaid access arrangement requires a "provider" as defined in the Prepaid Access rule; and
- Whether an entity or person that sells prepaid access qualifies as a "seller of prepaid access" under the rule. An entity that is involved in any way with prepaid access should carefully evaluate whether its activities are covered in either prong.

Key features of the final rule include:

- Defining key terms including:
    - **Prepaid access** – Access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number or personal identification number. Prepaid access applies to a very broad range of prepaid services, including but not limited to open-loop prepaid access, closed-loop prepaid access, prepaid access given for the return of merchandise, many prefunded employee programs such as a Health Savings Account, etc.
    - **Prepaid program** – An arrangement under which one or more persons acting together provide(s) prepaid access. The functionality of the specific prepaid access offered may determine regulatory obligations. Certain exemptions apply.
    - **Providers of prepaid access** – The participant within a prepaid program that agrees to serve as the principal conduit for access to information from its fellow program participants. The participants in each prepaid access program (which may be one or more) must determine a single participant within the prepaid program to serve as the provider of prepaid access ("provider"). The provider also will be the primary contact and source of information for FinCEN, law enforcement and regulators for the particular prepaid program.
    - **Sellers of prepaid access** – Any person who receives funds or the value of funds in exchange for an initial or subsequent loading of prepaid access if:
        - That person either sells prepaid access offered under a prepaid program that can be used before the customer's identity can be captured (including name, address, date of birth and identification number) and verified; or
        - That person sells prepaid access (including closed-loop prepaid access) to funds that exceeds $10,000 to any person or entity (there is a limited exception for bulk sales) on any one day and has not implemented policies and procedures to reasonably prevent such sales.
- Renaming "stored value" as "prepaid access";
- Replacing the terms "issuer" and "redeemer" of prepaid access with the terms "provider" and "seller";
- Expanding AML requirements to include providers and sellers of prepaid access (e.g., registration requirements for "providers"; and for any entity that is a provider or seller of prepaid access, suspicious activity reporting, currency transaction reporting, customer information recordkeeping, policies and procedures, internal controls, training, new transactional recordkeeping and independent audits);
- Guidelines to assist participants in determining who would serve as the provider for the particular prepaid program; in the event the participants do not determine who will serve as the provider then it will be determined by FinCEN (although there is no grace period or safe harbor extended where the provider was not identified by the participants). If there is only one party in the prepaid program, and its prepaid access does not qualify for an exemption then it must be the prepaid access provider (unless it is a bank);
- Exemptions for lower-risk prepaid access arrangements with qualifying exclusions;
- Exemptions for bank centric programs for the provider of prepaid access requirements; and
- Limited exemptions for sellers of prepaid access.

1276. Why did the rule rename "stored value" as "prepaid access"?

The final rule renamed "stored value" as "prepaid access" because the technology used in the stored-value industry has changed. The final rule provides flexibility so it will not become obsolete as the industry advances to encompass all emerging payment methods, including but not limited to personal identification numbers, electronic serial numbers, cards, tokens, key fobs, mobile phones, etc.

FinCEN stated that prepaid access is not itself a device or vehicle, but that devices and vehicles are the means through which prepaid funds are accessed. The two main elements of prepaid access are:

- Funds that have been paid in advance; and
- Those funds that can be retrieved or transferred at some point in the future. FinCEN also clarified that it intended its definition to include the necessary regulatory elasticity to survive future technological advancements.

1277. What are the heightened money laundering and terrorist financing risks of prepaid access?

Transactions may involve funds that have been transferred to or from an unknown party or from a party that wants to engage in illicit transactions or money laundering. Law enforcement has voiced concerns in part due to the ease with which prepaid access can be obtained, the high velocity of money that potentially can be moved with prepaid access and the anonymous use of some prepaid access. However, unlike cash, there are records available for all of the transactions performed for a particular prepaid access device.

Following are examples of types of factors that may increase the risk associated with a prepaid access product:

- Reloadability
- High value/unlimited load amount
- Lack of account relationship with issuer and/or seller of the products
- Lack of identification of purchaser
- Source used to fund product is cash, credit card or another stored-value product
- Ability to conduct cross-border transactions
- Ability to make cash withdrawals

1278. Is the definition of prepaid access limited to cards?

No. The regulatory definition of prepaid access was designed to be applicable to emerging and developing technologies, which may include but are not limited to the following:

- Near field communications (NFC) (set of short-range wireless technologies that establish electromagnetic radio fields that enable devices to communicate with each other when touching or in close proximity)
- Chip technology
- Magnetic strips
- Cellular phones
- Prepaid access through the Internet using PINs/codes
- Prepaid access through fobs, tokens, chips or other technology
- E-cards
- Virtual currency

Prepaid access products encompass a large number of current and emerging growth products, such as open-loop general purpose reloadable (GPR) cards, certain closed-loop cards, mobile phone access, fob or barcode access.

1279. Do all types of prepaid access products pose the same degree of risk?

No. FinCEN has issued guidance that the following types of prepaid access products pose lower risk:

- **Closed-loop prepaid access** - Prepaid access to funds or the value of funds with a maximum dollar threshold of $2,000 that can be used only for goods or services involving a defined merchant or location (or set of locations), such as a specific retailer or retail chain, a college campus, or a subway system;
- Devices that do not permit international use (e.g., use at foreign merchants via the Internet or face to face);
- Non-reloadable devices

1280. What is the difference between a closed-loop and open-loop prepaid access product?

Closed-loop prepaid access products are usable only at a specific merchant, or a group of merchants using the same branding, such as a Starbucks card. They may be in a fixed amount or reloadable. Open-loop prepaid access products may be used at multiple merchants, such as a prepaid card that contains a Visa logo and can be used at any merchant that accepts Visa debit cards. Open-loop cards may also come in fixed or reloadable amounts.

1281. Can a closed-loop prepaid access product be used to launder illicit funds?

As with any type of payment product or service, it is possible for a closed-loop prepaid access product to be misused. Law enforcement has identified instances where drug dealers used illicit funds to purchase closed-loop gift cards, and the cards were then used to purchase retail items. However, there have been few reported incidents of misuse of either closed- or open-loop prepaid cards in the United States to date, especially for cards issued by a U.S.-based issuer.

1282. Which prepaid access arrangements are excluded from the definition of prepaid access program?

The rule has identified five arrangements that are excluded from the definition of prepaid access program with three high-risk factors that would negate some exclusions. Two of the five excluded arrangements can be summarized as follows:

- Prepaid access to funds with the following criteria:
    - Load limit less than or equal to $1,000 at the point of initial load;
    - Total maximum value less than or equal to $1,000 can be accessed at any point in the lifecycle of the prepaid access; and
    - Less than or equal to $1,000 can be withdrawn with the use of the prepaid access on any given day.
- Payroll and Benefit Cards - The payment of benefits, incentives, wages or salaries through payroll cards or other such electronic devices for similar purposes;

If the aforementioned excluded arrangements display any one of the following three high-risk factors, they would no longer be exempt from prepaid access regulations:

- International use (e.g., can be used to withdraw cash or purchase goods and services from foreign ATMs or foreign merchants via the Internet or in person);
- Person-to-person transfers; and
- Re-loads from a non-depository source (e.g., retail stores, MSBs).

The three remaining excluded arrangements can be summarized as follows:

- Closed-loop products with a maximum value less than or equal to $2,000 on any day that cannot be redeemed for cash;
- Government Funded Prepaid Access - Payment of government benefits such as salaries, tax refunds, and benefits, including unemployment, child support, disability, social security, and disaster assistance, through electronic devices; and
- Flexible Spending and Dependent Care Funded Prepaid Access - Reimbursement of funds for defined, qualifying expenses related to pre-tax flexible spending accounts for healthcare and dependent care expenses or Health Reimbursement Arrangements (as defined in 26 U.S.C. §§105(b) and 125) for health care expenses.

Exclusions have nuances that need to be carefully reviewed before relying on them.

1283. Does the $2,000 threshold for closed-loop products apply to a single device or per individual?

The $2,000 threshold is applied to the device or vehicle and does not require aggregation of all purchases of distinct closed-loop prepaid access devices bought by an individual in a single day. However, as discussed further below, an entity that sells more than $10,000 in almost any combination of prepaid access is subject to the portion of the Prepaid Access rule applicable to “sellers of prepaid access.”

1284. Must a prepaid access product display its maximum value on the product itself?

No. The final rule did not include the requirement that the maximum value of a prepaid access product be clearly visible on the product itself.

1285. Why is the "provider" assigned the primary responsibility for ensuring a prepaid access program is in compliance with AML laws and regulations?

The final rule centralizes the primary regulatory obligations with the provider of a prepaid access program since it is often the party with the greatest access and/or ability to gain access to relevant information to comply with BSA reporting requirements. The provider is generally the participant with principal oversight and control over one or more prepaid programs.

FinCEN believes the provider is the entity in the best position to file CTRs and SARs, maintain or have access to transaction records, and establish and maintain AML programs because it is likely to have business relationships with most or all of the other participants in the transaction chain.

1286. How is the "provider" of a prepaid access program determined?

The final rule provides two methods for determining the provider of a prepaid access program:

- **Agreement Approach** – A contractual determination among the participants in a prepaid access program as to who would serve as the provider. The determination is communicated to FinCEN when the provider registers as a money services business utilizing the Registration of Money Services Businesses (RMSB) form.
- **Provider Criteria** – In the event participants in a prepaid access program fail to come to an agreement or the provider has failed to register, the following five factors, each of which is not dispositive on its own, will be used by FinCEN to determine a provider of a prepaid access program:
    - Organizer of the prepaid program (e.g., initiated or established the program);
    - Sets the terms and conditions and determines that the terms have not been exceeded;
    - Determines the other businesses that will participate in the prepaid program, which may include the issuing bank, the payment processor or the distributor;
    - Controls or directs the appropriate party to initiate, freeze or terminate prepaid access;
    - Engages in activity that demonstrates control and oversight of transactions.

1287. Are there exemptions to the definition of a "provider" of prepaid access?

Yes. Banks and financial institutions regulated by the SEC and the CFTC are exempted from the definition of "provider" by the final rule. While not subject to prepaid access regulations, financial institutions that offer prepaid access products should take risk management steps to reduce the AML risks of these products and third-party payment processors (TPPP) who offer these products. For further guidance, please refer to the Prepaid Access, Stored-Value and E-Cash and Third-Party Payment Processor sections.

1288. Why are sellers of prepaid access subject to prepaid access regulations?

FinCEN has determined that because sellers of prepaid access generally have face-to-face contact with consumers at the point-of-sale, they are in one of the best positions to collect customer identifying information and detect potentially suspicious activity.

1289. Are any persons that accept payments for an initial or subsequent loading of prepaid access not considered "sellers" for the purpose of regulatory requirements for prepaid access?

Yes. Persons that accept payments for an initial or subsequent loading of prepaid access are not considered "sellers" if they:

- Do not sell prepaid access under a prepaid program that can be used before the purchaser's identification can be obtained and verified; and
- Have implemented policies and procedures to reasonably prevent the sale of prepaid access (including closed-loop prepaid access) to funds that exceed $10,000 to any person during any one day.

1290. How does the prepaid access final rule amend the regulatory requirements for MSBs?

In addition to updating the definition of "stored value" to "prepaid access," MSBs that qualify as providers or "sellers of prepaid access" are now required to file suspicious activity reports, register with FinCEN and take a number of other actions. Remaining regulations for MSBs remain unaffected by the Prepaid Access rule. For further guidance on the AML requirements of MSBs, please refer to the Money Service Businesses section.

1291. Are additional regulations expected for prepaid access?

Yes. The Consumer Financial Protection Bureau (CFPB) held a hearing in May 2012 regarding prepaid access, with a focus on general purpose reloadable (GPR) cards. The CFPB is expected to issue additional regulations that may include the following:

- A definition for GPR cards;
- What current consumer protections apply to GPR cards under Regulation E;
- What disclosures will be required regarding fees;
- How to enable consumers to effectively compare various GPR cards;
- Whether consumers should be notified of the existence or lack thereof of FDIC pass-through insurance;
- Costs, benefits and consumer protection issues related to any credit or savings features of GPR cards;
- Efficacy of credit reporting features on GPR cards in enabling consumers to improve or build credit; and
- Regulatory compliance.

1292. What guidance has been issued on prepaid access?

The following are examples of information and guidance that have been issued on prepaid access:

- **"Prepaid Cards/Stored-Value Cards" subsection within Electronic Cash – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **"E-Banking" and "Emerging Retail Payment Technologies" within the "Retail Payment Systems" sections within the FFIEC Information Technology Examination Handbook** by the FFIEC
- **Report on Money Laundering Using New Payment Methods** (2012) by the Financial Action Task Force (FATF)
- **Payroll Cards: An Innovative Product for Reaching the Unbanked and Underbanked** (2005) by the Office of the Comptroller of Currency (OCC)
- **The 2008 Survey of Consumer Payment Choice** by the Federal Reserve Bank of Boston
- **Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems** (2012) by FATF
- **Consumer Payment Choice: A Central Bank Perspective** by the Consumer Payments Research Center at the Federal Reserve Bank of Boston
- **Prepaid Cards: Vulnerable to Money Laundering?** (2007) by the Federal Reserve Bank of Philadelphia
- **The Laws, Regulations, Guidelines, and Industry Practices That Protect Consumers Who Use Gift Cards** (2008) by the Federal Reserve Bank of Philadelphia
- **Emerging Risk Forum "Cash, Check, or Cell Phone?" Protecting Consumers in a Mobile Finance World** (2010) by the Federal Reserve Bank of Boston
- **New Technologies, New Risks? Innovation and Countering the Financing of Terrorism** (2010) by the World Bank (WB)
- **Survey of Developments in Electronic Money and Internet and Mobile Payments** (2004) by the Bank of International Settlements (BIS)
- **Recommended Practices for Anti-Money Laundering Compliance for U.S.-Based Prepaid Card Programs** (2008) by the Network Branded Prepaid Card Association (NBPCA)

- **Person-to-Person Electronic Funds Transfers: Recent Developments and Policy Issues** (2010) by the Federal Reserve Bank of Boston
- **Understanding Risk Management in Emerging Retail Payments** (2008) by the Federal Reserve Bank of New York

Additional organizations providing guidance on stored-value products include, but are not limited to, the following:

- Federal Reserve Bank of Boston Risk and Policy Analysis Unit
- Federal Reserve Bank of Boston Consumer Payments Research Center (CPRC)
- Federal Reserve Bank of Philadelphia Payment Cards Center
- Network Branded Prepaid Card Association (NBPCA)

Key AML and Sanction Requirements

1293. With which key AML and sanction requirements are "providers of prepaid access" required to comply?

Prepaid access providers must comply with the following key AML and sanction requirements:

- Establishment of an AML program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program and conducts an independent review of the AML program. The AML program must be sufficiently detailed with standards and criteria specified for how the information is to be accessed, collected, verified and retained, and must have provisions addressing communication to employees and for the training of any individuals or entities acting as their agent.
- Retaining access to customer information that was collected, which must, at a minimum include:
    - Name
    - Date of birth
    - Address
    - Identification number
    - Additionally, a provider must establish and maintain procedures to verify the identity of a person who obtains prepaid access under a prepaid program (similar in scope to CIP verification procedures).
- Retaining transaction records generated in the ordinary course of business that would be needed to reconstruct prepaid access activation, loads, reloads, purchases, withdrawals, transfers, or other prepaid-related transactions. Such information must be retained for a period of five years after the last use of the prepaid access. Such information may include, but is not limited to:
    - Type of transaction (ATM withdrawals, POS purchase, etc.)
    - Amount and location of transaction
    - Date and time of transaction
    - Any other unique identifiers related to transactions
- Filing of CTRs
- Filing of SARs
- Filing of Reports of Foreign Bank and Financial Accounts (FBAR)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIR)
- Information-sharing (i.e., Section 314(a), in some cases, mandatory; Section 314(b), optional)
- Registration with FinCEN as a Provider of Prepaid Access
- OFAC and other sanction program requirements

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections.

1294. With which key AML requirements are sellers of prepaid access required to comply?

Sellers of prepaid access are required to comply with the same AML requirements as providers, except registration with FinCEN. Among other things, "sellers of prepaid access" have an obligation to collect and retain customer information on the purchaser. FinCEN indicated there are two situations under which a seller of prepaid access must collect customer information. Sellers that sell prepaid access that allows access to funds under a "prepaid access program" without the verification of customer information are responsible for collecting customer information, or sellers that sell any type of prepaid access in a combined amount greater than $10,000 in a day to a person or an entity (excluding the bulk sale exception noted above) must also obtain customer information.

1295. Are providers and sellers of prepaid access required to register with FinCEN as required for money services businesses?

Providers of prepaid access are required to register with FinCEN. Sellers of prepaid access are not required to register with FinCEN.

1296. What information must a provider of prepaid access provide when registering with FinCEN?

In addition to a complete and accurate Registration for Money Services Businesses (RMSB) form, a prepaid access provider is, among other things, required to provide a complete list of the prepaid programs for which it serves as a provider. For further guidance on RMSBs, please refer to the Registration section within the Money Services Businesses section.

1297. Do providers and sellers of prepaid access have CIP obligations?

Providers and sellers of prepaid access are not subject to the CIP requirement (unless they are otherwise required to do so under the Bank Secrecy Act (BSA)); however they are subject to their own customer information recordkeeping requirement that mirrors the CIP requirement. As described above, entities that qualify as "providers of prepaid access" or "sellers of prepaid access" must obtain, verify and retain the following information on the customer involved in the initial purchase of the prepaid product:

- Name
- Date of birth
- Address
- Identification number

There may be situations in which both are responsible for collecting customer information. In these instances, providers and sellers must agree as to who will collect the information (although the provider will remain liable in any event). Where an entity qualifies as a "seller of prepaid access" for selling more than $10,000 in prepaid access in a day to a person or an entity, there may be situations under which only the seller, but not the provider, is obligated to collect the customer information. For further guidance on CIP, please refer to Section 326 – Verification of Identification.

1298. What other records must be retained by providers of prepaid access?

The BSA requires the retention of all BSA reports (e.g., SAR-MSBs, CTRs, FBARs, CMIRs). Additionally, "providers of prepaid access" must retain transactional records generated in the ordinary course of business that would be necessary to reconstruct prepaid access activation, loads, reloads, purchases, withdrawals, transfers or other prepaid related transactions.

The BSA outlines additional requirements for other types of financial institutions (e.g., depository institutions, broker-dealers, casinos) as well. For further guidance, please refer to the Recordkeeping Requirements and Non-Bank Financial Institutions sections.

1299. How long are providers and sellers of prepaid access required to retain records?

Both providers and sellers of prepaid access are required to retain records for five years. Providers of prepaid access must retain access to records for five years after the last use of the prepaid access. Sellers must retain access to records for five years from the date of the sale of the prepaid access.

1300. Are providers and sellers of prepaid access required to file CTRs?

Yes, providers and sellers of prepaid access are required to file CTRs. For a listing of financial institutions required to file CTRs at the time of this publication, please refer to the Currency Transaction Reports section.

1301. Can providers and sellers of prepaid access grant CTR exemptions?

No. Only depository institutions (banks, savings associations, thrift institutions or credit unions) can grant exemptions, and then only for their U.S. customers.

1302. Is the SAR filed by providers and sellers of prepaid access unique?

Beginning March 29, 2012, FinCEN replaced industry specific SARs with a single form which must be submitted electronically. However, FinCEN will continue to accept legacy versions of the new SAR via electronic means until March 31, 2013. If a prepaid access provider or seller decides to continue to submit legacy reports, they are required to file the Suspicious Activity Report by Money Services Businesses (SAR-MSB) for suspicious transactions of $2,000 (or aggregating to $2,000) or more. For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

1303. What types of activities require a SAR to be filed for prepaid access providers?

Prepaid access providers should file a SAR upon detection of the following activities:

- Any transactions conducted or attempted by, at, or through a “provider” or “seller of prepaid access” involving or aggregating funds or other assets of at least $2,000 when the “provider” or “seller of prepaid access” knows, suspects or has reason to suspect that:
    - The transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, but not limited to, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or avoid any transaction reporting requirement under Federal law; or is designed to evade any BSA regulations.
    - The transaction is designed, whether through structuring or other means, to evade any regulations promulgated under the BSA.
    - The transaction has no business or apparent lawful purpose and the “provider” or “seller of prepaid access” knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.
    - The transaction involves the use of the “provider” or “seller of prepaid access” to facilitate criminal activity.

There are other SAR reporting requirements additionally applicable to issuers of money orders or traveler’s checks in connection with their review of clearance records that involves or aggregates funds or other assets of at least $5,000. For red flags that assist in identifying suspicious activity as outlined above, please refer to the Suspicious Activity Red Flags section.

1304. Are persons transporting or shipping prepaid access products across the U.S. border in an aggregate amount of more than $10,000 required to file a Report of International Transportation of Currency or Monetary Instrument (CMIR)?

Currently, the CMIR is required to be filed by:

- Each person who physically transports, mails or ships, or causes to be physically transported, mailed or shipped, currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time from the United States to any place outside of the United States or into the United States from any place outside of the United States; and

- Each person who receives U.S. currency or other monetary instrument(s) in an aggregate amount exceeding $10,000 at one time, which has been transported, mailed or shipped from any place outside of the United States.

In October of 2011, FinCEN proposed amending the definition of "monetary instruments" to include tangible prepaid access devices that would be subject to reporting on CMIRs; however, no final rule on this proposed change has yet been issued. The term "tangible prepaid access device" has been defined in the proposed regulations as the following:

- Any physical item that can be transported, mailed, or shipped into or out of the United States and the use of which is dedicated to obtaining access to prepaid funds or the value of funds by the possessor in any manner without regard to whom the prepaid access is issued.

This definition would include devices such as general-use prepaid cards, gift cards, store cards, payroll cards, government benefit cards, and any tangible device to the extent that they can provide access to prepaid funds or the value of funds by being readable by a device employed for the purpose by merchants (e.g., cell phones, key fobs, etc.). The definition does not extend to credit and debit cards.

It is important to note that if a prepaid access provider transports or ships covered monetary instruments exceeding $10,000, it is required to file a CMIR on these activities.

For further guidance, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

1305. Are providers and sellers of prepaid access required to comply with OFAC and other sanction regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. In addition, under limited circumstances, OFAC applies to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

1306. Do providers and sellers of prepaid access have additional obligations as they relate to their agents?

The AML program of "providers" and "sellers of prepaid access" should address communication and training of any individuals or entities acting as their agents. For further guidance, please refer to the Agents section within Money Services Businesses.

1307. Who is responsible for examining providers and sellers of prepaid access for compliance with AML laws and regulations?

The responsibility for examining providers and sellers of prepaid access is delegated to the IRS by FinCEN, unless the provider or seller is a bank or financial institution regulated by the SEC or CFTC. Many states also examine providers and sellers of prepaid access and their agents for compliance with AML and other regulations if they come within the scope of licensure within the state.

Broker-Dealers

Definition

1308. Which types of broker-dealers are required to comply with AML requirements?

Virtually all broker-dealers registered or required to be registered with the SEC under the Securities Exchange Act of 1934 are required to comply with AML requirements.

1309. Who is responsible for examining broker-dealers for compliance with AML laws and regulations?

The SEC and FINRA (formerly the NASD) are responsible for examining broker-dealers for compliance with AML requirements. In addition, examinations may be conducted by the broker-dealer's SRO. The responsible SRO is based upon where the broker-dealer is registered and/or listed (e.g., NYSE, Municipal Securities Rule Board [MSRB]).

1310. What is an SRO?

An SRO is a nongovernment organization that has the power to create and enforce industry regulations and standards. Examples include, but are not limited to, the following: NASDAQ, NYSE and Amex.

1311. Have the SEC, FINRA, or SROs issued supplemental rules or guidance for broker-dealers?

Yes. Prior to FINRA's formation, the NASD and the NYSE maintained two separate "rule books" for governing broker-dealers. When the NASD became FINRA, the two rule books were consolidated to develop uniformity and consistency between the two organizations. As of January 1, 2010, FINRA Consolidated Rule 3310 replaced NASD Rule 3311 as the rule governing AML requirements.

1312. Does the Consolidated Rule 3310 have any significant changes to the AML requirements for broker-dealers?

No. The Consolidated Rule 3310 did not make any significant changes to the existing AML requirements for broker-dealers.

1313. How is the term "account" defined for a broker-dealer?

The term "account" denotes a formal relationship with a broker-dealer established to effect transactions in securities, including, but not limited to, the purchase or sale of securities, securities loaned and borrowed activity, and the holding of securities or other assets for safekeeping or as collateral. For additional guidance on the types of accounts and customers subject to the CIP requirement, please refer to Section 326 – Verification of Identification.

It does not include an account the broker-dealer acquires through an acquisition, merger or purchase of assets or assumption of liabilities, or that is opened to participate in an employee benefit plan established under the Employee Retirement Income Security Act (ERISA).

1314. Who "owns" the account/customer when both introducing and clearing brokers are involved?

Both the introducing broker and clearing broker "own" the account and therefore are obligated to comply with applicable AML requirements (e.g., performing CIP, monitoring and reporting suspicious activity). However, under certain circumstances, introducing and clearing brokers are able to rely on each other for parts of their CIP programs. For example, an introducing broker would be in a better position to conduct CIP since it established the relationship with the customer. The clearing broker would likely be in a better position to monitor for suspicious activity since it processes the transactions and has visibility into the customer's transaction activity.

1315. What are the risks of the relationships between introducing brokers and clearing brokers?

Both the introducing broker and clearing broker face third-party risk in which the other financial institution relied upon to support the AML Compliance Program (e.g., CIP, sanctions screening, monitoring for potentially suspicious activity) may not adequately execute its AML responsibilities consistent with regulatory and/or internal standards. For further guidance on third-party risk, please refer to the Know Your Third Parties section.

1316. How is the term "correspondent account" defined for a broker-dealer?

The term "correspondent account" is defined as "any formal relationship established for a foreign financial institution to provide regular services to effect transactions in securities." According to the Treasury Department, correspondent accounts for broker-dealers include:

- Accounts to purchase, sell or lend securities (e.g., securities repurchase agreements)

- Prime brokerage accounts
- Accounts trading foreign currency
- Over-the-counter derivatives contracts
- Custody accounts holding settled securities as collateral

For further guidance on correspondent banking, please refer to the Correspondent Banking and Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts sections.

1317. How is the term "private banking account" defined for broker-dealers?

The term "private banking account" is defined as an account that: (a) requires a minimum deposit of assets of at least $1 million; (b) is established or maintained on behalf of one or more non-U.S. persons who are direct or beneficial owners of the account; and (c) has an employee assigned to the account who is a liaison between the broker-dealer and the non-U.S. person. For additional guidance on private banking and related EDD requirements, please refer to the Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts section.

Key AML and Sanction Requirements

1318. With which key AML and sanction requirements are broker-dealers required to comply?

Broker-dealers must comply with the following key AML requirements:

- Establishment of an AML program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program and conducts an independent review of the AML program
- Establishment of a Customer Identification Program (CIP)
- Filing of Suspicious Activity Reports (SAR)
- Filing of Currency Transaction Reports (CTR)
- Filing of Reports of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300) (only where not required to file a CTR)
- Filing of Reports of Foreign Bank and Financial Accounts (FBAR)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIR)
- Recordkeeping and retention (e.g., Funds Transfer Rule, Travel Rule, Purchase and Sale of Monetary Instruments)
- Information sharing (Section 314(a) (mandatory), Section 314(b) (optional))
- Complying with Special Measures (Section 311)
- Obtaining Foreign Bank Certifications (Section 319(b))
- Establishing an enhanced due diligence (EDD) program for foreign correspondent account relationships, private banking relationships and politically exposed persons (PEPs)
- OFAC and other sanction requirements

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to broker-dealers is provided below.

1319. Are there special requirements for the AML compliance officer of a broker-dealer?

Neither the USA PATRIOT Act nor FINRA Rule 3310 (formerly NASD rule 3311) requires AML compliance officers to register either as representatives or as principals. However, FINRA's general registration requirements state that persons who engage in the supervision, solicitation or conduct of investment banking or securities business for member firms need to register. Thus, being the AML compliance officer of a member firm would not necessarily trigger registration requirements, but instructing registered persons on a particular securities product could.

Generally, the individual responsible for overseeing the entire AML program should be an officer of the broker-dealer.

Broker-dealers, are, however, not only required to designate an AML compliance officer, but also to provide the following information to FINRA through the FINRA Contact System (FCS):

- Name
- Title
- Mailing address
- E-mail address
- Telephone number
- Facsimile number

1320. Is someone with trading authority over an account considered a "customer" under the CIP requirement?

A person with trading authority prior to the effective date of the CIP regulation is not a "customer." However, any person granted trading authority after the effective date of the CIP regulation is a customer and is subject to the requirements of CIP.

1321. How does the SEC's Books and Records Customer Account Records Rule compare to the CIP requirement?

The SEC's Books and Records Customer Account Records Rule (BRCA Rule), also known as the suitability rule, differs in purpose, requirements and timing from the CIP requirement. The purpose of the BRCA Rule is to assess the suitability of potential clients, not to verify their identities. The BRCA Rule requires the following information in addition to that required for CIP:

- Telephone number
- Employment status (including occupation and whether the customer is an associated person of a broker-dealer)
- Annual income
- Net worth (excluding value of primary residence)
- Investment objectives
- Signatures and/or approvals by appropriate personnel (dated in some instances)

Unlike the CIP requirement, the BRCA Rule does not prohibit broker-dealers from opening an account if the required information is not obtained. Information can be obtained during the account opening process. Record retention rules also differ. Information must be retained for six years after the closing of the account or after the date the information was replaced or updated, whichever is earlier, as opposed to five years under the CIP requirement.

1322. Are there types of customers or accounts that may present regulatory challenges for broker-dealers?

Yes. Regulatory challenges may arise with the following customer and account types:

- **Correspondent accounts** – Treasury has defined "correspondent accounts" for broker-dealers to include:
    - Accounts to purchase, sell, lend or otherwise hold securities, including securities repurchase agreements;
    - Prime brokerage accounts that clear and settle securities transactions for clients;
    - Accounts for trading foreign currency;
    - Custody accounts for holding securities or other assets in connection with securities transactions as collateral; and
    - Over-the-counter derivatives contracts.
- **Master/Sub-accounts** – Master/Sub-accounts are an account trading model in which a master account is established for a client that permits subordinate accounts ("sub-account") for different trading activities. The

master account is typically established for a legal entity while sub-accounts are established for use by individual traders associated with the legal entity.

- **Omnibus accounts** – Omnibus accounts are established by financial intermediaries for the purpose of executing transactions that will clear or settle at another financial institution.

Challenges arise in identifying and verifying the beneficial owner of accounts and/or underlying assets within accounts maintained for these types of customers by broker-dealers. For further guidance on correspondent accounts, please refer to the Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts and Correspondent Banking sections. For further guidance on customer due diligence, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence and Beneficial Ownerships sections.

1323. Are broker-dealers required to file CTRs?

Yes, Broker-dealers are required to file CTRs. For a listing of financial institutions required to file CTRs at the time of this publication, please refer to the Currency Transaction Reports section.

1324. Can broker-dealers grant CTR exemptions?

No. Only depository institutions (banks, savings associations, thrift institutions or credit unions) can grant exemptions.

1325. Is the SAR filed by broker-dealers unique?

Beginning March 29, 2012, FinCEN replaced industry-specific SAR forms with a single form that must be submitted electronically. However, FinCEN will continue to accept legacy versions of the new SAR via electronic means until March 31, 2013. If a broker-dealer decides to continue to submit legacy reports, it is required to file the Suspicious Activity Report by the Securities and Futures Industries (SAR-SF) for suspicious transactions of $5,000 (or that aggregate to $5,000) or more, but may voluntarily file on suspicious transactions that are less than $5,000.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

1326. What types of activities require a SAR to be filed for broker-dealers?

Upon the detection of the following activities, broker-dealers should file a SAR:

- **Transactions aggregating to $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act (BSA)** – Any transaction(s) totaling or aggregating to at least $5,000 conducted by a suspect through the broker-dealer, where the broker-dealer knows, suspects or has reason to suspect that the transaction: involved illicit funds or is intended or conducted to hide or disguise funds or assets derived from illegal activities (including, but not limited to, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any law or regulation or avoid any transaction reporting requirement under federal law; or is designed to evade any BSA regulations.
- **Evasion** – A SAR should be filed in any instance where the broker-dealer detects that the transaction was designed, whether through structuring or other means, to evade any BSA regulations.
- **No business or apparent lawful purpose** – The transaction has no business or apparent lawful purpose and there is no known reasonable explanation for the transaction after examination of available facts, including the background and possible purpose of the transaction.
- **Facilitation of criminal activity** – The transaction involves the use of the broker-dealer to facilitate criminal activity.

For red flags to assist in identifying suspicious activity as outlined above, please refer to the Suspicious Activity Red Flags section.

1327. Are there exceptions to the suspicious activity reporting requirement for broker-dealers?

Yes. The suspicious activity reporting requirement for broker-dealers contains three exceptions from reporting violations that otherwise would be reported to various law enforcement authorities. The following activities are not required to be reported:

- A robbery or burglary that is reported by the broker-dealer to appropriate law enforcement authorities
- Lost, missing, counterfeit or stolen securities that are reported by the broker-dealer pursuant to Rule 17f-1 under the reporting requirements of 17 CFR 240.17f-1

- A violation of the federal securities laws or rules of a self-regulatory organization (SRO) by the broker-dealer, its officers, directors, employees or registered representatives, that is reported appropriately to the SEC or an SRO, except for a violation of Rule 17a-8 under 17 CFR 240.17a-8 or 17 CFR 405.4, if the violation is appropriately reported to the SEC, or an SRO, which must be reported on a SAR.

1328. Who is responsible for reporting suspicious activity on a customer that is shared between introducing and clearing firms?

Introducing firms are often in a better position to "know the customer," and therefore, to identify potentially suspicious activity at the account opening stage, including verification of the identity of the customer and deciding whether to open an account for a customer. Clearing firms, in turn, may be in a better position to monitor customer transaction activity including, but not limited to, trading, wire transfers and the deposit and withdrawal into and out of accounts of different financial institutions. The obligation to file a SAR rests with each broker-dealer involved in the transaction, but only one SAR filing is required per transaction.

For additional guidance on third-party reliance, please refer to the Third-Party Reliance section.

1329. Are there any exceptions to the independent testing requirement of the AML program for broker-dealers?

No. Previously, under FINRA Rule 3310 (formerly NASD rule 3011), broker-dealers that did not execute transactions for customers or otherwise hold customer accounts or act as an introducing broker with respect to customer accounts (e.g., engage solely in proprietary trading or conduct business only with other broker-dealers) were only obligated to independently test their AML program every two years. This exception was eliminated effective January 1, 2010.

1330. Are broker-dealers allowed to provide services to a foreign shell bank through a correspondent account?

No. Broker-dealers are prohibited from providing any service to a foreign shell bank. In addition, they must ensure they are not providing services to a shell bank through a correspondent relationship by requesting a Foreign Bank Certification from their respondents. For additional guidance on Foreign Bank Certifications, please refer to the Foreign Bank Certifications section.

1331. What are the key recordkeeping requirements of the BSA for broker-dealers?

The BSA requires the retention of all BSA reports (e.g., SARs, CTRs, FBARs, CMIRs). Additionally, other required documentation must be retained by broker-dealers, such as the following:

- When required, a taxpayer identification number (TIN) (or passport number or description of a government issued identification for nonresident aliens) of each person for whom a deposit or share account is opened and for each person who has a financial interest in the account
- List of names, addresses and account or credit line numbers of those persons from whom the broker-dealer was unable to obtain the above information
- Each document granting signature or trading authority over each customer's account
- Each record described in 240.17a-3(a) (1), (2), (3), (5), (6), (7), (8) and (9) of Title 17, Code of Federal Regulations
- A record of each remittance or transfer of funds or of currency, checks, other monetary instruments, investment securities or credit of more than $10,000 to a person, account or place outside of the United States
- A record of each receipt of currency, other monetary instruments, checks or investment securities and of each transfer of funds or credit of more than $10,000 received on any one occasion directly and not through a domestic financial institution, from any person, account or place outside of the United States

The above applies to broker-dealers. The BSA outlines additional requirements for other types of financial institutions (e.g., depository institutions, currency dealers or exchangers, casinos) as well. For further guidance, please refer to the Recordkeeping Requirements, Money Services Businesses and Casinos or Card Clubs sections.

1332. Are broker-dealers required to comply with OFAC and sanction regulations?

Yes. OFAC and other sanction requirements apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. In addition, under limited circumstances, OFAC sanction requirements apply to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

1333. What key AML guidance has been issued on broker-dealers?

The following key AML guidance and resources has been issued on broker-dealers:

- **Anti-Money Laundering (AML) Source Tool for Broker-Dealers** (2012) by the Securities and Exchange Commission (SEC)
- **Anti-Money Laundering Template for Small Firms** (2010) by Financial Industry Regulatory Authority (FINRA)
- **AML E-Learning Courses** (2012) by FINRA
- **Money Laundering and Terrorist Financing in the Securities Sector** (2009) by Financial Action Task Force (FATF)
- **Wolfsberg Frequently Asked Questions on Selected Anti-Money Laundering Issues in the Context of Investment and Commercial Banking** (2006) by the Wolfsberg Group
- **Principles on Client Identification and Beneficial Ownership for the Securities Industry** (2004) by International Organization of Securities Commissions (IOSCO)
- **Guidance on Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities** (2006) by FinCEN
- **Question and Answer Regarding the Broker-Dealer Customer Identification Program Rule** (2003) by Securities and Exchange Commission (SEC)
- **Frequently Asked Questions – Customer Identification Program Responsibilities under the Agency Lending Disclosure Initiative** (2006) by FinCEN
- **Customer Identification Program Rule No-Action Position Respecting Broker-Dealers Operating Under Fully Disclosed Clearing Agreements According to Certain Functional Allocations** (2008) by FinCEN
- **Bank Secrecy Act Obligations of a U.S. Clearing Broker-Dealer Establishing a Fully Disclosed Clearing Relationship with a Foreign Financial Institution** (2008) by FinCEN
- **Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries** (2006) by FinCEN

Futures Commission Merchants and Introducing Brokers

Definition

1334. What is a futures commission merchant (FCM)?

An FCM is a person or entity registered, or required to register, as an FCM with the Commodity Futures Trading Commission (CFTC) under the Commodity Exchange Act (CEA), except a person who registers pursuant to 4(f)(a)(2) of the CEA. FCMs conduct transactions in the futures market in a manner similar to that of brokers in the securities market.

1335. What is an introducing broker (IB) in the context of FCMs?

An IB is any person or entity that is registered, or required to be registered, with the CFTC as an IB under the CEA, except a person who registers pursuant to 4(f)(a)(2) of the CEA.

Key AML and Sanction Requirements

1336. With which key AML and Sanction requirements are FCMs and IBs required to comply?

FCMs and IBs must comply with the following key AML requirements:

- Establishment of an AML program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, and conducts an independent review of the AML program
- Establishment of a Customer Identification Program (CIP)
- Filing of Suspicious Activity Reports (SARs)
- Filing of Currency Transaction Reports (CTRs)
- Filing of Reports of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300) (where not subject to CTR filings)
- Filing of Reports of Foreign Bank and Financial Accounts (FBAR)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Recordkeeping and retention (e.g., Funds Transfer Rule, Travel Rule, Purchase and Sale of Monetary Instruments)
- Information-sharing (Section 314(a) (mandatory), Section 314(b) (optional))
- Complying with Special Measures (Section 311)
- Obtaining Foreign Bank Certifications (Section 319(b))
- Establishing an enhanced due diligence (EDD) program for correspondent account relationships, private banking relationships and politically exposed persons (PEPs) (Section 312)
- OFAC and other sanction requirements

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to FCMs and IBs is provided below.

1337. Are there special requirements for the AML compliance officer of FCMs and IBs?

The CFTC's general registration requirements state that persons who engage in the supervision, solicitation or conduct of futures business for member firms need to register. Being an AML compliance officer may not, in and of itself, trigger the need to register, but other responsibilities could.

Generally, the individual responsible for overseeing the entire AML program should be an officer of the futures firm.

FCMs and IBs are, however, not only required to designate an AML compliance officer, but also to provide the following information to FINRA through the FINRA Contact System (FCS):

- Name
- Title
- Mailing address
- E-mail address
- Telephone number
- Facsimile number

1338. Is the SAR filed by FCMs and IBs unique?

Beginning March 29, 2012, FinCEN replaced industry-specific SAR forms with a single form that must be submitted electronically. However, FinCEN will continue to accept legacy versions of the new SAR via electronic means until March 31, 2013. If an FCM or IB decides to continue to submit legacy reports, it should file the SAR-SF for suspicious transactions of $5,000 (or that aggregate to $5,000) or more.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

1339. What obligations do FCMs and IBs have with respect to SAR filings?

FCMs and IBs are obligated to file SARs in good faith and maintain the confidentiality of the SAR filing and any information that would reveal the existence of a SAR ("SAR information"). In other words, no FCM and IB, and no director, officer, employee or agent of the institution who files a SAR, may notify any person (or their agent, such as their attorney) involved in the transaction that it has been reported.

1340. Are there exceptions to the SAR disclosure prohibition?

Provided that no person involved in the transaction is notified that the transaction has been reported, the SAR disclosure prohibition does not include disclosures of SAR information to the following:

- FinCEN
- Any federal, state or local law enforcement agency
- Any federal regulatory agency that examines the depository institution for compliance with the BSA
- Any state regulatory authority that examines the depository institution for compliance with state laws requiring compliance with the BSA

Guidance has also been provided by FinCEN on a broker-dealer's ability to share SAR information within its organizational structure to fulfill its duties under the BSA. FCMs and IBs may share SAR information with the following:

- Head office or controlling companies, whether domestic or foreign
- Domestic affiliates and subsidiaries that are also subject to SAR requirements

For further guidance, please refer to the Suspicious Activity Reports and Confidentiality sections.

1341. How do FCMs and IBs submit CTRs and SARs to FinCEN?

Beginning July 1, 2012, FCMs and IBs must submit CTRs and SARs through the BSA E-Filing System, an Internet-based e-filing system developed by FinCEN to enable financial institutions to file CTR and SAR forms electronically. While the use of the BSA E-Filing System can be beneficial for all financial institutions, its use is generally more cost-effective for financial institutions with large volumes of CTR and SAR filings since it enables the batching of forms.

1342. Are FCMs and IBs required to comply with OFAC regulations?

Yes. OFAC and other sanction requirements apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. In addition, under limited circumstances, sanction requirements apply to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

1343. Who is responsible for examining FCMs and IBs for compliance with AML laws and regulations?

The CFTC is responsible for examining FCMs and IBs for compliance with AML laws and regulations. In addition, examinations may be conducted by the firm's SRO. The responsible SRO is based upon where the firm is registered and/or listed (e.g., NYSE, National Futures Association [NFA]).

Commodity Trading Advisers

Definition

1344. What is a commodity trading adviser (CTA)?

A CTA is a person who directs (i.e., is given decision-making authority over) account activities, client commodity futures and options accounts, and is registered or required to be registered as a CTA with the CFTC under the CEA. Generally, the CEA has defined a CTA as any person who is in the business of directly or indirectly advising others as to the value or advisability of trading futures contracts or commodity options for compensation or profit.

Key AML and Sanction Requirements

1345. With which key AML and sanction requirements are CTAs required to comply?

CTAs are required to comply with the following key AML requirements:

- Filing of Reports of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- OFAC and other sanction requirements

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to CTAs is provided below.

1346. Are CTAs required to establish an AML program?

No. At present, the AML program requirement of the USA PATRIOT Act does not apply to CTAs. In 2003, FinCEN issued a proposed rule which would have required CTAs to establish AML Programs. The proposed rule was withdrawn in 2008. In its withdrawal notice, FinCEN said the primary reason for withdrawing the regulation was "passage of time." FinCEN further indicated that it would continue to consider whether it should impose AML Program requirements on CTAs.

1347. Are CTAs subject to the CIP requirement?

No. Currently, CTAs are not subject to the Customer Identification Program (CIP) requirement. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

1348. Are CTAs required to file CTRs?

No. Currently, CTAs are not required to file Currency Transaction Reports (CTRs). CTAs are, however, required to file Form 8300 for cash payments over $10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

1349. Are CTAs required to file SARs?

While CTAs are not currently obligated to file Suspicious Activity Reports (SARs), FinCEN encourages the voluntary filing of a SAR for suspected money laundering and terrorist activity. There is a checkbox on Form 8300 for indicating that a transaction is potentially suspicious. For further guidance, please refer to the Form 8300 section.

1350. Are CTAs required to comply with the information-sharing requirement?

No. Only those institutions required to establish an AML program are obligated to comply with the information-sharing requirement (i.e., 314(a)). For further guidance on information sharing, please refer to Section 314 – Cooperative Efforts to Deter Money Laundering.

1351. Are CTAs required to comply with OFAC regulations?

Yes. OFAC and other sanction requirements apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. In addition, under limited circumstances, sanction requirements apply to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

1352. Who is responsible for examining CTAs for compliance with AML laws and regulations?

The CFTC is responsible for examining CTAs for compliance with AML laws and regulations. In addition, examinations may be conducted by the firm's SRO. The responsible SRO is based upon where the firm is registered and/or listed (e.g., NYSE, National Futures Association [NFA]).

Mutual Funds

Definition

1353. What is a mutual fund?

A mutual fund is an open-ended investment company that is registered or required to register with the Securities and Exchange Commission (SEC) under Section 5 of the Investment Company Act.

1354. What AML guidance has been issued related to mutual funds?

The following are examples of key guidance that has been issued related to or discussing mutual funds:

- **Nonbank Financial Institutions – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Anti-Money Laundering (AML) Source Tool for Mutual Funds** (2012) by the Securities and Exchange Commission (SEC)
- **Frequently Asked Questions: Suspicious Activity Reporting Requirements for Mutual Funds** (2006) by FinCEN
- **Sharing Suspicious Activity Reports by Securities Broker-Dealers, Mutual Funds, Futures Commission Merchants, and Introducing Brokers in Commodities with Certain U.S. Affiliates** (2010) by FinCEN
- **Assessing the Impact of Amendments to the Regulations Defining Mutual Funds as Financial Institutions** (2010) by FinCEN
- **Anti-Money Laundering Guidance for Mutual Funds and Other Pooled Investment Vehicles** (2012) by the Wolfsberg Group
- **Foreign Asset Control Regulations for the Securities Industry** (2004) by OFAC
- **Opening Securities and Futures Accounts from an OFAC Perspective** (2008) by OFAC
- **Risk Factors for OFAC Compliance in the Securities Industry** (2008) by OFAC

In addition, the website of the Investment Company Institute (www.ici.org), the national association of U.S. investment companies, includes viewpoints and comment letters on money laundering issues of interest to the mutual funds community.

Key AML and Sanction Requirements

1355. With which key AML laws and regulations are mutual funds required to comply?

Mutual funds must comply with the following key AML laws and regulations:

- Establishment of an AML program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, and conducts an independent review of the AML program
- Establishment of a Customer Identification Program (CIP)
- Filing of Reports of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300) (only where not required to file a CTR)
- Filing of Suspicious Activity Reports (SARs)
- Filing of Currency Transaction Reports (CTRs)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Recordkeeping and retention (e.g., Funds Transfer Rule, Travel Rule, Purchase and Sale of Monetary Instruments)
- Information-sharing (Section 314(a) (mandatory), Section 314(b) (optional))
- Screening for Special Measures (Section 311)
- Requiring Foreign Bank Certifications (Section 319(b))
- Establishment of an enhanced due diligence (EDD) program for customers deemed to be of higher risk, correspondent account relationships, private banking relationships and politically exposed persons (PEPs) (Section 312)
- OFAC and other sanction requirements

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to mutual funds is provided below.

1356. Are mutual funds required to file CTRs?

Yes, mutual funds are now required to file CTRs as a result of a final rule published by FinCEN in April 2010. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

1357. Can mutual funds grant CTR exemptions?

No. Only depository institutions (banks, savings associations, thrift institutions or credit unions) can grant exemptions. For further guidance on exemptions, please refer to the CTR Exemptions section.

1358. Is the SAR report filed by mutual fund companies unique?

Beginning on March 29, 2012, FinCEN replaced industry-specific SAR forms with a single form that must be submitted electronically. However, FinCEN will continue to accept legacy versions of the new SAR via electronic means until March 31, 2013. If a mutual fund decides to continue to submit legacy reports, it is required to file the SAR by SAR-SF on suspicious activity of $5,000 (or that aggregates to $5,000) or more, but may voluntarily file on suspicious transactions that are less than $5,000.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

1359. How do mutual funds submit CTRs and SARs to FinCEN?

Beginning July 1, 2012, mutual funds must submit CTRs and SARs through the BSA E-Filing System, an Internet-based e-filing system developed by FinCEN to enable financial institutions to file CTR and SAR forms electronically.

While the use of the BSA E-Filing System can be beneficial for all financial institutions, its use is generally more cost-effective for financial institutions with large volumes of CTR and SAR filings since it enables the batching of forms.

1360. Is it permissible for a broker-dealer, other financial institution or servicing provider that is involved in the same transaction(s) with one or more mutual funds to file a joint SAR on behalf of the mutual fund(s)?

Yes. One SAR is sufficient to report the same suspicious activity. Under the suspicious activity reporting requirement for mutual funds, joint SAR filings are permissible so long as the report contains all relevant facts, including the identification in the narrative section of all mutual funds on whose behalf the report is being filed.

It is still the responsibility of all firms involved to confirm that at least one SAR was filed on the suspicious activity, regardless of which firm actually filed the report.

1361. Does the joint filing of a SAR violate the confidentiality requirement of SAR filings?

No. The suspicious activity reporting requirement specifically permits a mutual fund to share information pertaining to a suspicious transaction with any other mutual fund or financial institution involved in the transaction provided that such mutual fund or financial institution is not expected to be the subject of the report.

1362. Is a mutual fund permitted to inform an investment adviser who is in control of the fund about a SAR filing?

Yes. A mutual fund may inform the investment adviser who controls the fund, whether domestic or foreign, about a SAR filing. Additionally, the SAR can be shared with the parent company/companies of the investment adviser.

In all exchanges of sensitive information, particularly when SARs are involved, mutual funds should ensure that the proper policies, procedures and controls are in place to protect the confidentiality of the exchanged information.

1363. Are mutual funds required to comply with OFAC and other sanction regulations?

Yes. OFAC requirements apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S.-incorporated entities and their foreign branches. In addition, under limited circumstances, OFAC applies to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

1364. Who is responsible for examining mutual funds for compliance with AML laws and regulations?

The U.S. Department of the Treasury has designated the SEC as responsible for examining mutual funds for compliance with AML laws and regulations.

Insurance Companies

Definition

1365. Which types of insurance companies are required to comply with AML laws and regulations?

An insurance company or insurer that is engaged within the United States as a business in the issuing or underwriting of a covered product is required to comply with AML laws and regulations.

1366. How is the term “covered product” defined?

Covered products are defined as:

- Permanent life insurance policies, other than group life insurance policies

- Annuity contracts, other than group annuity contracts
- Any other insurance products that have cash value or investment features

1367. Are there any exemptions from the definition of insurance companies that are not subject to AML laws and regulations?

The definition of insurance company currently excludes group insurance products, term (including credit), life, title, health, and many property and casualty insurers. It also excludes products offered by charitable organizations (e.g., charitable annuities), as well as reinsurance and retrocession contracts. It also excludes entities that offer annuities or other covered products as an incidental part of their business.

1368. What guidance has been issued related to insurance companies and covered products?

The following are examples of key guidance that has been issued related to insurance companies:

- **Insurance – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Frequently Asked Questions: Customer Identification Programs and Banks Serving as Insurance Agents** (2006) by FinCEN
- **Insurance Industry Suspicious Activity Reporting: An Assessment of Suspicious Activity Report Filings** (2010) by the Financial Crimes Enforcement Network (FinCEN)
- **Frequently Asked Questions from the Insurance Industry** (2012) by the Office of Foreign Assets Control (OFAC)
- **Risk-Based Approach for the Life Insurance Sector** (2009) by the Financial Action Task Force (FATF)
- **Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism** (2004) by the International Association of Insurance Supervisors (IAIS)
- **Anti-Money Laundering Guidance Notes** (2003) by the IAIS

Key AML and Sanction Requirements

1369. With which key AML and sanction requirements are insurance companies required to comply?

Insurance companies must comply with the following key AML requirements:

- Establishment of an AML program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program and conducts an independent review of the AML program
- Filing of Reports of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300)
- Filing of Suspicious Activity Reports (SARs)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Information-sharing (Section 314(a) (mandatory), Section 314(b) (optional))
- OFAC and other sanction requirements

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to insurance companies is provided below.

1370. Are insurance agents and brokers subject to AML laws and regulations?

While insurance agents and brokers are not subject to separate AML laws and regulations, it is usually critical that agents and brokers be incorporated into the AML program of the insurance company, as they are most able to know the sources of investment assets, and the nature of the clients and their intentions for purchasing products.

1371. Are insurance companies subject to the CIP requirement?

No. Currently, insurance companies are not subject to the Customer Identification Program (CIP) requirement. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

1372. Are insurance companies required to file CTRs?

No. Currently, insurance companies are not subject to filing Currency Transaction Reports (CTRs). Insurance companies are, however, required to file Form 8300 for cash payments over $10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300, please refer to the Currency Transaction Reports and Form 8300 sections.

1373. Is there a unique SAR report that insurance companies must use?

Beginning March 29, 2012, FinCEN replaced industry-specific SAR forms with a single form that must be submitted electronically. However, FinCEN will continue to accept legacy versions of the new SAR via electronic means until March 31, 2013. If an insurance company decides to continue to submit legacy reports, it is required to file the SAR-SF for suspicious transactions of $5,000 (or that aggregate to $5,000) or more, but may voluntarily file on suspicious transactions that are less than $5,000.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

1374. How do insurance companies submit BSA reports to FinCEN?

Beginning July 1, 2012, insurance companies must submit BSA reports through the BSA E-Filing System, an Internet-based e-filing system developed by FinCEN to enable financial institutions to file BSA reports electronically.

1375. Are there exceptions to the suspicious activity reporting requirements for insurance companies?

Yes. Insurance companies are only required to file SARs with respect to suspicious transactions involving covered products. They are not required to report submissions involving false or fraudulent information to obtain a policy or make a claim, unless the company believes the activity relates to money laundering or terrorist financing.

Insurance companies registered with the SEC as broker-dealers are subject to the SAR filing requirements of broker-dealers and, therefore, are not obligated to file under the insurance company requirements. As registered broker-dealers, insurance companies are subject to additional AML requirements beyond those of an insurance company.

1376. Are there red flags for detecting potentially suspicious activity for insurance companies?

Yes. A comprehensive list of red flags for detecting potentially suspicious activity relating to account opening, transaction execution and high-risk products/services/transactions (e.g., cash, wires, monetary instruments, insurance) has been provided in this publication. For further guidance on red flags, please refer to the Suspicious Activity Red Flags and Insurance Products Red Flags sections.

1377. Are insurance companies required to comply with OFAC and other sanction regulations?

Yes. OFAC and other sanction requirements imposed by the United States apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. In addition, under limited circumstances, OFAC applies to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

1378. Who is responsible for examining insurance companies for compliance with AML laws and regulations?

The Internal Revenue Service (IRS) is responsible for examining insurance companies for compliance with AML laws and regulations. As stated above, if the insurance company is registered as a broker-dealer, then the SEC and applicable SRO would be responsible for examining the insurance company for compliance with AML laws and regulations.

1379. How does FinCEN interact with state insurance regulators?

FinCEN has entered into individual memoranda of understanding (MOUs) with several state insurance regulators to enhance the level of cooperation in the fight against money laundering, fraud and other financial crimes. State insurance regulators have agreed to incorporate AML compliance reviews into their examinations of insurance companies. The MOUs also enable FinCEN and state insurance regulators to share supervisory and related information relevant to assessing risks and compliance with applicable AML laws and regulations.

Casinos or Card Clubs

Definition

1380. What is a casino?

A casino or gambling casino is a business licensed or authorized to do business as such in the United States, whether under the laws of a state or of a territory or insular possession of the United States, or under the Indian Gaming Regulatory Act or other federal, state or tribal law or arrangement affecting Indian lands. It includes casinos that operate on the assumption that no such authorization is required for operation on Indian lands. The term includes the principal headquarters and every domestic branch or place of business of the casino.

1381. What is a card club?

A card club is a gaming club, card room, gaming room or similar gaming establishment that is licensed or authorized to do business as such in the United States, whether under the laws of a state, territory or insular possession of the United States, or of a political subdivision of any of the foregoing, or under the Indian Gaming Regulatory Act or other federal, state or tribal law or arrangement affecting Indian lands. It includes establishments that operate on the assumption that no such authorization is required for operation on Indian lands for establishments of such type. The term includes the principal headquarters and every domestic branch or place of business of the establishment.

1382. Which types of casinos or card clubs are required to comply with AML laws and regulations?

Casinos or card clubs that have a gross annual gaming threshold in excess of $1 million are required to comply with AML laws and regulations.

1383. How should the $1 million gaming threshold be calculated?

All gaming activity must go into the calculation of gross annual gaming revenue, including activity that would not deem an establishment a casino on its own (e.g., pari-mutuel wagering, bingo).

1384. Which types of gaming activities may qualify an institution as a casino or card club subject to AML laws and regulations?

The following types of gaming activities may qualify an institution as a casino or card club subject to AML requirements:

- Racino
- Race book or sports pool operator
- Off-track betting
- Greyhound racing clubs that generate in excess of $1 million from poker tables
- Tribal gaming offering slot or table games

In some instances, qualification as a casino is dependent on whether an institution is licensed or authorized by state law.

1385. How is the term “racino” defined for casinos and card clubs?

The term “racino” has not yet been clearly defined for casinos and card clubs. Generally, the term “racino” refers to horse racetracks that may be authorized under state law to engage in or offer a variety of collateral gaming operations, including slot machines, video lottery terminals, video poker or card clubs.

1386. How is the term “greyhound racing club” defined for casinos and card clubs?

The term “greyhound racing club” is defined as a gaming establishment that offers the sport of racing greyhounds, in which trained dogs chase an artificial hare or rabbit around a track until they arrive at a finish line. Such clubs that offer table games that generate gross annual gaming revenue in excess of $1 million from poker tables are duly licensed or authorized by state or local government to do business as a gaming club or gaming room or similar establishment, and therefore, would be required to comply with AML requirements for casinos and card clubs.

1387. How is the term “business day” defined for casinos and card clubs?

For casinos, the term “business day” is the gaming day by which they keep their books and records for business, accounting and tax purposes.

1388. How is the term “customer” defined for casinos and card clubs?

The term “customer” is defined for casinos and card clubs as a person involved in a currency transaction with a casino, whether or not that person participates or intends to participate in the gaming activities offered by the casino or card club.

Key AML and Sanction Requirements

1389. With which key AML and sanction requirements are casinos and card clubs required to comply?

Casinos and card clubs must comply with the following key AML requirements:

- Establishment of an AML program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, and conducts an independent review of the AML program
- Filing of Currency Transaction Reports (CTRs)
- Filing of Reports of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300) (for nongaming activities, such as restaurants or shops)
- Filing of Suspicious Activity Reports (SARs)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Recordkeeping and retention (e.g., Funds Transfer Rule, Travel Rule, Purchase and Sale of Monetary Instruments)
- Information-sharing (Section 314(a) (mandatory), Section 314(b) (optional))
- OFAC and other sanction requirements

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to casinos and card clubs is provided below.

1390. Are casinos and card clubs subject to the CIP requirement?

No. Currently, casinos are not subject to the Customer Identification Program (CIP) requirement. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

1391. What due diligence should casinos and card clubs perform on “regular” customers?

Casinos and card clubs should apply risk-based due diligence procedures on “regular” customers, including junket representatives. For additional guidance on due diligence and enhanced due diligence (EDD) standards, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence section.

1392. What is a “junket representative”?

A “junket representative” is the organizer of a group of well-known players; a “junket” who travel together for the purpose of gambling.

1393. What due diligence is required for junket representatives?

Casinos and banks that establish accounts for junket representatives face similar customer due diligence challenges as correspondent, omnibus and trust accounts. Financial institutions must identify and, in some instances, verify the identity of all persons in the junket with a financial interest in the account for the purposes of complying with CIP, CTR and SAR reporting requirements.

1394. There are several types of CTRs (e.g., CTR, CTR-C). Which one should casinos and card clubs file?

Casinos and card clubs are required to file the new Currency Transaction Report (CTR). If a casino or card club decides to continue to submit legacy reports, they are required to file the Currency Transaction Report for Casinos (CTR-C). For additional guidance on CTRs, please refer to the Currency Transaction Reports section.

Casinos in Nevada with gross annual gaming revenues of $10 million or more and “table games statistical win” of $2 million or more are required to file a CTR-C form. The Nevada Gaming Commission Regulation 6A was repealed as of June 30, 2007, terminating the usage of FinCEN Form 103-N (CTR for Casinos/Nevada).

1395. Are there exceptions to the CTR filing requirement for certain transactions in casinos and card clubs?

Yes. The following transactions are exempt from the requirement to file CTRs:

- Currency transactions with domestic banks (generally, nonbank financial institutions [e.g., casino or card club] are not required to report currency transactions with commercial banks);
- Currency transactions with dealers in foreign exchange or check cashers conducted pursuant to a contractual agreement covering purchases of a casino check and exchanges of currency for currency, including foreign currency;
- Cash-ins to the extent the same physical currency was wagered previously in a money play on the same table without leaving the table;
- Bills inserted into electronic gaming devices in multiple transactions;
- Cash outs won in a money play, to the extent it is the same physical currency wagered; or
- Jackpots from slot machines or video lottery terminals.

1396. What are examples of currency transactions conducted in casinos and card clubs?

Currency transactions for casinos and card clubs include, but are not limited to, the following:

- Purchases or redemptions of chips, tokens and gaming instruments
- Front money deposits or withdrawals
- Safekeeping deposits or withdrawals
- Payments or advances on any form of credit, including markers and counter checks
- Bets or payments of bets in currency
- Currency received by a casino for transmittal of funds through wire transfer for a customer
- Purchases of checks or cashing of checks or other negotiable instruments

- Exchanges of currency for currency, including foreign currency
- Reimbursements for customers' travel and entertainment expenses by the casino

1397. What are multiple transaction logs?

Many casinos and card clubs record currency transactions within a given threshold, usually $2,500 to $3,000, on multiple transaction logs (MTLs) pursuant to state, tribal or local laws. Some casinos use MTLs to assist in aggregating transactions for CTR filing, as well as identifying potentially suspicious activity.

1398. Do casinos and card clubs also have to comply with Form 8300 reporting requirements?

Casinos and card clubs are required to comply with Form 8300 requirements for currency transactions of more than $10,000 received or paid for nongaming-related activities by a gambling or gaming establishment (e.g., hotel, restaurants, shops). For additional guidance, please refer to the Form 8300 section.

1399. Can casinos and card clubs grant CTR exemptions?

No. Only depository institutions (banks, savings associations, thrift institutions or credit unions) can grant exemptions and then only for their U.S. customers. For further guidance on exemptions, please refer to the CTR Exemptions section.

1400. Is there a unique SAR report that must be used by casinos and card clubs?

Beginning March 29, 2012, FinCEN replaced industry-specific SARs with a single report that must be submitted electronically. However, FinCEN will continue to accept SARs via electronic means until March 31, 2013. If a casino or card club decides to continue to submit legacy reports, it is required to file the Suspicious Activity Report by Casinos and Card Clubs (SAR-C) for suspicious transactions of $5,000 (or that aggregate to $5,000) or more, but may voluntarily file on suspicious transactions that are less than $5,000.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

1401. What types of activities require a SAR to be filed for casinos and card clubs?

Upon the detection of the following activities, casinos and card clubs should file a SAR:

- **Transactions aggregating to $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act (BSA)** – Any transaction(s) totaling or aggregating to at least $5,000 conducted by a suspect through the casino or card club, where the casino or card club knows, suspects or has reason to suspect that the transaction: involved illicit funds or is intended or conducted to hide or disguise funds or assets derived from illegal activities (including, but not limited to, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any law or regulation or avoid any transaction reporting requirement under federal law; or is designed to evade any BSA regulations.
- **Evasion** – A SAR should be filed in any instance where the casino or card club detects that the transaction was designed, whether through structuring or other means, to evade any BSA regulations.
- **No business or apparent lawful purpose** – The transaction has no business or apparent lawful purpose and there is no known reasonable explanation for the transaction after examination of available facts, including the background and possible purpose of the transaction.
- **Facilitate criminal activity** – The transaction involves the use of the casino or card club to facilitate criminal activity.

For red flags to assist in identifying suspicious activity as outlined above, please refer to the Suspicious Activity Red Flags section.

1402. Are there exceptions to the suspicious activity reporting requirements for casinos and card clubs?

Yes. Casinos and card clubs are not required to file a SAR for a robbery or burglary committed or attempted that is reported to appropriate law enforcement authorities.

1403. Are there red flags for detecting potentially suspicious activity for casinos and card clubs?

Yes. A comprehensive list of red flags for detecting potentially suspicious activity relating to account opening, transaction execution and high-risk products/services/transactions (e.g., cash, wires, monetary instruments) has been provided in this publication. For further guidance on red flags, please refer to the Suspicious Activity Red Flags and Casino Red Flags sections.

1404. How do casinos and card clubs submit CTRs and SARs to FinCEN?

Beginning July 1, 2012, casinos must submit CTRs and SARs through the BSA E-Filing System, an Internet-based e-filing system developed by FinCEN to enable financial institutions to file CTR and SAR forms electronically.

1405. What is the requirement for casinos and card clubs to perform independent testing of their AML programs?

Unlike the independent testing requirements imposed on other financial institutions, the final FinCEN rule on casinos and card clubs permits these entities to determine the scope and frequency of independent reviews at their discretion based on an evaluation of the money laundering and terrorist financing risks posed by their operations.

1406. What are the key recordkeeping requirements of the BSA for casinos and card clubs?

The BSA requires the retention of all BSA reports (e.g., SARs, CTRs, FBARs, CMIRs). Additionally, other required documentation must be retained by casinos and card clubs, such as the following:

- When required, a taxpayer identification number (TIN) (or passport number or description of a government-issued identification for nonresident aliens), name and address of each person for whom a deposit is made, an account is opened or line of credit is extended, or for each person who has a financial interest in the account
- List of names, addresses and account or credit line numbers of those persons from whom the casino or card club was unable to obtain the above information
- A record of each receipt (including, but not limited to, funds for safekeeping or front money) of funds by the casino or card club for deposit or credit account of any person that includes the name, address and TIN or passport number of the person from whom the funds were received
- A record of each bookkeeping entry comprising a debit or credit to a customer's deposit or credit account with the casino or card club
- Each statement, ledger card or other record of each deposit or credit account with the casino or card club, showing each transaction (including deposits, receipts, withdrawals, disbursements or transfers) in or with respect to a customer's deposit or credit account with the casino or card club
- A record of each extension of credit in excess of $2,500, the terms and conditions of such extension of credit and repayments, name, address, TIN or passport number of the customer, and date and amount of transactions
- A record of each advisement, request or instruction received or given by the casino or card club for itself or another person with respect to a transaction involving a person, account or place outside of the United States, including, but not limited to, communications by wire, letter or telephone; if the transfer was made on behalf of a third party, the record shall include the third party's name, address, TIN or passport number, signature, and date and amount of the transaction
- Records prepared or received by the casino or card club in the ordinary course of business, which would be needed to reconstruct a person's deposit or credit account with the casino or card club or to trace a check deposited with the casino or card club through the casino or card club's records to the bank of deposit
- All records, documents or manuals required to be maintained by the casino or card club under state and local laws or regulations, regulations of any governing Indian tribe or tribal government or terms of (or any regulations issued under) Tribal-State compacts entered into pursuant to the Indian Gaming Regulatory Act, with respect to the casino or card club in question
- All records that are prepared or used by a casino or card club to monitor a customer's gaming activity

- A separate record containing a list including the date and amount of the transaction, type of instrument, name and address of the customer, name of the drawee or issuer of the instrument, reference numbers (e.g., personal check number, casino account number), name or casino license number of the employee who conducted the transaction, of the following types of instruments having a face value of $3,000 or more:
    - Personal checks (excluding instruments that evidence credit granted by a casino or card club strictly for gaming, such as markers)
    - Business checks (including casino checks)
    - Official bank checks
    - Cashier's checks
    - Third-party checks
    - Promissory notes
    - Traveler's checks
    - Money orders
- Copy of the compliance program
- In the case of card clubs only, records of all currency transactions by customers, including, without limitation, records in the form of currency transaction logs and multiple currency transaction logs, and records of all activity at cages or similar facilities, including, without limitation, cage control logs
- Any record required to be maintained under the Funds Transfer Recordkeeping Requirements
- All indexes, books, programs, record layouts, manuals, formats, instructions, file descriptions and similar materials, which would enable a person to access and review the records described above readily

The above applies to casinos and card clubs. The BSA outlines additional requirements for other types of financial institutions (e.g., depository institutions, currency dealers or exchangers, broker-dealers) as well. For further guidance, please refer to the Recordkeeping Requirements, Money Services Businesses and Broker-Dealers sections.

1407. Are casinos and card clubs required to comply with OFAC and other sanction regulations?

Yes. OFAC requirements and other sanctions imposed by the United States apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. In addition, under limited circumstances, OFAC applies to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

1408. Who is responsible for examining casinos and card clubs for compliance with AML laws and regulations?

The Internal Revenue Service (IRS) is responsible for examining casinos and card clubs.

1409. Do other agencies have any role in overseeing casinos and card clubs?

States have various gaming regulatory agencies that supervise the industry. (For a list of state gaming agencies, please go to www.nagra.org.) State gaming regulators license and oversee casinos' and card clubs' operations. They also hold hearings and conduct background checks on personnel who own and are employed by these businesses as part of their effort to detect organized crime and other illegal activity.

The National Indian Gaming Commission (NIGC) is an independent federal regulatory agency whose primary mission is to regulate gaming activities on Indian lands for the purposes of ensuring that Indian tribes are the primary beneficiaries of gaming revenues, and assuring that gaming is conducted fairly and honestly by both operators and players. The NIGC is authorized to: conduct background investigations of primary management officials and key employees of a gaming operation, conduct audits, review and approve tribal gaming ordinances and management contracts, promulgate federal regulations, investigate violations of these gaming regulations, and undertake enforcement actions (including the assessment of fines and issuance of closure orders). Both Class II gaming (e.g.

bingo and certain card games) and Class III gaming (e.g. baccarat, blackjack, slot machines, and electronic or electromechanical facsimiles of any game of chance) are subject to the provisions of the Indian Gaming Regulatory Act (IGRA) and oversight by the NIGC. However, in general, the primary regulator for these activities is the tribal nations themselves.

Tribal-level regulators: Many tribal gaming commissions have been established by the tribes to oversee tribal gaming. The tribal nations have primary regulatory authority over Class II gaming. Regulation of Class III gaming may be addressed in the Tribal-State compacts (i.e. agreements between a state and a tribe, which are approved by the Secretary of the Interior, concerning the rules to govern the conduct of Class III gaming within the state). Although the terms of Tribal-State compacts vary by state, in most instances, the tribes remain the primary regulator for Class III gaming.

1410. What AML guidance has been issued related to casinos?

The following key guidance has been issued related to casinos:

- **Nonbank Financial Institutions – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Money Laundering of Casinos and Gaming Sector Report** (2009) by the Financial Action Task Force (FATF)
- **Risk-Based Approach for Casinos** (2008) by the FATF
- **Guidance on Casino or Card Club Risk-Based Compliance Indicators** (2010) by FinCEN
- **Guidance (Frequently Asked Questions) – Casino Recordkeeping, Reporting and Compliance Program Requirements** (2007, 2009, 2012) by FinCEN
- **Guidance on Casino or Card Club Compliance Program Assessment** (2010) by FinCEN
- **Definition of Money Services Business (Casinos as Money Services Businesses)** (2005) by FinCEN
- **Suspicious Activity Reporting Guidance for Casinos** (2003) by FinCEN
- **Guidance on Recognizing Suspicious Activity – Red Flags for Casinos and Card Clubs** (2008) by FinCEN
- **Currency Transaction Reporting: Aggregation by Casinos at Slot Machines** (2005)by FinCEN
- **Guidance on Determining Whether Tribally Owned and Operated Casinos are Eligible for Exemption from CTR Requirements** (2002) by FinCEN
- **A Cash Wager on Table Game Play Represents a "Bet of Currency"** (2006) by FinCEN
- **Casino Industry Currency Transaction Reporting: An Assessment of Currency Transaction Reports filed by Casinos Between July 1, 2006 and June 30, 2008** by FinCEN

Additionally, the **Indian Gaming Working Group (IGWG)** consists of representatives from the FBI's financial crimes, public corruption and organized crime subprograms as well as representatives from other federal law enforcement agencies that meet to address significant criminal violations in the Indian gaming arena.

Operators of Credit Card Systems

Definition

1411. What is an operator of a credit card system?

An operator of a credit card system is a business in the United States that administers a system for clearing and settling transactions in which the operator's credit card, whether acting as a credit card or debit card, is used to purchase goods or services or to obtain a cash advance, and authorizes another entity to serve as an issuing or acquiring institution for the operator's credit card, which must be usable in the United States. Although there are many issuing and acquiring institutions, there are few operators of such systems in the United States (e.g., MasterCard, Visa).

1412. Which types of operators of credit card systems are required to comply with AML laws and regulations?

All operators of credit card systems doing business in the United States are required to comply with AML laws and regulations. There is no exemption from the definition.

1413. What is the difference between an operator of a credit card system and an issuing/acquiring institution?

Any entity authorized by the operator to issue the operator's credit card is an "issuing institution." Any entity authorized to contract with merchants to process transactions involving the operator's credit card is called an "acquiring institution." Often, the operator authorizes both issuing and acquiring institutions (member institutions) and prescribes rules that member institutions must follow.

1414. What is the difference between general-purpose credit cards and merchant cards?

General-purpose credit cards (e.g., Discover, MasterCard, Visa) are cards accepted by a variety of merchants worldwide.

Other credit cards in the United States are issued by a particular merchant or vendor and may only be used in connection with purchases made from that merchant or vendor. Examples include department store and oil company credit cards.

1415. Are any operators of credit card systems exempted from AML requirements?

Merchants, vendors or banks whose issuance of credit cards is restricted to merchant cards (i.e., a credit card that may only be used at a specified merchant) do not fall within the definition of an operator of a credit card system and, therefore, are not subject to AML requirements.

Key AML and Sanction Requirements

1416. With which key AML and sanction requirements are operators of credit card systems required to comply?

Operators of credit card systems must comply with the following key AML requirements:

- Establishment of an AML program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program and conducts an independent review of the AML program
- Filing of Reports of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Information-sharing (Section 314(a) (mandatory), Section 314(b) (optional))
- OFAC and other sanction requirements

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to operators of credit card systems is provided below.

1417. Are operators of credit card systems subject to the CIP requirement?

No. Currently, operators of credit card systems are not subject to the Customer Identification Program (CIP) requirement. However, the operator must have written policies and procedures designed to ensure the operator does not authorize or maintain authorization for anyone to serve as an issuing or acquiring institution to guard against money laundering or terrorist financing. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

1418. Are operators of credit card systems required to file CTRs?

No. Currently, operators of credit card systems are not required to file Currency Transaction Reports (CTRs). Operators of credit card systems are, however, required to file Form 8300 for cash payments over $10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

1419. Are operators of credit card systems required to file SARs?

While they are not currently obligated to file Suspicious Activity Reports (SARs), FinCEN encourages operators to file a SAR voluntarily for reporting suspected money laundering and terrorist activity. There is a checkbox on Form 8300 for indicating that a transaction is potentially suspicious.

1420. Are operators of credit card systems required to comply with OFAC and other sanction regulations?

Yes. OFAC and other sanction requirements imposed by the United States apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. In addition, under limited circumstances, OFAC applies to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

Dealers in Precious Metals, Stones or Jewels

Definition

1421. Which types of dealers in precious metals, stones or jewels are required to comply with AML laws and regulations?

Anyone engaged as a business in the purchase and sale of covered goods (i.e., in precious metals, stones or jewels) that purchase and sell $50,000 or more of “covered goods” in the preceding year is required to comply with AML requirements.

1422. How are the terms “covered goods,” “precious metals,” “finished goods,” “jewels” and “stones” defined?

“Covered goods” include precious metals, stones or jewels, or finished goods that derive 50 percent or more of their value from precious metals, stones or jewels contained in or attached to the finished goods.

“Precious metals” are defined as gold, silver and certain other metals at a level of purity of 500 parts per 1,000 or greater and an alloy containing 500 or more parts per 1,000.

“Jewels” and “stones” are defined as organic substances that have a market-recognized gem level of quality, beauty and rarity.

“Finished goods” include, but are not limited to, jewelry, numismatic items and antiques.

1423. How should the $50,000 sales threshold be calculated?

The $50,000 sales threshold should be based on the value of precious metals, stones and jewels purchased and sold during the preceding year. It should not be based on the selling price of the finished goods purchased or sold. In other words, if a business purchases and sells finished goods that derive 50 percent or more of their value from precious stones, metals or jewels, the $50,000 sales threshold should be calculated based on the value of the precious stones, metals or jewels contained in the finished goods, not the selling price of the finished goods themselves.

The rule applies only to persons who both purchased $50,000 or more in covered goods and sold $50,000 or more in covered goods in the preceding calendar or tax year.

1424. Are trades or exchanges considered purchases?

For purposes of meeting the definition of "dealer" only, the purchase and sale of covered goods does not include retail transactions in which the dealer or retailer accepts from a customer covered goods, the value of which the dealer or retailer credits to the customer's account or to another purchase by the customer, and no funds are provided to the customer in exchange for the covered goods.

Trades or exchanges that are used for credit against the purchase of new covered goods should not be included in the $50,000 sales threshold used to define a dealer. Rather, the focus is on cash purchases.

Businesses that meet the definition of dealer should still examine the risk of trades or exchanges as they would with other transactions involving covered goods. Also, this exception is not an exception to the scope of the AML program required of a covered dealer other than a retailer.

1425. Does "toll-refining" constitute the purchase and sale of covered goods?

No. Toll-refining is the refining of scrap metal or concentrates for which the refinery is paid a fee. There is no change in ownership of the metal recovered. The payment of a fee is made in exchange for the service of refining, not for the extracted precious metal; therefore, this type of transaction would not constitute the purchase or sale of a covered good.

1426. Are retail establishments, such as department stores that sell high-end jewelry, required to establish an AML program?

The interim final rule distinguishes between "dealer" and "retailer." A retailer is a person in the United States engaged in sales of covered goods, primarily to the public. As long as retailers purchase covered goods from U.S.-based dealers/retailers or limit purchases from non-U.S.-based dealers/retailers to less than $50,000, they are not required to establish an AML program.

If retailers purchase $50,000 or more from non-U.S.-based dealers/retailers and sell more than $50,000 of covered goods over the same time they are covered, they are required to have an AML program to address the risks associated with purchases from foreign suppliers.

1427. Are there additional exemptions from the definition of "dealer"?

Businesses licensed or registered as pawnbrokers under state or municipal law are exempt from the definition of "dealer." Pawnbrokers are included in the USA PATRIOT Act's expanded definition of "financial institution." However, implementing regulations have yet to be issued.

Additionally, persons who merely facilitate the purchase and sale of covered goods (e.g., auctioneers, bankruptcy trustees) do not meet the definition of dealer.

Key AML and Sanction Requirements

1428. With which key AML and sanction requirements are dealers of precious metals, stones or jewels required to comply?

Dealers must comply with the following key AML and sanction requirements:

- Establishment of an AML program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, and conducts an independent review of the AML program
- Filing of Reports of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Information-sharing (Section 314(a) (mandatory), Section 314(b) (optional))
- OFAC and other sanction requirements

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to dealers is provided below.

1429. Are dealers subject to the CIP requirement?

No. Currently, dealers are not subject to the Customer Identification Program (CIP) requirement. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

1430. Are dealers required to file CTRs?

No. Currently, dealers are not required to file Currency Transaction Reports (CTRs). Dealers are, however, required to file Form 8300 for cash payments over $10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

1431. Are dealers required to file SARs?

While they are not currently obligated to file Suspicious Activity Reports (SARs), FinCEN encourages dealers to file a SAR voluntarily for reporting suspected money laundering and terrorist activity. There is a checkbox in Form 8300 for indicating that a transaction is potentially suspicious.

1432. Are dealers required to comply with OFAC and other sanction regulations?

Yes. OFAC and other sanction requirements apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. In addition, under limited circumstances, sanction requirements apply to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

1433. Who is responsible for examining dealers for compliance with AML laws and regulations?

The IRS is responsible for examining dealers for compliance with AML laws and regulations.

Investment Advisers and Unregistered Investment Companies

Definition

1434. What is an investment adviser?

The Investment Advisor Act of 1940 defines an “investment adviser” as “any person who, for compensation, engages in the business of advising others, either directly or through publications or writings, as to the value of securities or as to the advisability of investing in, purchasing, or selling securities, or who, for compensation and as part of a regular business, issues or promulgates analyses or reports concerning securities.”

1435. Are there any exemptions from the term “investment adviser”?

Yes. The term “investment adviser” does not include the following:

- A bank, or any bank holding company (BHC) as defined in the Bank Holding Company Act of 1956, which is not an investment company, except that the term ‘‘investment adviser’’ includes any bank or bank holding company to the extent that such bank or bank holding company serves or acts as an investment adviser to a registered investment company, but if, in the case of a bank, such services or actions are performed through a separately identifiable department or division, the department or division, and not the bank itself, shall be deemed to be the investment adviser;
- Any lawyer, accountant, engineer, or teacher whose performance of such services is solely incidental to the practice of his profession;

- Any broker or dealer whose performance of such services is solely incidental to the conduct of his business as a broker or dealer and who receives no special compensation therefore;
- The publisher of any bona fide newspaper, news magazine or business or financial publication of general and regular circulation;
- Any person whose advice, analyses, or reports relate to no securities other than securities which are direct obligations of or obligations guaranteed as to principal or interest by the United States, or securities issued or guaranteed by corporations in which the United States has a direct or indirect interest which shall have been designated by the Secretary of the Treasury, pursuant to section 3(a)(12) of the Securities Exchange Act of 1934, as exempted securities for the purposes of that Act;
- Any nationally recognized statistical rating organization, as that term is defined in section 3(a)(62) of the Securities Exchange Act of 1934, unless such organization engages in issuing recommendations as to purchasing, selling, or holding securities or in managing assets, consisting in whole or in part of securities, on behalf of others;
- Any family office, as defined by rule, regulation, or order of the Commission, in accordance with the purposes of this title; or
- Such other persons not within the intent of this paragraph, as the Commission may designate by rules and regulations or order.

1436. What is the role of the investment adviser in the fight against money laundering and terrorist financing?

Investment advisers play an important role in combating money laundering and terrorist financing because of their transactional knowledge. An investment adviser may be the only one with a complete understanding of the source of invested assets, the nature of the client's or the investment objectives and, therefore, is in a unique position to monitor customer transactions for suspicious activity.

1437. What is an investment company?

According to the Investment Company Act of 1940, an "investment company'' is defined as any issuer which:

- Is or holds itself out as being engaged primarily, or proposes to engage primarily, in the business of investing, reinvesting, or trading in securities;
- Is engaged or proposes to engage in the business of issuing face-amount certificates of the installment type, or has been engaged in such business and has any such certificate outstanding; or
- Is engaged or proposes to engage in the business of investing, reinvesting, owning, holding, or trading in securities, and owns or proposes to acquire investment securities having a value exceeding 40 per centum of the value of such issuer's total assets (exclusive of government securities and cash items) on an unconsolidated basis.

1438. Are all investment advisers and investment companies required to register with the SEC?

No. Some investment advisers and investment companies are exempt from registration requirements. In 2011, the Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA) amended many financial regulations, including the Investment Advisor Act of 1940 and the Investment Company Act of 1940. The exemption based on number of clients was eliminated, thereby subjecting previously exempted entities, such as hedge funds and private investment funds, to registration requirements with the SEC.

Key AML and Sanction Requirements

1439. With which key AML laws and regulations are investment advisers and unregistered investment companies required to comply?

Investment advisers and unregistered investment companies must comply with the following AML requirements:

- Filing of Reports of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)

- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- OFAC and other sanction requirements

For additional guidance on the various AML laws and regulations, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to investment advisers is provided below.

1440. Are investment advisers and unregistered investment companies required to establish an AML program?

No. At present, the AML program requirement of the USA PATRIOT Act does not apply to investment advisers or unregistered investment companies. In 2002 and 2003, FinCEN issued proposed rules which would have required certain types of investment advisors and unregistered investment companies to establish AML programs. The proposed rules were withdrawn in 2008. In its withdrawal notice, FinCEN said the primary reason for withdrawing the regulation was "passage of time." FinCEN further indicated that it would continue to consider whether it should impose AML program requirements on investment advisors and unregistered investment companies taking into consideration the significant changes in the regulatory framework due to the passage of the Dodd-Frank Act.

Even without further FinCEN action, investment advisers are still subject to the AML and Sanction requirements as noted above.

1441. Are investment advisers and unregistered investment companies subject to the CIP requirement?

No. Currently, investment advisers and unregistered investment companies are not subject to the Customer Identification Program (CIP) requirement. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

1442. Are investment advisers and unregistered investment companies required to file CTRs?

No. Currently, investment advisers and unregistered investment companies are not required to file Currency Transaction Reports (CTRs). Investment advisers are, however, required to file Form 8300 for cash payments over $10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

1443. Are investment advisers and unregistered investment companies required to file SARs?

While investment advisers and unregistered investment companies are not currently obligated to file Suspicious Activity Reports (SARs), FinCEN encourages the voluntary filing of a SAR for suspected money laundering and terrorist activity. There is a checkbox in Form 8300 for indicating that a transaction is potentially suspicious.

For further guidance on SARs, please refer to the Suspicious Activity Reports section.

1444. Are investment advisers and unregistered investment companies required to comply with the information-sharing requirement?

No. Only those institutions required to establish an AML program are obligated to comply with the information-sharing requirement (i.e., 314(a)).

1445. Are investment advisers and unregistered investment companies required to comply with OFAC and other sanction regulations?

Yes. OFAC requirements and other sanctions imposed by the United States apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. In addition, under limited circumstances, sanction requirements apply to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

Persons Involved in Real Estate Settlements and Closings

Definition

1446. Which types of persons involved in real estate settlements and closings are required to comply with AML laws and regulations?

FinCEN issued an advance notice of proposed rulemaking on April 3, 2003, defining a real estate settlement or closing as the process involving the payment of the purchase price to the seller and the transfer of title to the buyer.

The manner in which the process is carried out differs depending on a number of factors, including location. The process may be conducted by an attorney, a title insurance company, an escrow company or another party.

1447. Are all types of real estate transactions subject to AML laws and regulations?

Proposed rulings have not excluded any types of real estate transactions; however, regulators have sought comments on the possibility of exempting commercial real estate activity from AML laws and regulations.

1448. Who is considered a person "involved" in real estate settlements and closings?

Under the proposed rule, involved persons include, but are not limited to, the following:

- Real estate broker
- Attorney representing buyer/seller
- Financing entity (e.g., bank, mortgage broker)
- Title insurance company
- Escrow agent
- Real estate appraiser

1449. What factors are being considered by the U.S. Treasury Department to determine which involved persons will be subject to further AML laws and regulations?

The following factors are being considered by the U.S. Treasury:

- Persons offering high-risk products/services in connection with a real estate closing and settlement (i.e., products/services that can be abused by money launderers or terrorists)
- Persons who are positioned to monitor for suspicious activity effectively (e.g., those who can identify the source, purpose and nature of transactions)

Concerned with the conflicts between the requirement to report suspicious activity and attorney-client privilege and client confidentiality, some law firms have suggested utilizing the following factor to determine applicability:

- Position as financial intermediary (i.e., persons who handle the receipt and transmission of cash proceeds through accounts that they control in the act of closing a real estate transaction)

Though the financial intermediary factor may be of assistance in clearly defining "involved persons," it is important to note that individuals who do not "touch the money" may still be in positions to detect and report suspicious activity related to real estate settlements and closings (e.g., suspicious documentation, identity theft).

1450. Are any persons involved in real estate settlements and closings exempt from AML laws and regulations?

Purchasers and sellers of their own real estate are exempted from the definition of real estate settlements and closings and are not subject to AML laws and regulations.

1451. What is the difference between a closing and a settlement?

The terms “closing” and “settlement” refer to the same process. Use of either term is dependent on the jurisdiction in which the activity takes place. Other terms used to describe the closing/settlement process include “New York style table closing,” “Western style table closing” or “escrow closing.”

1452. What AML guidance has been issued related to real estate?

The following are examples of key guidance that has been issued related to real estate:

- **Lending Activities – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **An OFAC Primer for the Real Estate Settlement and Title Insurance Industry** (2003) by the Office of Foreign Assets Control (OFAC)
- **RBA Guidance for Real Estate Agents** (2008) by the Financial Action Task Force (FATF)
- **Money Laundering and Terrorist Financing Through the Real Estate Sector** (2007) by FATF
- **Money Laundering in the Commercial Real Estate Industry: An Assessment Based Upon Suspicious Activity Report Filing Analysis** (2006) by the Financial Crimes Enforcement Network (FinCEN)

Key AML and Sanction Requirements

1453. With which key AML and sanction requirements are persons involved in real estate settlements and closings required to comply?

Persons involved in real estate settlements and closings are required to comply with the following key AML requirements:

- Filing of Reports of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- OFAC and other sanction requirements

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to persons involved in real estate settlements and closings is provided below.

1454. Are persons involved in real estate settlements and closings required to establish an AML program?

No. At present, the AML program requirement of the USA PATRIOT Act does not apply to persons involved in real estate settlements and closings. However, some institutions, such as banks, are already covered and are subject to AML requirements.

1455. Are persons involved in real estate settlements and closings subject to the CIP requirement?

No. Currently, persons involved in real estate settlements and closings are not subject to the Customer Identification Program (CIP) requirement. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

1456. Are persons involved in real estate settlements and closings required to file CTRs?

No. Currently, persons involved in real estate settlements and closings are not required to file Currency Transaction Reports (CTRs). They are, however, required to file Form 8300 for cash payments over $10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

1457. Are persons involved in real estate settlements and closings required to file SARs?

While they are not currently obligated to file Suspicious Activity Reports (SARs), FinCEN encourages the voluntary filing of a SAR for suspected money laundering and terrorist activity. There is a checkbox on Form 8300 for indicating that a transaction is potentially suspicious.

1458. Are there red flags for detecting potentially suspicious activity for persons involved in real estate settlements and closings?

Yes. A comprehensive list of red flags for detecting potentially suspicious activity relating to account opening, transaction execution, and high-risk products/services/transactions (e.g., cash, wires, monetary instruments, lending) has been provided in this publication. For further guidance on red flags, please refer to the Suspicious Activity Red Flags, Lending Red Flags and Mortgage and Real Estate Red Flags sections.

1459. Are persons involved in real estate settlements and closings required to comply with the information-sharing requirement?

No. Only those institutions required to establish an AML program are obligated to comply with the information-sharing requirement (i.e., 314(a)).

1460. Are persons involved in real estate settlements and closings required to comply with OFAC and other sanction regulations?

Yes. OFAC requirements and other sanctions imposed by the United States apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. In addition, under limited circumstances, OFAC applies to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

Nonbank Residential Mortgage Lenders and Originators

Definition

1461. What is a “nonbank residential mortgage lender or originator”?

Nonbank residential mortgage lenders and originators (RMLOs) are a subset of loan and finance companies that deal directly with customers to provide loans and financing for residential mortgage loans.

A residential mortgage lender is defined as “the person to whom the debt arising from a residential mortgage loan is initially payable on the face of the evidence of indebtedness or, if there is no such evidence of indebtedness, by agreement, or to whom the obligation is initially assigned at or immediately after settlement.” Individuals who finance the sale of their own dwelling or real property are not included in the definition of residential mortgage lender.

A residential mortgage originator is defined as “a person who accepts a residential mortgage loan application or offers or negotiates terms of a residential mortgage.”

1462. What is a “residential mortgage”?

A residential mortgage is defined as “a loan that is secured by a mortgage, deed of trust or other equivalent consensual security interest on:

- A residential structure that contains one to four units, including, if used as a residence, an individual condominium unit, cooperative unit, mobile home or trailer; or
- Residential real estate upon which such a structure is constructed or intended to be constructed.”

1463. Are nonbank RMLOs considered to be "financial institutions" under the Bank Secrecy Act (BSA) or the USA PATRIOT Act?

The definition of "financial institution" under the BSA, which was significantly expanded by the USA PATRIOT Act, does not specifically include nonbank RMLOs. However, the term "financial institution" includes "loan or finance companies" which now include nonbank RMLOs pursuant to FinCEN's final rule, "Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Residential Mortgage Lenders and Originators." FinCEN regulations do not define "loan or finance company" but do indicate that the following are excluded:

- Banks;
- Person regulated/examined by the U.S. Securities and Exchange Commission or the Commodity Futures Trading Commission;
- Government-sponsored enterprise (GSE) regulated by the Federal Housing Finance Agency;
- Federal or state agency or authority administering mortgage or housing assistance, fraud prevention or foreclosure prevention programs; and
- An individual employed by a bank, loan or finance company, or other regulated business.

1464. Are any other types of entities included in the definition of "loan or finance company"?

At this time, only nonbank RMLOs fall under the definition of "loan or finance company." FinCEN has indicated that it has plans to add other types of entities in an incremental approach to implementing AML regulations for loan and finance companies.

1465. Are any nonbank RMLOs exempt from the final rule?

No. All nonbank RMLOs are required to comply with the final rule, regardless of size or other criteria or characteristic.

1466. What is the purpose of this final rule?

In 2006, FinCEN began a series of extensive studies around mortgage fraud and other related financial crimes; this focus was heightened by the financial crisis. These efforts led to the observation that nonbank RMLOs are uniquely positioned, through their direct contact with customers, to identify, assess, and report on risks of fraudulent activity and money laundering. The imposition of these AML requirements on nonbank RMLOs is intended to close or mitigate an identified gap in reporting on this activity.

FinCEN and other government agencies, including the U.S. Department of Justice (DOJ), anticipate that requiring nonbank RMLOs to file SARs will assist their ability to uncover large-scale mortgage fraud in addition to traditional money laundering, through an increased number of SAR filings, and serve as a deterrent to criminal activity.

1467. Who is responsible for examining nonbank RMLOs for compliance with AML laws and regulations?

Where nonbank RMLOs do not have a federal functional regulator, FinCEN is proposing that Congress allow FinCEN to rely on examinations conducted by state supervisory agencies.

1468. What guidance has been issued regarding the differences in requirements for loan or finance company subsidiaries of other financial institutions?

On August 13, 2012, FinCEN issued an Administrative Ruling to clarify expectations regarding "*Compliance obligations of certain loan or finance company subsidiaries of federally regulated banks and other financial institutions*." The ruling indicated that loan or finance subsidiaries would be obligated to comply with the AML laws and regulations applicable to their parent financial institution. Additionally, the loan or finance subsidiary would be subject to examination by the parent financial institution's federal functional regulator.

1469. Is FinCEN focused on other participants in the mortgage market in addition to nonbank RMLOs?

Yes. FinCEN has and continues to consider whether and how AML requirements should apply to other participants in the mortgage market, including the following:

- Persons involved in real estate closings and settlements; and

- Housing GSEs (e.g., Freddie Mac, Fannie Mae).

As part of the proposed rule for housing GSEs, FinCEN requested comments on what other mortgage-related activities and entities should be subject to AML program and SAR filing requirements. Specifically, FinCEN has solicited feedback on the following participants in the mortgage market:

- Private mortgage insurers (and reinsurers);
- Mortgage servicers; and
- Other types of businesses in the primary and secondary mortgage markets.

For further guidance, please refer to the sections: Housing Government Sponsored Enterprises and Persons Involved in Real Estate Settlements and Closings.

1470. What other guidance been issued to assist nonbank RMLOs in complying with AML laws and regulations?

FinCEN has created a page on its website, dedicated to mortgage companies and brokers, with publications and webinar trainings to assist RMLOs in complying with AML laws and regulations. Additionally, on August 16, 2012, FinCEN issued a notice specifically to remind RMLOs of the forthcoming AML laws and requirements and re-outlined the requirements in order to help support RMLOs in understanding the extent of the new regulations applicable to them.

Additionally, FinCEN has developed substantial data analytics around mortgage-related financial crimes to help RMLOs understand the significance and purpose behind the AML laws and regulations. The publications on these metrics include:

- Mortgage Fraud SAR Data Tables by State, Urban Area and County
- Suspected Mortgage Fraud (Including Quarterly Written Reports)
- Suspected Money Laundering and Fraud in the Residential Real Estate Industry
- Suspected Money Laundering and Fraud in the Commercial Real Estate Industry
- Home Equity Conversion Mortgages (Reverse Mortgages)
- Mortgage Fraud Cases Supported by FinCEN Filings
- Foreclosure Rescue Scams & Loan Modification Fraud

There is also access to links for other government agencies and initiatives, such as the Financial Fraud Enforcement Task Force (FFETF).

For additional information, please refer to the Mortgage Fraud section.

Key AML and Sanction Requirements

1471. With which key AML and sanction requirements are nonbank RMLOs required to comply?

Nonbank RMLOs are required to comply with the following key AML and sanction requirements:

- Establishment of an AML program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, and conducts an independent review of the AML program
- Filing of Suspicious Activity Reports (SARs)
- Filing of Reports of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Information sharing (Section 314(a) (mandatory), Section 314(b) (optional))

- OFAC and other sanction requirements

The proposed rule requires that the AML program be risk-based, approved by senior management and made available to FinCEN or its designee upon request.

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections.

1472. Are nonbank RMLOs subject to the CIP requirement?

No. Currently, nonbank RMLOs are not subject to the Customer Identification Program (CIP) requirement. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

1473. Are nonbank RMLOs required to file CTRs?

No. Currently, nonbank RMLOs are not required to file Currency Transaction Reports (CTRs). They are, however, required to file Form 8300 for cash payments over US$10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

1474. Are nonbank RMLOs required to comply with OFAC and other sanction laws and regulations?

Yes. OFAC requirements and other sanctions imposed by the United States apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S.-incorporated entities and their foreign branches. In addition, under limited circumstances, OFAC requirements apply to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

1475. What is the SAR filing requirement for nonbank RMLOs?

Nonbank RMLOs are required to report a transaction that involves funds of at least $5,000 and that the nonbank RMLO knows, suspects, or has reason to suspect that a transaction:

- Involves funds derived from illegal activity or is intended or conducted to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
- Is designed, whether through structuring or other means, to evade any reporting requirements under regulations promulgated by the BSA;
- Has no business or apparent lawful purpose or is not the sort in which the particular nonbank RMLO customer would normally be expected to engage, and the nonbank RMLO knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or
- Involves the use of the nonbank RMLO to facilitate criminal activity.

For further guidance, please refer to the Suspicious Activity Reports section.

1476. Are the SAR filing requirements for nonbank RMLOs the same as for other covered financial institutions?

Yes. Nonbank RMLOs' SAR filing requirements (e.g., time frame for filing, dollar thresholds, confidentiality, etc.) are the same as those for banks and non-bank financial institutions. For additional guidance on SAR filing requirements, please refer to the Suspicious Activity Reports section.

1477. Are nonbank RMLOs afforded the same "Safe Harbor" protection as other covered financial institutions?

Yes. Nonbank RMLOs, as well as their directors, officers, employees and agents, would be covered under the Safe Harbor provision. For further guidance, please refer to the Safe Harbor section.

1478. Are nonbank RMLOs permitted to file a SAR jointly with another financial institution?

Yes, in instances where more than one nonbank RMLO or other financial institution is obligated to report on the same transaction(s), only one SAR should be filed on behalf of all the financial institutions involved. That SAR should identify all of the financial institutions involved and provide all the relevant facts relating to each institution. Each institution should retain a copy of the SAR, along with supporting documentation. For further guidance, please refer to the Joint Filings of SARs section.

1479. What are some examples of red flags with which nonbank RMLOs may be concerned?

Common red flags include, but are not limited to, the following:

- Borrower arrives at a real estate closing with a significant amount of cash;
- Borrower purchases property in the name of a nominee, such as an associate or a relative;
- Borrower negotiates a purchase for market value or above asking price, but records a lower value on documents, paying the difference "under the table";
- Borrower sells property below market value with an additional "under the table" payment;
- Borrower or agent of the borrower purchases property without much knowledge about the property inspection or does not appear sufficiently knowledgeable about the purpose or use of the real estate being purchased;
- Borrower purchases multiple properties in a short time period or appears to be buying and selling the same piece of real estate for no apparent legitimate purpose;
- Seller requests that proceeds be sent to a high-risk jurisdiction or offshore bank; and
- Borrower makes payments with funds from a high-risk jurisdiction or offshore bank.

For additional guidance, please refer to the sections: Mortgage Fraud, Mortgage and Real Estate Red Flags and Lending Red Flags.

1480. Can a nonbank RMLO rely on third parties to conduct parts of its AML program?

Yes. It is permissible for nonbank RMLOs to delegate responsibility to a third party and rely on the compliance programs of third parties that are subject to their own AML Compliance Program requirements under the BSA.

Additionally, nonbank RMLOs that rely on financing from banks or insured depository institutions can expect that banking partners will inquire about their new AML programs and may need evidence of compliance with the new rule.

1481. Does delegating aspects of its AML program to a third party mean a nonbank RMLO will not be held responsible?

No. Any nonbank RMLO that delegates responsibility to a third party remains fully responsible for the effectiveness of its AML program and for ensuring that compliance examiners are able to obtain access to any information they need relating to the nonbank RMLO's AML Compliance Program.

1482. Are nonbank RMLOs permitted to participate in the information sharing provisions under Sections 314(a) and (b) of the USA PATRIOT Act?

Yes. Any financial institutions required to establish an AML program under Section 352, including nonbank RMLOs, are obligated to comply with Section 314(a) information requests and may voluntarily participate in the information sharing mechanisms established by Section 314(b). Specifically, Sections 1010.520 and 1010.540 implement Sections 314(a) and (b) for nonbank RMLOs.

For further guidance, please refer to the sections: Section 314(a) – Cooperation among Financial Institutions, Regulatory Authorities and Law Enforcement Authorities and Section 314(b) – Cooperation Among Financial Institutions.

Housing Government Sponsored Enterprises

Definition

1483. What is a government sponsored enterprise (GSE)?

A government sponsored enterprise (GSE) is a financial services organization created and regulated by the U.S. government (specifically, by Congress) and functioning to increase the availability and reduce the cost of credit to targeted sectors such as education, agriculture and home finance. Examples of GSEs include, but are not necessarily limited to:

- Federal National Mortgage Association (Fannie Mae)
- Federal Home Loan Mortgage Corporation (Freddie Mac)
- Federal Agricultural Mortgage Corporation (Farmer Mac)
- The 12 Federal Home Loan Banks (FHLBanks)
- Federal Farm Credit Banks
- Financing Corporation (FICO)
- National Veterans Business Development Corporation

1484. Which GSEs are required to comply with AML laws and regulations?

The Financial Crimes Enforcement Network (FinCEN) issued a Notice of Proposed Rulemaking (NPR) on November 8, 2011, defining certain "Housing" GSEs as financial institutions for the purpose of requiring them to establish AML programs and comply with certain reporting requirements pursuant to the Bank Secrecy Act (BSA) and the USA PATRIOT Act. Housing GSEs that are subject to the proposed rule include the following:

- Fannie Mae
- Freddie Mac
- FHLBanks

1485. What is the purpose of this proposed rule?

FinCEN indicated that the proposed rule is another effort to help restore the integrity of the mortgage market by providing law enforcement with quicker access to data about potential financial crimes that will help them better hold illicit actors accountable for mortgage fraud and other scams. In the last five years, as an offshoot of the financial crisis, FinCEN has made increasing the focus on preventing, detecting and reporting mortgage fraud one of its highest priorities. For further information, please refer to the Mortgage Fraud section.

1486. Is a GSE considered a "financial institution" under the BSA or the USA PATRIOT Act?

The definition of "financial institution" under the BSA, which was significantly expanded by the USA PATRIOT Act, does not specifically include GSEs. However, the term, "financial institution" includes "any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any [covered financial institution] is authorized to engage." As stated above, the NPR designates certain Housing GSEs as financial institutions.

1487. Would designating Housing GSEs as covered financial institutions trigger additional AML requirements beyond those outlined in the proposed rule?

No. Under the proposed rule, the Housing GSEs would only be considered financial institutions under the U.S. Treasury Department's BSA authority and would not be included within the definition of "financial institution" under FinCEN's regulation 31 CFR 1010.100(t). Thus, Housing GSEs would not be subject to other recordkeeping and reporting requirements triggered by that regulation.

1488. Why are only Housing GSEs subject to this proposed rule?

Of the various types of GSEs, Housing GSEs are those most closely involved with the lending processes and are best positioned to provide relevant and meaningful data to FinCEN for tracking and data analytics purposes. Housing GSEs are also the most vulnerable to the use of mortgages to commit financial crimes. Prohibitive measures for these institutions would best serve the entire financial system.

1489. Who would be responsible for examining GSEs for compliance with AML laws and regulations?

Currently, authority over the Housing GSEs resides with its primary regulator, the Federal Housing Finance Agency (FHFA); however, the FHFA does not currently have the authority to enforce FinCEN regulatory requirements. According to the Notice of Proposed Rulemaking, FinCEN anticipates delegating examination for compliance with the proposed rule to the FHFA, but will continue to retain enforcement authority, as it does with other types of financial institutions.

1490. Are the Housing GSEs likely to encounter any unique challenges in implementing FinCEN's proposed rule?

Although current practice requires that the Housing GSEs have comprehensive information related to commercial loans they acquire, they traditionally have relied on the selling institutions to analyze retail borrowers and have not collected information for individual retail borrowers. This will create an obvious challenge to identifying suspicious activity at the retail customer level even though the proposed rule suggests that Housing GSEs would not be expected to collect information they don't currently collect.

1491. Is FinCEN focused on other participants in the mortgage market in addition to Housing GSEs?

Yes. FinCEN has and continues to consider whether and how AML requirements should apply to other participants in the mortgage market, including the following:

- Persons involved in real estate closings and settlements; and
- Loan and finance companies.

Shortly after issuing the proposed rule for Housing GSEs, FinCEN issued a Final Rule in February 2012 requiring Non-Bank Residential Mortgage Lenders and Originators, a subset of a loan and finance company, to establish AML programs and file SARs. For further guidance, please refer to the Nonbank Residential Mortgage Lenders and Originators section.

Additionally, as part of the proposed rule, FinCEN requested comments on what other mortgage-related activities and entities should be subject to AML program and SAR filing requirements. Specifically, FinCEN has solicited feedback on the following participants in the mortgage market:

- Private mortgage insurers (and reinsurers);
- Mortgage servicers; and
- Other types of businesses in the primary and secondary mortgage markets.

1492. What key AML guidance has been issued on Housing GSEs?

In January 2010, the FHFA issued fraud reporting regulations that require Housing GSEs to implement processes for identifying, and timely reporting to the FHFA upon discovery that they had purchased or sold, a fraudulent loan or financial instrument. The required processes must include policies, procedures, internal controls and training for identifying the fraudulent transactions. While not described per se as AML requirements, FinCEN believes these FHFA requirements likely mean that most, if not all, of the GSEs already have anti-fraud programs that will go a long way toward satisfying the proposed FinCEN requirements.

Key AML and Sanction Requirements

1493. With which key AML and sanction requirements are Housing GSEs required to comply?

Housing GSEs are required to comply with the following key AML and sanction requirements:

- Filing of Reports of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- OFAC and other sanction requirements

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections.

1494. Are Housing GSEs subject to the CIP requirement?

No. Currently, Housing GSEs are not subject to the Customer Identification Program (CIP) requirement. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

1495. Who are the typical customers of Housing GSEs?

Housing GSEs support the primary mortgage market by providing liquidity through loan purchases and collateralized advances that permit their customers, typically commercial banks, credit unions and thrifts, to offer a broad range of credit products and related services. Many of their typical customers are subject to AML laws and regulations.

1496. Are Housing GSEs required to file CTRs?

No. Currently, Housing GSEs are not required to file Currency Transaction Reports (CTRs). They are, however, required to file Form 8300 for cash payments over US$10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

1497. Are Housing GSEs required to comply with OFAC and other sanction laws and regulations?

Yes. Office of Foreign Assets Control (OFAC) requirements and other sanctions imposed by the United States apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S.-incorporated entities and their foreign branches. In addition, under limited circumstances, OFAC applies to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

1498. What additional AML requirements would the proposed rule impose on Housing GSEs?

FinCEN's proposed rule would require Housing GSEs to comply with the following AML requirements:

- Establishment of an AML program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, and conducts an independent review of the AML program
- Filing of Suspicious Activity Reports (SARs)
- Information-sharing (314(a) (mandatory), 314(b) (optional))

The proposed rule requires that the AML program be risk-based, approved by senior management and made available to FinCEN or its designee upon request.

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections.

1499. How does the SAR filing requirement impact existing suspicious activity reporting requirements of Housing GSEs?

Under the existing FHFA requirement, Housing GSEs file reports of fraudulent activity with the FHFA. Where appropriate, the FHFA then files SARs with FinCEN, based on the fraud reports submitted by the Housing GSEs. Under the proposed rule, SARs would be filed directly with FinCEN by the Housing GSE. If the proposed rule is adopted, it is possible that FHFA may amend its rule to avoid duplicative efforts.

Additionally, Housing GSEs would have to report on financial crimes broader than fraud, including transactions conducted or attempted by, at or through a Housing GSE that aggregate to at least US$5,000, and that the Housing GSE knows, suspects or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

- Involves funds derived from illegal activity or is intended or conducted to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
- Is designed, whether through structuring or other means, to evade any reporting requirements under regulations promulgated by the BSA;
- Has no business or apparent lawful purpose or is not the sort in which the particular Housing GSE customer would normally be expected to engage, and the Housing GSE knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or
- Involves use of the Housing GSE to facilitate criminal activity.

1500. Would the SAR filing requirements for Housing GSEs be the same as for other covered financial institutions?

Yes. Housing GSE SAR filing requirements (e.g., time frame for filing, dollar thresholds, confidentiality, etc.) would be the same as those for banks and non-bank financial institutions. For additional guidance on SAR filing requirements, please refer to the Suspicious Activity Reports section.

1501. Would Housing GSEs be afforded the same "Safe Harbor" protection as other covered financial institutions?

Yes. Housing GSEs, as well as their directors, officers, employees and agents, would be covered under the Safe Harbor provision. This is especially important for Housing GSEs because the "Safe Harbor" enables the uninhibited filing of SARs for types of activity to which the Housing GSEs may not be accustomed. For further guidance, please refer to the Safe Harbor section.

1502. Would a Housing GSE be permitted to file a SAR jointly with another financial institution?

Yes. In instances where either a second Housing GSE or other covered financial institution is involved in a transaction or activity resulting in the filing of a SAR, only one report is required to be filed. The report should contain all of the facts pertaining to each institution's involvement, and each institution should maintain a copy of the SAR filed along with supporting documentation. For further guidance, please refer to the Joint Filings of SARs section.

1503. What are some examples of red flags with which Housing GSEs may be concerned?

Common red flags for mortgage-related products and services include, but are not limited to, the following:

- Customer is looking to conduct associated transactions (e.g., real estate purchases, down payments, fees, closing costs, etc.) in cash
- Borrower purchases property in the name of a nominee, such as an associate or a relative
- Borrower negotiates a purchase for market value or above asking price, but records a lower value on documents, paying the difference "under the table"
- Borrower sells property below market value with an additional "under the table" payment
- Borrower or agent of the borrower purchases property without much knowledge about the property inspection or does not appear sufficiently knowledgeable about the purpose or use of the real estate being purchased
- Borrower purchases multiple properties in a short period of time or appears to be buying and selling the same piece of real estate for no apparent legitimate purpose
- Seller requests that proceeds be sent to a high-risk jurisdiction or offshore bank
- Borrower makes payments with funds from a high-risk jurisdiction or offshore bank
- Borrower pays off the original loan with cash and/or significantly in advance of the expected terms of the loan

For additional guidance, please refer to the sections: Mortgage Fraud, Mortgage and Real Estate Red Flags and Lending Red Flags.

1504. May a Housing GSE rely on third parties to conduct parts of its AML program?

The FinCEN proposal acknowledges that some components of a Housing GSE's AML program might best be conducted by third parties and indicates that it is permissible for the Housing GSE to delegate responsibility to a third party and rely on the compliance programs of third parties that are subject to their own AML Compliance Program requirements under the BSA.

1505. Does delegating aspects of its AML program to a third party mean a Housing GSE will not be held responsible?

No. Any Housing GSE that delegates responsibility to a third party remains fully responsible for the effectiveness of its program and for ensuring that compliance examiners are able to obtain access to any information they need relating to the Housing GSE's AML Compliance Program.

1506. Would Housing GSEs be permitted to participate in the information sharing provisions under Sections 314(a) and (b) of the USA PATRIOT Act?

Yes. Any financial institutions required to establish an AML program under Section 352, including Housing GSEs, are obligated to comply with Section 314(a) information requests and may voluntarily participate in the information sharing mechanisms established by Section 314(b). Specifically, Sections 1010.520 and 1010.540 implement Sections 314(a) and (b) for Housing GSEs.

For further guidance, please refer to the sections: Section 314(a) – Cooperation among Financial Institutions, Regulatory Authorities and Law Enforcement Authorities and Section 314(b) – Cooperation Among Financial Institutions.

Nonfinancial Businesses

Definition

1507. Which types of nonfinancial businesses pose a higher money laundering and terrorist financing risk?

Nonfinancial businesses considered to be high-risk for money laundering and terrorist financing include those that are cash-intensive; those that allow for the easy conversion of cash into other types of assets; those that provide opportunity to abuse authoritative powers and assist in disguising the illegal transfer of funds; those that lack transparency; those that involve international transactions/customers; and those that offer high-risk or high-value products. High-risk nonfinancial businesses include, but are not limited to, the following:

- Accounting firms
- Aircraft engine/part and military armored vehicle manufacturing
- Amusement, gambling and recreation activities
- Art/antiques dealers
- Car washes
- Charitable organizations/Nongovernmental organizations (NGOs)
- Cigarette distributors
- Consumer electronics rentals and dealers
- Convenience stores
- Flight training schools
- Gas stations

- Importers/exporters
- Law firms
- Leather manufacturing, finishing and goods stores
- Liquor stores
- Notaries
- Offshore companies
- Parking garages
- Restaurants
- Retail establishments
- Businesses controlled by politically exposed persons (PEPs) and political organizations
- Small arms and ammunition manufacturing
- Tobacco wholesalers
- Transportation services and equipment rental
- Textile businesses
- Vending machine operators

Accounting firms, law firms and notaries are considered professional service providers and, in some countries, are subject to AML requirements of their own. For additional guidance on professional service providers and other high-risk entities, please refer to the following sections: High Risk Customers, Professional Service Providers, Business Entities: Shell Companies and Private Investment Companies and Nongovernmental Organizations and Charities.

Key AML and Sanction Requirements

1508. With which key AML and sanction requirements are nonfinancial institutions required to comply?

Nonfinancial institutions must comply with the following key AML requirements:

- Filing of Reports of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- OFAC and other sanction requirements

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to nonfinancial institutions is provided below.

1509. Are nonfinancial institutions required to comply with OFAC regulations?

Yes. OFAC requirements and other sanctions imposed by the United States apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. In addition, under limited circumstances, OFAC applies to foreign subsidiaries of U.S. entities. OFAC is not an AML law or regulation per se, but since the OFAC list includes alleged money launderers and terrorists, financial institutions often consider the OFAC program to be a subset of their overall AML program. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Government Sanctions Programs section.

1510. Are nonfinancial institutions required to establish an AML program?

No. At present, the AML program requirement of the USA PATRIOT Act does not apply to nonfinancial institutions. However, some nonfinancial institutions have opted to implement an AML program voluntarily to mitigate reputation risk of being abused for money laundering or terrorist financing.

1511. Are nonfinancial institutions required to file CTRs?

No. Currently, nonfinancial institutions are not required to file Currency Transaction Reports (CTRs). Nonfinancial institutions are, however, required to file Form 8300 for cash payments over $10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

1512. Are nonfinancial institutions required to file SARs?

While nonfinancial institutions are not currently obligated to file Suspicious Activity Reports (SARs), FinCEN encourages the voluntary filing of SARs on suspected money laundering and terrorist activity. There is a checkbox on Form 8300 for indicating that a transaction is potentially suspicious.

1513. Are there red flags for detecting potentially suspicious activity for nonfinancial businesses?

Yes. A comprehensive list of red flags for detecting potentially suspicious activity relating to transaction execution and high-risk products/services/transactions (e.g., cash, monetary instruments) has been provided in this publication. For further guidance on red flags, please refer to the Suspicious Activity Red Flags and Retail Red Flags sections.

1514. Are nonfinancial institutions required to comply with the information-sharing requirement?

No. Only those institutions required to establish an AML program are obligated to comply with the information-sharing requirement (i.e., 314(a)).

1515. What are the benefits of voluntarily implementing an AML program in a nonfinancial institution?

Nonfinancial institutions increasingly are becoming involved in money laundering schemes as it becomes more difficult for criminals to introduce illicit funds into the financial system. Law enforcement investigations that result from money laundering allegations may damage an organization's reputation. Therefore, beyond the legal and regulatory requirements noted above, nonfinancial businesses need to consider and take seriously the risk of being targeted or used for money laundering, either by employees or outside parties.

While a nonfinancial business is not subject to the requirements of the USA PATRIOT Act to implement an AML program, the existence of an AML program for such an institution may help to mitigate the organization's money laundering and terrorist financing risk and preserve the institution's reputation.

CONVERGENCE OF AML WITH FRAUD AND OTHER REGULATORY TOPICS

AML and Anti-Fraud Programs

1516. Why are some financial institutions considering integrating their AML and anti-fraud programs?

Financial institutions that are considering integrating AML and anti-fraud programs are motivated by the potential synergy available through cross channel alerts, access to broad financial intelligence as well as the possibility of cost savings by leveraging technology platforms and pooling resources.

In addition, financial regulators, as well as the Director of FinCEN, have also expressed support of the combined AML and anti-fraud approach to take advantage of the potential efficiencies.

1517. What is a cross channel alert?

A cross channel alert involves the sharing of information between groups that has utility for all involved groups (e.g., AML and anti-fraud units).

1518. How do cross channel alerts aid in the process of detecting financial crimes?

The triggering of more than one type of alert, from AML and/or fraud sources, may increase the likelihood of detecting truly suspicious activities. Further, one channel could be used to heighten awareness in another channel and better focus the investigative process.

For example, if a customer generates an AML alert for activity out of profile, the fraud team may also benefit from this information, particularly if the fraud system has also detected unusual behavior. This practice is already used within AML compliance where receipt of a subpoena, National Security Letter (NSL) or an alert for a possible sanctions violation may trigger an investigation for potentially suspicious activity. For further guidance on monitoring and investigative processes, please refer to the Transaction Monitoring, Investigations and Red Flags section.

1519. Historically, how have AML and anti-fraud programs within the same financial institution interacted?

Historically, AML and anti-fraud programs viewed their missions as separate and distinct. Anti-fraud managers focused their efforts on internal and external embezzlement schemes resulting in financial loss to the institution, while AML managers primarily sought to protect the institution against money launderers and terrorists through the detection of potentially suspicious activity and potential sanctions violations.

Today, many financial institutions recognize that most perpetrators of fraud schemes seek to launder their ill-gotten gains and most money launderers have committed other frauds. From this perspective, anti-fraud units and AML units have a shared mission that is quite clear – to prevent and detect criminal activity.

1520. What is the financial services industry's view on merging AML and anti-fraud activities?

Conceptually, the idea of merging AML and anti-fraud activities is widely embraced, but the actual seamless merger of process and technology has yet to be accomplished broadly in the industry today. It is not uncommon for the AML and anti-fraud units to report to the same executive, but "reporting to" and truly leveraging each other in an

established process, leveraging technology across disciplines and from a true financial intelligence perspective are two entirely different things.

1521. What responsibilities could (or typically do) reside in an integrated AML and anti-fraud unit?

SAR filing is an "easy" answer. Clearly there is a benefit to collaboration and not filing duplicative SARS (duplicative in the sense that multiple SARS are being filed on the same customer for essentially the same suspicious activity). Another "easy" example is case management. Simply, it is hard to conceive of a reason to not have a common case management system. Cross channel alerts, as discussed previously, benefit both groups and should be a shared activity.

1522. How do the backgrounds and experience of AML and anti-fraud personnel compare?

Both AML and anti-fraud professionals are knowledgeable in relevant laws and regulations and are adept at conducting research, completing complex analytics, interviewing people at all professional levels and writing comprehensive reports. As a result, cross-training individuals between these groups should be relatively easy.

1523. What are examples of policies and procedures which tend to be shared across AML and anti-fraud programs?

AML and anti-fraud programs may share many policies and procedures within financial institutions, whether they operate as one unit or independently. Examples include, but are not limited, to the following:

- Investigative protocols
- Referral of information to law enforcement
- Disbarment/termination of customers for inappropriate activity
- Procedures for the receipt of information
- Due diligence activities and activities concerning the filing of SARs

1524. Have anti-fraud units and AML units within the same financial institution been successful with sharing data mining and other monitoring systems?

Despite the sophistication of data mining used at financial institutions and efforts to consolidate AML and anti-fraud units, the two units do not normally share data mining results and other monitoring systems. Often, AML monitoring systems and fraud detection systems operate on independent platforms. In addition, since the two units often have independent case management systems, more often than not they are unaware of each other's assignments.

1525. Should separate mechanisms exist for the receipt of allegations of money laundering/ terrorist financing and fraud and misconduct?

In keeping with the notion that all frauds may have a money laundering dimension and that money laundering may involve an underlying fraud, it makes sense to have one reporting mechanism for fraud and money laundering allegations.

Regulators and regulations encourage financial institutions to implement a fraud hotline as a confidential communication channel to identify fraud and reduce fraud-related losses. In its guidance to financial institutions, the FDIC, for example, recommends that to minimize inappropriate calls or complaints to the hotline that do not involve wrongdoing, institutions should communicate the hotline's purpose and define guidelines about what types of improprieties are reportable events. However, the FDIC does not explicitly state what violations, improprieties or crimes should be reportable to the hotline.

1526. What are some key challenges to integrating AML and anti-fraud programs?

Some key challenges for merging AML and anti-fraud programs include, but are not limited to, the following:

- Assuming that merging of reporting lines is the same as integrating separate programs. Organizational alignment without process/technology alignment only guarantees that everyone has a common manager and accomplishes little in reality

- Leadership from one or the other discipline may lack the knowledge and experience to manage the area effectively when dealing with issues outside of his/her traditional comfort zone.
- Similarly, management may see one program as more important than the other, and, as a result, may not allocate resources effectively
- Challenges with process redesign
- Cost of implementing technology solutions
- Cultural barriers

If the integration is done thoughtfully and with purpose, however, these challenges can be overcome.

CIP vs. Identity Theft Prevention Program

1527. How is the term "identity theft" defined by the Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003?

Identity theft is defined as fraud committed or attempted using the identifying information of another person without authority.

1528. How is the term "identifying information" defined?

Identifying information is defined as:

- Any name or number that may be used, alone or in conjunction with any other information, to identify a person, including:
    - Name, taxpayer identification number (TIN), Social Security Number (SSN), employer identification number (EIN), date of birth (DOB), official state- or government-issued driver's license number or identification number, alien registration number or government passport number
    - Unique biometric data, such as a fingerprint, voice print, retina or iris image or other unique physical representation
    - Unique electronic identification number, address or route code
    - Telecommunication identifying information or access device

1529. What are some methods of identity theft?

Some methods of identity theft include, but are not limited to, the following:

- Dumpster diving
- Employee/insider theft
- Electronic intrusions or hacking
- Pharming
- Shoulder surfing or browsing social networks for identity or other sensitive information
- Skimming
- Social engineering (e.g., phishing, spyware, keystroke loggers)

1530. What is "pharming"?

Pharming is a method of fraudulently obtaining identity or other sensitive information (e.g., passwords, security answers) by secretly redirecting users from legitimate websites to websites created by scammers.

1531. How is the term “skimming” defined with respect to identity theft?

Skimming is a method of fraudulently obtaining and storing credit/debit card information through the use of computers or specialized card readers in order to re-encode the account information onto the magnetic strips of blank credit/debit cards, which then can be used to make purchases.

1532. What is “phishing”?

Phishing is a method of fraudulently obtaining identity or other sensitive information (e.g., passwords, security answers) by masquerading as a legitimate entity in an electronic communication (e.g., e-mail, spyware). For example, an individual may receive an e-mail that appears to be from his or her bank that requests identity and/or password information under the guise of “verification” purposes.

1533. What are the requirements of an Identity Theft Prevention Program?

A financial institution must implement an Identity Theft Prevention Program (ITPP) to identify, detect, prevent and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts. An ITPP requires the following four basic elements:

- Identification of relevant red flags (i.e., pattern, practice or specific activity that indicates the possible existence of identity theft)
- Implementation of a monitoring program to detect identity theft red flags
- Establishment of appropriate responses to detected red flags to prevent and mitigate identity theft
- Written policies and procedures and periodic updates of the ITPP (e.g., changes to addresses as they relate to identity theft; changes in methods to detect, prevent or mitigate identity theft; changes in the types of accounts offered or maintained; changes in business arrangements, such as mergers, acquisitions, alliances, joint ventures, and service provider arrangements)

Additionally, financial institutions must:

- Obtain approval of the initial ITPP by the board of directors, a committee of the board, or a designated employee at the level of senior management; the financial institution may determine whether ongoing changes to the ITPP require approval by the board of directors/committee/senior management
- Involve the board of directors, a committee of the board, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the ITPP
- Train relevant staff
- Oversee service provider arrangements to ensure the activity of the service provider is conducted in accordance with the financial institution’s ITPP
- Conduct periodic assessments to determine whether the financial institution offers or maintains covered accounts; the assessment should consider the types of accounts offered, the methods of account opening, the methods/channels provided to access accounts and its previous experiences with identity theft

1534. Which institutions are required to implement an ITPP?

The following financial institutions, as defined in the Fair Credit and Reporting Act (FCRA), are required to implement an ITPP:

- Banks
- Savings and loan associations
- Mutual savings banks
- Credit unions
- Any person who directly or indirectly holds a transaction account belonging to a consumer and creditors (i.e., persons who participate in a credit decision, including those who arrange for the extension, renewal or continuation of credit, which in some cases could include third-party debt collectors or brokers)

Applicability of the Red Flags Rule to depository banks is fairly clear, and these institutions have been required to comply with the final Red Flags Rule since November 2008. In December 2010, the ITPP amended the definition of

"creditor" to include creditors who regularly, and in the ordinary course of business, meet one of three general criteria. They must:

- Obtain or use consumer reports in connection with a credit transaction;
- Furnish information to consumer reporting agencies in connection with a credit transaction;
- Advance funds to, or on behalf of, someone, except for funds for expenses incidental to a service provided by the creditor to that person.

1535. How is the term "transaction account" defined?

The term "transaction account" is defined by the Federal Reserve Act as a "deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers or other similar items for the purpose of making payments or transfers to third persons or others (e.g., demand deposits, negotiable orders of withdrawal accounts, savings deposits subject to automatic transfers, share draft accounts)."

1536. How is the term "covered account" defined?

A covered account is defined as:

- An account primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions
- Any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution from identity theft

1537. Are covered accounts limited to consumer accounts only?

No. Although identity theft occurs more frequently in consumer accounts than commercial accounts, the ITPP is not limited to consumer accounts. Financial institutions are expected to take a risk-based approach in identifying other types of accounts beyond consumer accounts that should be covered under the ITPP (e.g., small business accounts).

1538. How is the term "service provider" defined?

A service provider is a person who provides a service directly to the financial institution. A financial institution is ultimately responsible for complying with the ITPP requirement even if it outsources an activity (e.g., account opening) to a service provider.

1539. How can a financial institution detect identity theft red flags?

A financial institution can do the following to detect identity theft red flags:

- Obtain and verify identifying information at account opening
- Authenticate customers
- Monitor transactions
- Verify the validity of change of address requests

1540. What is a "notice of address discrepancy"?

A notice of address discrepancy is a notice sent to a user by a consumer reporting agency that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

Upon receipt of a notice of address discrepancy, users (e.g., card issuers) are required to develop and implement policies and procedures to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report (e.g., comparison of the information in the consumer report against the information maintained on the consumer).

1541. What are some examples of “appropriate responses” to the detection of identity theft red flags?

Some examples of appropriate responses include (depending upon the circumstances presented), but are not limited to, the following:

- Contacting the customer
- Changing passwords, security codes or other security devices that permit access to an account
- Reopening an account with a new account number
- Not opening a new account
- Closing an existing account
- Not attempting to collect on a covered account or not selling a covered account to a debt collector
- Notifying law enforcement
- Filing a Suspicious Activity Report (SAR)
- No response

1542. Does the ITPP require the use of any specific technology or systems?

No. The ITPP does not require the use of any specific technology or systems to detect identity theft.

1543. What other legal requirements should a financial institution consider when implementing its ITPP?

A financial institution should consider related legal requirements when implementing its ITPP that include, but are not limited to, the following:

- Filing of SARs
- Implementation of limitations on the extension of credit when fraud is detected
- Implementation of requirements for furnishing of information to consumer reporting agencies to correct or update inaccurate or incomplete information and to not report information that the financial institution has reasonable cause to believe is inaccurate
- Complying with prohibitions on the sale, transfer and placement for collection of certain debts resulting from identity theft

1544. Where can a financial institution obtain examples of red flags for identity theft?

An appendix to the Red Flags Rule provides a list of nonexclusive red flags that should be considered when performing an ITPP risk assessment. The red flags are organized into the following categories:

- Alerts, notifications or warnings from a consumer reporting agency
- Suspicious documents
- Suspicious personal identifying information
- Unusual use of or suspicious activity related to the covered account
- Notice from customers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft

1545. How is the ITPP different from the Customer Identification Program?

The ITPP and the Customer Identification Program (CIP) differ in the following manner:

- CIP is limited to new customers only
- CIP requires a one-time verification at account opening
- CIP requires verification of four elements: name, DOB, physical address and TIN

- ITPP applies to both new and existing customers
- ITPP requires monitoring of identifying information beyond what is included in CIP
- ITPP requires ongoing monitoring of existing customers, not just new customers
- ITPP is concerned with both verification of identifying information and authentication

For further guidance on CIP, please refer to Section 326 – Verification of Identification.

1546. What is the difference between identity theft and identity fraud?

Identity theft involves the theft of another person's identifying information, whereas identity fraud involves the use of false identifying information that may or may not belong to someone else (e.g., a fabricated SSN).

1547. What is the difference between "verification" and "authentication"?

Verification confirms that the information provided by a customer is valid (e.g., an individual with the provided name, address and TIN matches with an independent source, such as a credit reporting database).

Authentication attempts to ensure that the individual providing the information, or accessing the account(s), is the person he or she claims to be. Authentication is accomplished by requesting information that is not necessarily "found in a wallet" (e.g., previous address, previous employer). Often, once an individual has been verified, financial institutions will ask customers to create custom security questions (e.g., mother's maiden name, favorite movie, pet's name) that serve to authenticate customers.

(For additional guidance on identity theft and other privacy issues, please read *The Global Privacy and Information Security Landscape: Frequently Asked Questions*, a guide that covers information security, privacy trends, security breaches, privacy programs, guidance for victims of identity theft, and key laws and regulations, including the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, the European Union General DP Directive, and the Electronic Communications Privacy Act.)

1548. What key guidance has been provided on identity theft?

The following key guidance has been provided on identity theft:

- **Interagency Guidelines on Identity Theft Detection, Prevention and Mitigation** (2010) by the FFIEC
- **Guidance to Assist Financial Institutions with Identifying and Reporting Account Takeover Activity** (2011) by FinCEN
- **Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems** (2012) by the Financial Action Task Force (FATF)
- **Authentication in an Internet Banking Environment** (2005) by the FFIEC
- **Advisory: Tax Refund Fraud and Related Identity Theft** (2012) by FinCEN
- **FinCEN Study Examines Rise in Identity Theft on SARs** (2010) by FinCEN
- **FinCEN Examines Identity Theft-Related SARs Filed by Securities & Futures Firms** (2011) by FinCEN

Mortgage Fraud

1549. How is the term "mortgage fraud" defined?

Mortgage fraud is generally defined as any material misstatement, misrepresentation or omission relied upon by an underwriter or lender to fund, purchase or insure a loan.

There are two types of mortgage fraud: fraud for housing/property and fraud for profit. The former typically involves misstatements about income, debt or property value by the borrower in order to qualify for a mortgage in which he/she usually intends to pay. The latter typically involves collusion among industry professionals involved in the mortgage process (e.g., mortgage brokers, real estate agents, appraisers, attorneys, title examiners) in order to qualify for a mortgage and generate a profit with no intention to pay the mortgage. Profits can be generated in multiple ways, such as by obtaining a mortgage and not paying it back or by flipping properties with inflated property

values. In both types of mortgage fraud, lenders may extend credit that the lender would likely not have offered if the true facts were known.

1550. Which types of loan products typically have been used in mortgage fraud schemes?

A variety of loan products have been used in mortgage fraud schemes, including purchase loans, refinancing, home equity, second trust and construction loans. Over the last couple of years, there has been a significant increase in new mortgage fraud schemes involving distressed loans of all types.

1551. What are some examples of mortgage fraud schemes?

Some common schemes include, but are not limited to, the following:

- **Occupancy Fraud** – A borrower wants to obtain a mortgage on an investment property, but claims on his/her application that he/she will occupy the house in order to obtain a better interest rate than is warranted.
- **Property Flipping** – Property is purchased, falsely appraised at a higher value, and then quickly sold.
- **Property Flopping** – Foreclosed property is sold at an artificially low price to a straw buyer, who then sells the property at a higher price and pockets the difference.
- **Income Fraud** – Particularly during the period of lax underwriting standards that existed between approximately 2004 and 2007, many borrowers who could not qualify for loans based on their verified income chose – or were encouraged by unscrupulous brokers or lenders – to apply for stated income loans, and provided income amounts significantly in excess of what they actually earned in order for their applications to be approved. (This is discussed further below.) Income fraud also includes borrowers understating income to qualify for hardship concessions and modifications.
- **Failure to Disclose Liabilities** – Prospective borrowers may attempt to conceal certain financial obligations, such as other mortgages or credit card debt in an effort to try and reduce the appearance of recurring debt. This omission of liabilities helps to artificially lower the debt-to-income ratio (which is used by lenders in order to help quantify how much a prospective borrower may qualify for), in the hope of qualifying for a larger loan.
- **Occupation/Employment Fraud** – This type of fraud is significantly on the rise, as unemployment levels increase as a result of the economic crisis. Prospective borrowers may claim self-employment in a nonexistent company; may claim a higher position; or may claim that they still hold their previous position, to facilitate falsifying income.
- **Silent Second** – The buyer of a property borrows the down payment from the seller through the issuance of a non-disclosed second mortgage; the primary lender believes the borrower has invested his/her own money in the down payment and therefore, approves a mortgage for a borrower who typically would not have been approved.
- **Nominee Loan/Straw Borrower** – The identity of the borrower is concealed through the use of a nominee, and the borrower uses the nominee's name and credit history to apply for a loan. Sometimes, the nominee is a willing participant in the scheme. It is considered identity theft in instances in which the nominee is not a willing participant.
- **Asset Rental Fraud** – A borrower "rents" assets by temporarily depositing funds into his/her account to inflate the stated value of his/her assets in order to qualify for a mortgage. Funds are withdrawn after the borrower qualifies for the mortgage. In some instances, the borrower pays a "rental fee" for the borrowed assets.
- **Cash-Back Fraud** – This is frequently seen as part of money laundering activity, where the price of a property is illegally inflated, such that parties involved in the sale are eligible for "cash back" which is not disclosed to the lender.
- **Shotgunning** – A property owner applies for home equity loans with multiple lenders at the same time, and the lenders may not be aware of the other loans (e.g., lenders may not report to the same credit bureau, lag in reporting to credit bureaus); or a property owner, who may not be the rightful owner, sells the same property multiple times to different buyers.
- **Air Loans** – Nonexistent property loans where there is usually no collateral and often no real borrower.
- **Appraisal Fraud** – This type of fraud occurs when a borrower overstates home value to obtain more money from a sale or refinancing, or understates home value to purchase property at a lower cost. In instances when a home's value is overstated, more money can be obtained by the borrower in the form of a cash-out refinance. Additionally, identity theft can facilitate mortgage fraud, when an individual applies as a would-be borrower under

a stolen identity. For additional guidance on identity theft-related fraud, please refer to the CIP vs. Identity Theft Prevention Program section.

1552. What are some of the factors that give rise to mortgage fraud?

There are a number of variables that may contribute to the occurrence of mortgage fraud including greed, as people look for "get-rich-quick" opportunities, and economic/personal financial conditions that may prompt individuals, or groups of individuals, to commit mortgage fraud. Indicators of these variables may include:

- Loan delinquencies
- Defaults
- Foreclosures
- Poor credit
- Unemployment
- Increases in negative equity
- Overall housing prices and availability of properties

1553. What are some vulnerabilities that increase the fraud risks of the mortgage industry?

Some vulnerabilities of the mortgage industry include, but are not limited to, the following:

- Non-face-to-face/automated loan processing channels (e.g., Internet, telephone)
- Innovative loan products (e.g., interest-only loans, no- or low-documentation products, adjustable-rate mortgages) and subprime loans
- Applications taken by entities other than regulated financial institutions (e.g., mortgage brokers)
- Involvement and abuse by, and possible collusion among, multiple third parties (e.g., borrower, mortgage broker, real estate agent, appraiser, underwriter, lender, closing/settlement agent)

For a list of red flags, please refer to the Lending Red Flags and Mortgage and Real Estate Red Flags sections.

1554. What resources and guidance are available on mortgage fraud?

As the prevalence of mortgage fraud continues to increase, so do law enforcement's efforts to prevent and detect mortgage fraud. As a result, organizations such as the U.S. Federal Bureau of Investigation (FBI), the Financial Crimes Enforcement Network (FinCEN), and the Financial Fraud Enforcement Task Force (FFETF) have developed websites and annual reports intended to provide both the industry and consumers with valuable information about the extent of mortgage fraud:

- **FFETF** – In 2009, the FFETF was created in order to develop a working group (or multiple working groups) all operating toward the same goal of improving government efforts to identify, investigate, prosecute and prevent various financial crimes. With the rise in fraudulent scams related to the mortgage industry, this particular financial crime has been a significant area of focus for the FFETF. While the resources offered by the FFETF, available on its website, are largely aimed at protecting consumers against being victims of fraud, the information can also be leveraged by the industry to help stay apprised of ongoing developments in mortgage-related fraud, as well as efforts to combat this activity. This includes press releases and news articles of recent investigations and prosecutions, the FFETF's annual report publication, and links to other agencies also involved in the prevention of mortgage fraud (e.g., the U.S. Department of Housing and Urban Development). (http://www.stopfraud.gov/about.html)
- **FBI** – The FBI has developed a website, which provides access to both general information about mortgage fraud, as well as analytics reports dating back to 2006, coverage of recent incidents of identified mortgage fraud, details about key and emerging mortgage fraud scams, and potential ways to prevent consumers from becoming the target of mortgage fraud. (http://www.fbi.gov/about-us/investigate/white_collar/mortgage-fraud/mortgage_fraud)
- **FinCEN** – FinCEN, as a member of the FFETF, has a page on its website that is solely dedicated to providing information (both to the industry as well as consumers) about mortgage fraud. The website provides access to detailed reports, which similar to the FFETF and FBI reports, highlight new trends in mortgage fraud prevalence. There is also detailed information available regarding the number of Suspicious Activity Reports (SARs) filed

relating to mortgage fraud and trends in the volume of mortgage fraud, ongoing investigations, and multiagency crackdowns. (http://www.fincen.gov/news_room/rp/mortgagefraud.html)

Specifically, FinCEN has published the following releases:

- **Mortgage Fraud SAR Data Tables by State, Urban Area and County** (2012)
- **Suspected Mortgage Fraud (Including Quarterly Written Reports)** (2012)
- **Suspected Money Laundering and Fraud in the Residential Real Estate Industry** (2012)
- **Suspected Money Laundering and Fraud in the Commercial Real Estate Industry** (2011)
- **Home Equity Conversion Mortgages (Reverse Mortgages)** (2012)
- **Mortgage Fraud Cases Supported by FinCEN Filings** (2012)
- **Foreclosure Rescue Scams & Loan Modification Fraud** (2009)
- **Multi-Agency Crackdown Targeting Foreclosure Rescue Scams, Loan Modification Fraud** (2009)
- **Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding Loan Modification/Foreclosure Rescue Scams** (2009)
- **Mortgage Loan Fraud Update: Suspicious Activity Report Filings from July 1-September 30, 2009**
- **Mortgage Loan Fraud Update** (published in *The SAR Activity Review* – Trends, Tips & Issues (Issue 16, October 2009)
- **Suspicious Activity Related to Mortgage Loan Fraud** (August 16, 2012)
- **FinCEN Assesses Suspicious Activity Involving Title and Escrow Companies** (2012)
- **California, Nevada, Florida Top Mortgage Fraud SAR List** (2012)
- **FinCEN Attributes Increase in Suspicious Activity Reports Involving Mortgage Fraud to Repurchase Demands** (2012)
- **Mortgage Loan Fraud Connections with Other Financial Crime** (2009)
- **Filing Trends in Mortgage Loan Fraud** (2007)
- **Mortgage Loan Fraud: An Update of Trends Based Upon an Analysis of Suspicious Activity Reports** (2008)
- **Mortgage Loan Fraud Assessment** (2006)
- **Mortgage Fraud Report: SAR Filings Up; Potential Abuse of Bankruptcy Identified** (2010)

1555. Is mortgage fraud typically perpetrated at certain stages in the lending process?

Mortgage fraud can occur at any stage in the mortgage lending process and can involve any of the following market participants:

- Licensed/registered and non-licensed/registered mortgage brokers
- Lenders
- Appraisers
- Underwriters
- Accountants
- Real estate agents
- Settlement attorneys
- Land developers
- Investors
- Builders

- Bank account representatives and trust account representatives
- Organized criminal groups

Additionally, individuals applying for mortgages can be perpetrators of mortgage fraud, even though they may not be involved in the loan administration process.

1556. Are financial institutions required to report suspected mortgage fraud on SARs?

Yes. Financial institutions are required to report suspected mortgage fraud on SARs. According to FinCEN, in 2011, financial institutions submitted 92,028 SARs related to mortgage lending fraud, up 31 percent from 2010. These SARs accounted for 11 percent of all SARs in 2011 and 10 percent of all SARs in 2010. The fourth quarter of 2011 did show a decline of 9 percent from the same period the year before.

For 2011, 84 percent of mortgage fraud activity reported in SARs occurred more than two years prior to the SAR filing, compared to 77 percent in 2010. For 2011, a majority of reported activities actually began during or before 2007. Forty percent of SARs filed for mortgage loan fraud indicate that the filer turned down the requested loan or debt elimination attempt, indicating, according to FinCEN, that financial institutions are becoming much more proactive when reviewing borrowers' documents and increasing their due diligence standards.

Hot spots for mortgage fraud included California, Florida, Illinois and New York by volume, and California, Hawaii, Florida and Nevada per capita.

1557. What are the most common types of mortgage loan fraud reported in SAR filings?

According to the FinCEN's *Mortgage Loan Fraud Update: Suspicious Activity Report Filings*, published in April 2012, and its Q4 2011 *SAR Activity Review – By the Numbers* publication, suspicious activities include, in descending order of frequency:

- Occupancy fraud (21 percent)
- Income fraud (18 percent)
- Appraisal fraud (12 percent)
- Employment fraud (12 percent)
- Short sale fraud (10 percent)
- Liability fraud (9 percent)
- Debt elimination scheme (9 percent)
- Social Security Number fraud (7 percent)
- Identity theft (2 percent)

1558. Do mortgage lenders and originators have any AML requirements?

Yes. Residential mortgage lenders and originators (RMLOs) are subject to a rule published in February 2012 – the Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Residential Mortgage Lenders and Originators. Institutions covered by this rule were required to comply by August 13, 2012.

For additional guidance on the AML requirements for nonbank RMLOs, please refer to the Nonbank Residential Mortgage Lenders and Originators section.

1559. Are any other AML requirements under consideration with regard to participants in the mortgage market?

Yes. Due to the rise in abusive and fraudulent sales and financing practices in both the primary and secondary residential mortgage markets, FinCEN issued the following:

- Final rule "Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Residential Mortgage Lenders and Originators" in August 2012;
- Notice of proposed rule "Anti-Money Laundering Program and Suspicious Activity Report Requirements for Housing Government-Sponsored Enterprises" in November 2011; and

- Advance notice of proposed rulemaking (ANPR) "Persons Involved in Real Estate Closings and Settlements" in April 2003.

Together, these regulations, along with the requirements for RMLOs, are expected to increase the number of SAR filings from the mortgage industry and provide regulators and law enforcement with more information on mortgage fraud.

The proposed rule would require Housing GSEs to comply with Section 352 – AML Program of the USA PATRIOT Act, which requires the following:

- Development of written internal policies, procedures, and controls;
- Designation of an AML compliance officer;
- Ongoing AML employee training program; and
- Independent testing of the AML Compliance Program.

The proposed rule would also require Housing GSEs to file SARs. For further guidance on SAR filing requirements, please refer to the Suspicious Activity Report section.

Currently, the ANPR for "Persons Involved in Real Estate Closing and Settlements" suggests that these individuals and entities would also be required to implement an AML program, and sought to solicit public comment on the extent to which money laundering program laws and requirements should apply to persons involved in real estate closings and settlements. To date, no further action has been taken regarding the ANPR and public comments received.

For further guidance, please refer to the Nonbank Residential Mortgage Lenders and Originators, Housing Government Sponsored Enterprises and Persons Involved in Real Estate Closing and Settlements sections.

Unlawful Internet Gambling Enforcement Act

1560. What is Internet gambling?

Simply put, Internet gambling is the online wagering of money or other value. Other terms used include online gambling and the more comprehensive term, remote gambling, which includes gambling through the use of remote communications such as the Internet, smartphone, telephone, radio and television.

1561. How big is the global Internet gambling market?

As of 2012, some estimates suggest that the global Internet gambling market is approximately $30 billion, with rapid growth projected in coming years. Approximately 85 countries permit and license various forms of online gambling.

1562. How big is the U.S. Internet gambling market?

For 2012, it has been estimated that the U.S. Internet gambling market is approximately 15 percent of the global market, or approximately $4 billion to $5 billion.

1563. What is "unlawful Internet gambling"?

Under the U.S. Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA), unlawful Internet gambling includes placing, receiving or otherwise knowingly transmitting a bet or wager by any means that involves the use, at least in part, of the Internet, where such bet or wager is unlawful under any applicable federal or state law in the state or tribal land in which the bet or wager is initiated, received or otherwise made. The term does not include certain bets or wagers that are excluded under the Act as an intrastate transaction or an intra-tribal transaction, and does not include any activity that is allowed under the Interstate Horseracing Act of 1928. The intermediate routing of electronic data does not determine the location or locations in which a bet or wager is initiated, received or otherwise made.

1564. Are there any exemptions to "unlawful Internet gambling" under the UIGEA?

The UIGEA exempts participation in any game or contest in which participants do not stake or risk anything of value other than personal efforts of the participants in playing the game or contest or obtaining access to the Internet, or points or credits that the sponsor of the game or contest provides to participants free of charge and that can be used or redeemed only for participation in games or contests offered by the sponsor.

The UIGEA also exempts participation in any fantasy or simulation sports game or educational game or contest in which (if the game or contest involves a team or teams) no fantasy or simulation sports team is based on current membership of an actual team that is a member of an amateur or professional sports organization and meets each of the following conditions:

- All prizes and awards offered to winning participants are established and made known to the participants in advance of the game or contest and their value is not determined by the number of participants or the amount of any fees paid by those participants;
- All winning outcomes reflect the relative knowledge and skill of the participants and are determined predominantly by accumulated statistical results of the performance of individuals (athletes in the case of sports events) in multiple real-world sporting or other events; and
- No winning outcome is based on the score, point spread or any performance(s) of any single real-world team or any combination of teams, or solely on any single performance of an individual athlete in any single real-world sporting or other event.

The law also exempts the following:

- Deposits or transactions with insured depository institutions
- Contracts for insurance, indemnity or guarantee
- Certain other transactions governed by securities or commodity laws

1565. Are there other U.S. laws addressing Internet gambling?

On a federal level, the Interstate Wire Act of 1961 (Wire Act), also referred to as the Federal Wire Act, prohibits the use of a wire communication facility (e.g., Internet) for the transmission of sports bets or wagers or information assisting in the placement of such bets or wagers. However, the U.S. Department of Justice recently indicated that the scope of the Wire Act's prohibition is limited to sports betting.

The Professional and Amateur Sports Protection Act of 1992 (PASPA) prohibits sports wagering in all states except those with pre-existing operations (i.e., Delaware, Montana, Nevada, Oregon).

Other key gambling regulations and statutory provisions include the Travel Act of 1961, Interstate Transportation of Wagering Paraphernalia Act of 1961, Illegal Gambling Business Act of 1970, Racketeer Influenced and Corrupt Organizations Act of 1970, Interstate Wagering Amendment of 1994, Amendment to Interstate Horseracing Act, Illegal Money Transmitting Business Act of 1992, Gambling Ship Act, and the Indian Gaming Regulatory Act.

Additionally, some states have enacted laws that specifically prohibit certain Internet gambling activities.

As previously noted, however, there is no common definition of Internet gambling, so the legality or illegality of some activities must be determined based on the particular facts.

1566. Have any U.S. states legalized Internet gambling?

While the United States has enacted federal legislation to prohibit "unlawful Internet gambling," the U.S. Department of Justice indicated in a 2011 ruling that, with exception to sports wagering, individual states have the authority to determine whether to legalize intrastate online gambling.

New Jersey became the first state to legalize certain forms of Internet gambling. At the time of this publication, a number of states were in the process of attempting to legalize online gambling, including California and Nevada.

State lawmakers face a number of obstacles in attempting to pass legislation, including the potential difficulties in enforcing and monitoring appropriate compliance with online gambling regulations as well as possible interference with gambling conducted across state borders with varying legalities.

1567. Does the UIGEA have any applicability outside of the United States?

Foreign-located Internet gambling providers are prohibited from providing illegal Internet gambling services to U.S. customers if transactions are processed through a domestic payment processor.

The UIGEA encourages the cooperation of foreign governments and the Financial Action Task Force (FATF) in sharing information on Internet gambling and related abuses. Many countries have begun to implement Internet gambling laws of their own, ranging from restricting activities similar to the UIGEA to regulating the industry.

Certain foreign countries have challenged whether the United States can prevent Internet gambling.

1568. What challenges have been made to the UIGEA?

Challenges to the UIGEA have been made both domestically and internationally. Since the passage of the UIGEA, several members of the U.S. Congress have pushed for a regulated U.S. gaming environment, as have the 85 countries that license and permit certain types of online gambling, or a full repeal of the UIGEA. iMEGA, the Interactive Media Entertainment and Gaming Association, challenged the law in U.S. federal court, stating that the UIGEA was unconstitutional. iMEGA lost their case in 2009.

In 2005, Antigua accused the United States of protectionism and filed a complaint with the World Trade Organization (WTO). In 2006, the WTO ruled that the United States was in violation of the 1995 General Agreement on Trade and Services (GATS) Treaty, which committed to allowing foreign entrants into the online gaming market. After the passage of the UIGEA in 2006, the WTO maintained that this law continued to violate the GATS Treaty.

1569. Since various forms of gambling are permitted in the United States, why is Internet gambling a concern?

Those concerned about Internet gambling cite the following reasons:

- Potential for fraud, such as identity theft, over the Internet
- Children's access to gambling sites
- 24/7 access, which facilitates "problem gambling"
- Money laundering risks

1570. How does the UIGEA aim to prevent illegal Internet gambling?

The UIGEA of 2006 made it a criminal offense for persons engaged in the business of betting or wagering to knowingly accept payments in connection with the participation of another person in unlawful Internet gambling. It required the U.S. Treasury Department and the Federal Reserve Board to promulgate regulations requiring certain participants in the payment systems and financial transaction providers participating in such systems to have policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions.

Since the UIGEA was enacted in October 2006, and the U.S. Treasury Department and Federal Reserve Board published a proposed rule in October 2007 and a final rule in November 2008, the effective date for compliance for designated participants within specified payment systems was deferred until June 1, 2010, under the Prohibition on Funding of Unlawful Internet Gambling (Regulation GG).

1571. Which payment system participants are required to have policies and procedures to prohibit the processing of prohibited transactions?

Under the joint rule issued by the U.S. Treasury Department and the Federal Reserve Board, Regulation GG, the following payment systems are designated participants:

- **Automated clearing house (ACH) systems**. However, the participants processing a particular transaction through an automated clearing house system are exempt from the Act's requirements for establishing written policies and procedures, except for:
    - The receiving depository financial institution and any third-party processor receiving the transaction on behalf of the receiver in an ACH credit transaction;
    - The originating depository financial institution and any third-party processor initiating the transaction on behalf of the originator in an ACH debit transaction; and
    - The receiving gateway operator and any third-party processor that receives instructions for an ACH debit transaction directly from a foreign sender (which could include a foreign banking office, a foreign third-party processor, or a foreign originating gateway operator).
- **Card systems**, which are defined as a system for authorizing, clearing and settling transactions in which credit cards, debit cards, prepaid cards or stored-value cards (such cards being issued or authorized by the operator of the system) are used to purchase goods or services or to obtain a cash advance. The term includes systems both in which the merchant acquirer, card issuer and system operator are separate entities and in which more than one of these roles are performed by the same entity.

- **Check collection systems**. However, the participants in a particular check collection transaction through a check collection system are exempt from the Act's requirements for establishing written policies and procedures, except for the depositary bank.
- **Money transmitting businesses**, solely to the extent they: (1) engage in the transmission of funds, which does not include check cashing, currency exchange, or the issuance or redemption of money orders, traveler's checks and other similar instruments; and (2) permit customers to initiate transmission of funds transactions remotely from a location other than a physical office of the money transmitting business. The participants in a money transmitting business are exempt from the Act's requirement to establish written policies and procedures, except for the operator.
- **Wire transfer systems**. However, the participants in a particular wire transfer through such a system are exempt from the Act's requirement to establish written policies and procedures, except for the beneficiary bank.

These designated participants in the aforementioned payments systems are collectively referred to herein as "covered participants." For additional guidance on payment processors, please refer to the Third-Party Payment Processors section.

1572. Are any covered participants exempt from the requirement to have policies and procedures?

Yes, as detailed above, certain types of participants are exempt from establishing written policies and procedures, depending on their roles in the processing of transactions.

1573. Are customers of covered participants also subject to Regulation GG?

No. Regulation GG imposes the obligations to establish and implement written policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions on nonexempt participants in designated payment systems, not the customers of designated participants.

However UIGEA prohibits any person engaged in the business of betting or wagering from knowingly accepting payments in connection with the participation of another person in unlawful Internet gambling, and that other federal and state laws prohibiting illegal Internet gambling can apply directly to customers, and other parties to the transaction.

1574. What types of policies and procedures does Regulation GG require covered payment systems participants to develop and maintain?

Participants are required to develop and maintain written policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions. They may be customized to their businesses, and it is likely such policies and procedures may differ across different business lines. The focus of the policies and procedures is intended to be on the due diligence that financial institutions and third-party payment processors should conduct when deciding to establish and maintain commercial customer accounts.

A covered participant can be considered to be in compliance with the requirement to have such policies and procedures if it relies on and complies with the written policies and procedures of the designated payment system that are reasonably designed to identify and block restricted transactions, or otherwise prevent or prohibit the acceptance of the products or services of the designated payment system or participant in connection with restricted transactions, and such policies and procedures of the designated payment system comply with the law's requirements.

The implementing regulation to the Act, Regulation GG, provides that a covered party's procedures meet the standard of being reasonably designed if they include:

- Specified due diligence of its commercial customer accounts or commercial customer relationships including, but not limited to, the conducting of due diligence of a commercial customer and its activities at the time of establishment of the account or relationship commensurate with the participant's judgment of the risk of restricted transactions presented by the customer's business;
- Specified notice be given to all commercial customers;
- The participant (on the basis of its due diligence) is able to make a determination that the customer presents a minimal risk of engaging in an Internet gambling business; or

- If it is not able to reach such a determination through its due diligence, it obtains specified documentation, such as evidence of legal authority to engage in such business.

1575. What are card systems expected to do?

The policies and procedures of a card system operator, a merchant acquirer, third-party processor or a card issuer are deemed to be reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions if the policies and procedures provide for specified methods to conduct due diligence or implement a code system (e.g., transaction codes and merchant/business category codes) that are required to accompany the authorization request for a transaction (that must include specified functionality).

Additionally, the card system operator, merchant acquirer or third-party processor needs to have procedures to be followed when the participant has actual knowledge that a merchant has received restricted transactions through the card system, including but not limited to:

- Circumstances under which the merchant account should be closed; and
- Circumstances under which the access to the card system for the merchant, merchant acquirer or third-party processor should be denied.

1576. What are sufficient policies for money transmitters?

Money transmitters have reasonably designed policies and procedures if they:

- Address methods for the operator to conduct due diligence in established commercial customer relationships as set forth in the regulations;
- Address due diligence methods to be used where there is actual knowledge that an existing commercial customer engages in an Internet gambling business (as set forth in the regulations);
- Include procedures regarding ongoing monitoring or testing by the operator to detect potential restricted transactions, such as monitoring and analyzing payment patterns to detect suspicious payment volumes to any recipient; and
- Include procedures to be followed when the operator has actual knowledge that a commercial customer of the operator has received restricted transactions through the money transmitting business, that address the circumstances under which the money transmitting services should be denied to the commercial customer and the circumstances under which the account should be closed.

1577. What types of policies and procedures does Regulation GG expect covered participants to develop and implement?

Regulation GG contemplates that covered participants will develop and maintain policies and procedures addressing the following:

- Notices to new and existing commercial account holders that restricted transactions are prohibited from being processed through the account or relationship.
- Due diligence procedures designed to determine the following:
    - Whether a commercial customer poses minimal risk.
    - In the event the participant is unable to determine that the commercial customer poses only minimal risk, the financial institution must require:
        - A certification from the customer stating that it does not engage in Internet gambling or, if it does, a commercial license from a state or tribal authority authorizing the customer to engage in the business or a reasoned legal opinion (as defined in the regulation) that such activity does not involve restricted transactions;
        - A written commitment to report any change in its legal authority to engage in Internet gambling; and
        - A third-party certification that the customer's systems for engaging in Internet gambling are reasonably designed to ensure the customer will remain within legal limits.

1578. What if a covered participant has actual knowledge that a commercial customer is engaging in Internet gambling?

If a covered participant has actual knowledge that a commercial customer is engaging in Internet gambling, then the participant should obtain the documentation outlined in its policies and procedures:

- Evidence of legal authority to engage in such business (e.g., commercial license);
- Legal opinion that such activity does not involve restricted transactions;
- Written commitment to report any change in its legal authority; or
- Third-party certification that the customer's systems for engaging in Internet gambling are reasonably designed to ensure the customer will remain within legal limits.

The purpose of obtaining this documentation is to assist the covered participant in distinguishing between customers who engage in Internet gambling and those who conduct restricted transactions in violation of the UIGEA.

1579. What if a covered participant has actual knowledge that a customer is conducting restricted transactions?

Where it has knowledge that the customer is conducting restricted transactions, covered participants are expected to have policies and procedures to address continued transaction processing, account review, suspicious activity report (SAR) filing, and account closure.

1580. Since most covered participants are not expected to collect information proactively to identify restricted activities, how would participants acquire actual knowledge?

A participant may receive information about the transactions and their illegality from a source such as a government agency or may identify such transactions during the course of its usual business and compliance practices.

1581. Does Regulation GG provide any safe harbor to covered participants?

Yes, the rule gives examples of policies and procedures that constitute a safe harbor for compliance for each type of payment system. Also, a person who identifies and blocks a transaction, prevents or prohibits the acceptance of its products or services in connection with a transaction, or otherwise refuses to honor a transaction, shall not be liable to any party if:

- The transaction is a restricted transaction;
- Such person reasonably believes the transaction to be a restricted transaction; or
- The person is a participant in a designated payment system and blocks or otherwise prevents the transaction in reliance on the policies and procedures of the designated payment system in an effort to comply with the regulation.

1582. If an operator-driven system, such as a card system, has policies and procedures in place to comply with the UIGEA regulation, can participants in those systems leverage these policies and procedures?

The rule provides that participants in operator-driven systems may develop their own policies and procedures or may rely on and comply with conforming policies and procedures of the system operator. The participant may rely on a written statement or notice from the operator-driven system that its policies and procedures are designed to comply with the rule and may rely on these policies and procedures until and unless it is notified by its regulator that the policies and procedures are noncompliant.

1583. Which regulators are responsible for enforcing Regulation GG?

Enforcement is the responsibility of designated federal functional regulators; if no such regulator exists, the Federal Trade Commission (FTC) is responsible for enforcement.

1584. What are the consequences for not complying with the UIGEA?

A violation of the UIGEA can result in fines, up to five years imprisonment, or both, and a permanent injunction preventing the person from making or receiving bets or wagers. Additional other penalties and fines (including civil or

criminal) may be imposed under other federal or state laws. Financial institution regulators may impose additional sanctions.

1585. What is the relationship of the UIGEA to the Bank Secrecy Act (BSA)/AML compliance?

UIGEA compliance is separate and distinct from BSA/AML compliance, though customer due diligence is a tenet of both. Compliance with the UIGEA does not fulfill any other BSA/AML compliance requirement, such as the requirement to file SARs. For further guidance on BSA/AML requirements, please refer to the sections: Bank Secrecy Act and the USA PATRIOT Act.

1586. Have any companies been indicted for violations of the UIGEA?

Yes. In 2007, the first indictment for a violation of the UIGEA was against NETeller, an international money transmitter that offers online payment services to businesses and individuals. Several million dollars in customer funds were seized by the U.S. Department of Justice (DOJ) and returned to customers only after NETeller agreed to forfeit $136 million as part of a deferred prosecution agreement. Since then, NETeller has exited the U.S. market.

In 2011, three of the largest online poker companies were charged with violations of the UIGEA. The federal government shut down approximately 76 bank accounts in more than 14 countries totaling over $500 million in assets. These cases included Fultilt Poker (Ireland), Pokerstar (Isle of Man) and Absolute Poker (Costa Rica). All three companies were charged with fraud and money laundering. At the time of the bust, the domain names were initially seized but have since been returned.

1587. How did companies circumvent controls established by the UIGEA?

The following is one example of how poker companies allegedly circumvented the controls established by the UIGEA:

- Poker companies began using third-party payment processors (TPPPs) to deceive covered financial institutions by disguising Internet gambling payments as those made by phony businesses and websites.
- Specifically, the poker companies began to make unlawful payments to the TPPPs in order to compensate and persuade them to lie to financial institutions with regard to the nature of these payments.
- Poker companies worked with TPPPs to apply incorrect transaction codes to the Internet gambling transactions.
- Poker companies not only utilized credit cards, but also stored value cards and ACH transactions:
    - **Credit cards** – Phony companies established Visa and merchant processing accounts with offshore banks.
    - **Stored value cards** – Customers would purchase stored value cards from the phony companies.
    - **ACH** – Poker processors opened accounts in the name of the phony companies and processed fraudulent e-checking transactions.
- Small regional banks facing financial hardships were also allegedly bribed to participate in these schemes

1588. Do casinos and card clubs have additional obligations to comply with Regulation GG?

No. While casinos and card clubs may pose a higher risk for processing prohibited transactions due to the nature of their business, like any other financial institution or payment processor, they will have to evaluate their business lines for risk and establish appropriate internal controls to mitigate those risks in accordance with UIGEA/Regulation GG.

For additional guidance on the AML requirements of casinos, please refer to the Casinos and Card Clubs section.

1589. What are some of the common challenges to complying with the UIGEA/Regulation GG?

The following include some of the challenges that financial institutions and/or payment processors have experienced in complying with the UIGEA/Regulation GG:

- Lack of awareness by business units or departments of applicability to their specific job duties.
- Lack of or inadequate communication and implementation of effective internal policies and procedures in coordination with existing business processes (e.g., correspondent banking monitoring).

- Overreliance on relationship managers' knowledge about the activities of their commercial account holders, thereby leading to inadequate due diligence on commercial customers.
- Lack of incorporation into new or existing risk assessment methodologies for both customers and TPPPs.

Human Trafficking

1590. What is human trafficking?

Human trafficking is sometimes defined as modern slavery. It is the illegal trade of human beings for sexual exploitation or forced labor or services. Further, the physical transportation of victims from one location to another is not required for the crime to fall within the definition of human trafficking.

Human trafficking is the fastest growing criminal industry in the world: The International Labour Office (ILO) estimates that more than US$32 billion are generated annually from human trafficking, half of which is attributable to industrialized countries; and the U.S. Department of State estimates that as many as 27 million people are victims of human trafficking.

Human trafficking often involves, but is not limited to, illegal aliens as victims. It is not a problem exclusive to impoverished and developing nations. The problem of human trafficking and slavery is so widespread that it would be virtually impossible to find a home, school, church or business that doesn't contain slave-tainted goods.

1591. What are the key laws that address human trafficking?

The following U.S. laws establish key definitions and guidelines to combating human trafficking:

- The Victims of Trafficking and Violence Protection Act (TVPA) of 2000
- Trafficking Victims Protection Reauthorization Act of 2003
- Trafficking Victims Protection Reauthorization Act of 2005
- Trafficking Victims Protection Reauthorization Act of 2008

The TVPA laws define "severe forms of trafficking in persons" as:

- Sex trafficking in which a commercial sex act is induced by force, fraud or coercion, or in which the person induced to perform such an act has not attained 18 years of age; or,
- The recruitment, harboring, transportation, provision or obtaining of a person for labor or services, through the use of force, fraud or coercion, for the purpose of subjection to involuntary servitude, peonage, debt bondage or slavery.

The U.S. definition of human trafficking is consistent with the international definition established by the United Nations' Palermo Protocol:

- The Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children;
- The Protocol against the Smuggling of Migrants by Land, Sea and Air; and
- The Protocol against the Illicit Manufacturing and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime.

The international definition consists of three components:

- **Action**: Recruitment, transportation, transfer, harboring or receipt of persons;
- **Means**: Threat or use of force or other forms of coercion, abduction, fraud, deception, abuse of power or position of vulnerability, or giving or receiving of payments or benefits to achieve the consent of a person having control over another person; and
- **Purpose**: For exploitation (e.g., forced labor, prostitution, marriage, organ removal, adoption, etc.).

Washington enacted an anti-human trafficking statute in 2002, becoming the first state to do so. According to the Polaris Project, a nonprofit, non-governmental organization established in 2002 to combat human trafficking, as of

July 31, 2012, the number of states with anti-human trafficking criminal statutes, including the District of Columbia, has grown from 28 (in 2007) to 48 that have sex trafficking offenses and 50 that have labor trafficking offenses.

Other enacted or proposed laws and requirements include:

- The California Transparency in Supply Chains Act (CTSC Act) was enacted in January 2012. The CTSC Act requires retailers and manufacturers operating in California with annual revenues of more than $100 million to disclose their efforts to ensure their supply chains are free of slavery and human trafficking. Other states are expected to follow.
- A bill, modeled after the California law, was introduced in Congress. It would require publicly traded companies to disclose in their annual reports to the U.S. Securities and Exchange Commission (SEC) all measures taken to counter forced labor, human slavery, trafficking and child labor within companies' supply chains.
- Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act requires that companies disclose the source of any conflict minerals they use in their products (e.g., minerals mined in conditions of armed conflict and human rights abuses).
- President Barack Obama issued an executive order in September 2012, "Strengthening Protections Against Trafficking in Persons in Federal Contracts," mandating that government contractors implement compliance programs throughout the supply chain to prevent human trafficking.

1592. What statistics and trends are available for human trafficking?

Human trafficking, with more than $32 billion generated annually and affecting more than 160 countries, is a global problem, out-grossed only by drug and weapons trafficking. The following are select statistics and trends related to human trafficking:

- According to a report from the ILO in 2002, there were approximately 1.2 million children trafficked each year for forced labor and sexual slavery.
- The U.S. Department of State estimates 600,000-820,000 people are trafficked across national borders annually. Approximately 80 percent of victims are women and girls and 50 percent are minors. Approximately 50,000 or more victims (mainly women and children) are trafficked into the United States annually.
- According to the National Center for Missing and Exploited Children, 76 percent of transactions for sex with underage girls are conducted via the Internet.
- Of the more than 180 countries evaluated by the U.S. State Department, approximately 18 percent were fully compliant with minimum standards for anti-human trafficking, 47 percent were partially compliant, 23 percent were placed on watch and 13 percent were noncompliant.
- According to the Polaris Project Annual State Ratings, 21 states have strong anti-human trafficking laws; nine states have made nominal efforts toward passing anti-human trafficking laws; and four states (Arkansas, Montana, South Dakota and Wyoming) have made minimal efforts.
- Since the U.S. State Department began collecting this data in 2004, the number of global prosecutions for trafficking has ranged each year from approximately 5,200 to 6,800 through 2010, with an average conviction rate of 60 percent.
- Of the more than 34,500 prosecutions for human trafficking between 2005 and 2010, approximately 47 percent occurred in Europe, 20 percent in East Asia and the Pacific and 19 percent in South and Central Asia.
- According to the U.S. Department of Justice, of the more than 2,500 human trafficking cases in the United States occurring between January 2008 and June 2010, 80 percent were sex trafficking, of which 80 percent of the victims were identified as U.S. citizens. Of the approximately 250 cases classified as labor trafficking, 67 percent of the victims were identified as undocumented immigrants.
- The fact that very little information related to human trafficking has been reported on SARs is indicative of how underreported this crime is and how difficult it is for financial institutions to detect.

1593. What are the stages of human trafficking?

Human trafficking involves three stages:

- **Recruitment**: This initial stage involves the recruitment of a person from his/her community or country, often by coercion, deception or bondage (e.g., fake job offers, arranged marriages, educational opportunities, etc.).

- **Transportation**: This stage involves the movement of people, whether within the same geographic location (e.g., country) or across international borders, often by planes, boats, trains, etc.
- **Exploitation**: This is the final stage of human trafficking, where victims are sold for various exploitative reasons including, but not limited to, the following:
    - Bride trafficking
    - Child trafficking
    - Debt bondage
    - Forced labor
    - Illegal adoption
    - Removal of organs
    - Servitude
    - Sex tourism
    - Sexual labor
    - Slavery

1594. What roles can individuals play in a human trafficking operation?

According to the United Nations Office on Drugs and Crime (UNODC), a human trafficking operation involves many individuals with multiple roles, including:

- Coordinator or organizer
- Recruiter
- Transporter or guide
- Spotter
- Driver
- Messenger
- Enforcer
- Service provider or supplier

Human trafficking operations are increasingly being run by organized crime. According to FATF's "Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants," many trafficking and smuggling activities along the U.S.-Mexico border are supervised by the Mexican drug cartel, Los Zetas; in addition, Russian and Albanian gangs and the Italian mafia control a large portion of trafficking in Europe, while Chinese criminal groups and the Japanese Yakuza control trafficking in Asia.

According to EUROPOL, it is also not uncommon for former victims to assume some of these roles as they age.

1595. What is human smuggling and how is it different from human trafficking?

Human smuggling involves the covert transportation of individuals across international borders with the consent of the transported individuals. Human smuggling occurs during the "transportation" stage of human trafficking and typically ends after the transfer is complete.

The aim of smuggling people is unlawful cross-border transport for the purpose of gaining financial or other material benefit, whereas the purpose of trafficking in human beings is exploitation. Additionally, the physical transportation of victims from one location to another is not required for activity to fall within the definition of human trafficking.

1596. How are fees generated in a human trafficking and smuggling operation?

Fees can be generated through disparate activities with multiple parties during each stage of human trafficking: recruitment, transportation and exploitation.

Smugglers, also known as “coyotes,” often require a single payment for transportation of individuals across international borders, which generally includes the cost of transportation, bribery and fraudulent immigration documents. Fees for smuggling vary by country. Below are some current estimates:

- Mexico: $1,000-$3,500
- South America: $5,000-$7,000
- Eastern Europe: $18,000-$25,000
- China: $40,000-$70,000

1597. Which countries are at higher risk for human trafficking-related activities?

Various factors contribute to the higher occurrence of human trafficking and smuggling, including but not limited to war, corruption, economic and political instability, natural disasters, high rates of poverty and lack of education, gender discrimination, population pressure, lack of human rights and inadequate legal infrastructure to enforce laws related to human trafficking, smuggling and money laundering.

Victims of human trafficking are trafficked from many countries. According to FATF, the most common “sending” regions include the Commonwealth of Independent States (former Soviet Republics), Central and Southeast Europe, Western Africa and Southeast Asia. The top “receiving” regions include Western Europe, North America and Western Asia. Top “transit regions” include Western, Central and Southeast Europe, followed by Southeast Asia, Central America and Western Africa.

1598. Which states are at higher risk for human trafficking-related activities?

Statistics for domestic cases of human trafficking at the state level are difficult to obtain since most studies track these activities on a country level and it is generally difficult to identify human trafficking activities. Generally, states with strong tourism and agricultural industries are at higher risk for sex and labor trafficking.

According to the National Human Trafficking Resource Center (NHTRC), states with the highest number of reports of potential trafficking cases and victims located within their state in 2011 were:

- California
- Texas
- Florida
- New York
- District of Columbia
- Illinois
- Virginia
- Ohio
- North Carolina

As of July 2012, the Polaris Project Annual State Ratings reported Arkansas, Montana, South Dakota and Wyoming as the four states with the weakest anti-human trafficking laws.

1599. What are some high-profile examples of human trafficking and smuggling cases?

Following are examples of recent high-profile human trafficking and smuggling cases:

- In 2001, a California restaurateur and real estate tycoon, Lakireddy Balireddy, was sentenced to 10 years for two counts of transportation of minors for illegal sexual activity, conspiracy to commit immigration fraud and filing a false tax return. Due to the lack of applicable anti-human trafficking statutes at the time of trial, attorneys filing a civil suit claimed “slave labor,” “false imprisonment” and “infliction of emotional distress.” Victims were illegally smuggled into the United States from Balireddy’s village in India, many from the “untouchable class” who were promised a better life by a man with a net worth of more than $60 million based on his California properties alone. Five members of Balireddy’s family were also implicated and indicted for rape and conspiracy to commit immigration fraud for more than a decade. Balireddy served an eight-year prison term and was ordered to pay $2 million in restitution and register as a California sex offender. Many claim that this case fueled reform in

California, leading to anti-human trafficking laws with higher criminal penalties, monetary restitution and civil actions by victims against traffickers.

- In 2005, the former owner of a garment factory located in Hawaii was sentenced to 40 years in prison for involuntary servitude and trafficking; it stands as one of the largest trafficking cases prosecuted in the United States. The owner, Kil Soo Lee, was ordered by a federal judge to pay $1.8 million in restitution to approximately 300 workers who were subjected to abuse such as threats, lack of food and pay, confinement, sexual advances and unsafe living and working conditions. Another court ruled that the owner owed the workers $3.5 million in back pay and damages. In return for their testimony, some workers were granted special visas from the U.S. government.
- In 2012, several members of an extended Hungarian criminal organization in Canada were sentenced in the largest human trafficking case in Canadian history. Joszef Domotor, a "mid-level" player in his family's criminal organization, pleaded guilty to conspiring to commit human trafficking and being part of a criminal organization. His wife, Kristina Csazar, plead guilty to being part of a criminal organization, welfare fraud and obstruction of justice. At least 19 victims were recruited from their native Hungary with the promise of steady work and future plans to bring over their children. Victims were forced to work for free and lie to immigration and welfare officials. Six others have pleaded guilty to human trafficking and five more have pleaded to related charges. After serving their time in prison, Domotor and his wife will be deported to Hungary.

FATF's "Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants" provides details on 15 human trafficking and smuggling case studies. Case studies detail methods of recruitment, retention and exploitation of victims and methods of money transmission and laundering, including, but not limited to, the following:

- Frequent use of money service businesses (MSBs), informal value transfer systems (IVTS) and casinos;
- Commingling of illicit proceeds with funds of legitimate cash-intensive businesses, including takeovers of existing companies;
- Use of front companies, shell companies and straw persons;
- Purchasing of real estate abroad and luxury items (e.g., foreign cars); and
- Use of multiple bank accounts and credit cards in the names of associates and extended family members of traffickers.

FATF's report also provides a list of red flags by industry to assist banks, MSBs, dealers in high-value goods and casinos in detecting potential human trafficking schemes. In addition, the U.S. Immigration and Customs Enforcement (ICE) periodically provides on its website summaries of cases in which they have successfully rescued victims and prosecuted traffickers.

1600. What challenges exist to combating human trafficking?

Challenges to combating human trafficking include, but are not limited to, the following:

- Lack of comprehensive anti-human trafficking laws or poor enforcement of existing laws;
- Lack of awareness of existing anti-human trafficking laws and perception that human trafficking is a problem limited to a few countries;
- Insufficient training of local law enforcement on indicators for human trafficking and identifying and securing key evidence to assist in the successful prosecution of traffickers;
- Lack of cooperation, internationally and among federal, state and local organizations, leading to fragmented investigation processes;
- Lack of comprehensive data due to gaps, discrepancies and inconsistent methodologies in the collection of information on human trafficking cases (e.g., victims, traffickers, geographies, profits, etc.); and
- Lack of self-identification due to fear and/or shame of victims, particularly those who have been isolated for long periods of time.

Language and cultural barriers and lack of victim cooperation and testimony, often due to fear and distrust, lead to difficulties in prosecuting traffickers.

1601. What are the components of an effective anti-human trafficking program?

Key components to an effective anti-human trafficking program include:

- Implementation and enforcement of victim-friendly laws and regulations with criminal penalties for traffickers;
- Monitoring of adherence to existing legislation and activities contributing to human trafficking and analysis of successful prosecutions;
- Awareness and training programs for community members and law enforcement;
- Process to identify victims;
- Provision of support services to victims (e.g., protection, transportation, medicine, counseling, shelter, legal assistance, etc.);
- Process to reintegrate or voluntarily repatriate victims;
- Prosecution of traffickers;
- Forfeiture and confiscation of assets of traffickers; and
- Civil actions and monetary restitution for victims.

The president's executive order, "Strengthening Protections Against Trafficking in Persons in Federal Contracts," calls for the following:

- Employee awareness program
- Process to report violations without retaliation
- Certification that subcontractors/suppliers have not engaged in human trafficking-related activities (e.g., misleading recruitment, charging recruitment fees, destroying employees' identification documents, etc.)

Due to the fragmented and complex system of human trafficking, collaboration among community members, service providers and law enforcement, domestically and internationally, is key to developing an effective anti-human trafficking program.

1602. What obligations do financial institutions have related to human trafficking?

Financial institutions have an obligation to identify and report potential cases of human trafficking of their customers through routine suspicious activity monitoring processes. In addition, financial institutions may be subject to other requirements that require them to ensure their supply chains are free of human trafficking activities.

1603. What resources can a financial institution use to assess country risk related to human trafficking?

The U.S. State Department issues an annual "Trafficking in Persons Report" (TIP Report), similar to the Financial Action Task Force (FATF) Mutual Evaluation Reports (MERs), that evaluates each country on its compliance with the minimum standards of the Trafficking Victims Protection Act (TVPA) based on the following:

- Enactment and implementation of anti-human trafficking laws
- Criminal penalties for trafficking offenses
- Victim identification measures
- Victim protection and assistance efforts (e.g., legal assistance, primary healthcare, counseling, shelter)
- Victim repatriation and/or reintegration efforts

Each country is assigned a ranking of one of four tiers:

- Tier One: Fully compliant
- Tier Two: Partially compliant with progress in areas of noncompliance
- Tier Two Watch List: Partial compliance but significant occurrences of human trafficking violations continue to exist or there is a lack of evidence on progress in areas of noncompliance

- Tier Three: Noncompliant with lack of evidence of efforts to progress in areas of noncompliance

Of the more than 180 countries evaluated by the U.S. State Department, approximately 18 percent were fully compliant with minimum standards for anti-human trafficking, 47 percent were partially compliant, 23 percent were placed on watch and 13 percent were noncompliant. Noncompliant countries included the following:

- Algeria
- Burma
- Central African Republic
- Cuba
- Democratic Republic of Congo (DRC)
- Equatorial Guinea
- Eritrea
- Guinea-Bissau
- Iran
- North Korea
- Kuwait
- Lebanon
- Libya
- Madagascar
- Mauritania
- Micronesia
- Papua New Guinea
- Saudi Arabia
- Sudan
- Turkmenistan
- Venezuela
- Yemen
- Zimbabwe

Financial institutions can consider utilizing these tiered rankings as part of their risk assessment methodology. For additional guidance on risk assessments, please refer to the Customer Risk Assessment and High-Risk Geographies sections.

1604. Are there penalties for noncompliance with human trafficking laws?

Yes. Governments of countries that receive a Tier Three ranking may be subject to certain sanctions, including, but not limited to:

- The withholding or withdrawal of non-humanitarian, non-trade-related foreign assistance;
- Withholding of funding for government employees' participation in educational and cultural exchange programs; or
- Withdrawal of support to receive assistance from international financial institutions (e.g., International Monetary Fund [IMF], World Bank [WB]).

1605. What resources can a financial institution use to assess domestic risk as it relates to human trafficking?

Annually, the Polaris Project releases a state ratings map that assesses the strengths of human trafficking laws based on the following categories:

- Sex trafficking provision
- Labor trafficking provision
- Asset forfeiture and/or investigative tools for law enforcement
- Training requirement and/or human trafficking task force
- Posting a human trafficking hotline
- Safe harbor: protecting trafficked minors
- Lower burden of proof for sex trafficking of minors
- Victim assistance
- Access to civil damages
- Vacating convictions for sex trafficking victims

States are assigned a ranking of one of four tiers:

- Tier One: Highest ranking indicating state has passed significant anti-human trafficking laws
- Tier Two: State has passed numerous anti-human trafficking laws but needs to improve and implement its laws
- Tier Three: State has made nominal efforts to pass anti-human trafficking laws
- Tier Four: State has not made minimal efforts to pass anti-human trafficking laws

As of July 2012, the Polaris Project Annual State Ratings reported the following results of its assessment:

- Tier One: 21 states
- Tier Two: 16 states and Washington, D.C.
- Tier Three: 9 states (Arizona, Colorado, Delaware, Mississippi, New Hampshire, North Dakota, Pennsylvania, Utah and West Virginia)
- Tier Four: 4 states (Arkansas, Montana, South Dakota and Wyoming)

Financial institutions can consider utilizing these tiered rankings as part of their risk assessment methodology. For additional guidance on risk assessments, please refer to the Customer Risk Assessment and High-Risk Geographies sections.

1606. Which types of businesses are considered potentially high risk for human trafficking and smuggling?

Certain types of businesses are more easily used and abused by human traffickers and smugglers. Such businesses include those that are cash-intensive, lack transparency, involve international transactions/customers, require seasonal labor, and have less stringent regulatory requirements.

The Polaris Project distinguishes “perpetrators” from “facilitators” of human trafficking. Some of these businesses are directly involved in human trafficking, while others knowingly or unknowingly facilitate human trafficking by providing advertising, transportation, financial services and spaces to operate.

High-risk businesses and industries include, but are not limited to, the following:

- Adult film industry
- Advertisers (e.g., online websites, phone books, newspapers)
- Agriculture and farms

- Attorneys (e.g., immigration)
- Beauty salons (e.g., hair, nail)
- Brothels and prostitution rings
- Car washes
- Domestic work service providers (e.g., cleaning and janitorial services)
- Diplomats or government officials
- Escort service providers
- Factories
- Fishing
- Hostess and strip clubs
- Hotel and hospitality services
- Import/export companies
- Labor brokers
- Landlords
- Logging
- Manufacturers (e.g., textile)
- Massage parlors
- Mining
- Non-banking financial institutions (e.g., currency exchange houses, money transmitters, check cashing facilities) and informal banking systems (e.g., hawala, hundi, fei ch'ien, black market peso exchange)
- Prostitution
- Restaurants
- Sales crews (e.g., peddling and begging rings)
- Shelters (e.g., homeless, domestic violence, child abuse)
- Ship, bus or plane operators
- Taxi services
- Travel agencies
- Truck stops

The president's executive order, "Strengthening Protections Against Trafficking in Persons in Federal Contracts," directs federal agencies to establish a process to identify industries and sectors with a history of human trafficking.

For additional guidance on high-risk customers, please refer to the Customer Risk Assessment and High-Risk Customers sections.

1607. What are some common red flags for suspicious activity related to human trafficking?

Red flags that can be used by financial institutions to better identify and report potential suspicious activity related to human trafficking include, but are not limited to, the following:

- Customer with an excessive number of individual accounts
- A common mobile number, address and/or employment references that are used to open multiple accounts under different names
- Customer's telephone numbers linked to personal advertisements verified through public sources

- Customer's address linked to residence and/or hotel with suspected ties to trafficking (e.g., named in previous investigations and busts, offers hourly rates)
- Households with an unusually high number of residents who also appear unrelated
- Accounts opened in the name of unqualified minors
- Accounts reported for identity theft
- Accounts opened with fraudulent or missing/incomplete documentation
- Repeat payments to advertisers that promote the sex industry (e.g., websites, newspapers, escort services)
- Bill payments using money orders as opposed to paying with personal checks
- Cash deposits into one account from multiple locations throughout all states
- Frequent use of cash couriers
- High number of cash deposits structured to avoid reporting requirements
- Frequent deposits and withdrawals from multiple ATMs
- Frequent transfers utilizing money transmitters to common recipients, often in high-risk countries
- Frequent transfers or checks payable to casinos
- Frequent payments for rent, hotels, airline tickets or other travel-related accommodations
- Frequent small-dollar international funds transfers for "repayment of debt"
- High volume of payments for multiple mobile phones
- High volume of deposits of government benefits for multiple beneficiaries followed immediately by cash withdrawals
- Accounts lacking commercial activity or activity inconsistent with the stated nature of business/expected activity
- Purchases of luxury items or assets in high-risk countries
- Account activity beyond the living standard of the account holder

The fragmented and complex system of human trafficking and smuggling contributes to the difficulty in detecting potentially suspicious financial transactions related to human trafficking. Data mining may be a more effective method of detecting these types of activities than traditional suspicious transaction monitoring.

For additional examples of red flags, please refer to the Suspicious Activity Red Flags section.

1608. Are there instances in which a financial institution should notify law enforcement in advance of filing a SAR?

Whenever a violation is ongoing, financial institutions should immediately notify law enforcement, even before the SAR is filed.

U.S. Immigration and Customs Enforcement (ICE) has established a hotline at 1.866.DHS.2ICE to report instances of suspected human trafficking.

1609. Does notifying law enforcement of suspicious activity serve as a replacement or in any way relieve a financial institution's obligation to file a SAR?

No. Notifying law enforcement does not remove or in any way affect a financial institution's obligation to file a SAR if it detects suspicious activity.

For additional guidance on the reporting of potentially suspicious activity, please refer to the Suspicious Activity Reports section.

1610. What key groups have played an important role in the development and implementation of anti-human trafficking standards?

Recognizing the international focus on anti-human trafficking, many groups are active in issuing guidance and driving anti-human trafficking efforts, including, but not limited to, the following:

- The United Nations (UN) issued the Palermo Control, including the Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children; the Protocol against the Smuggling of Migrants by Land, Sea and Air; and the Protocol against the Illicit Manufacturing and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime. The United Nations Office on Drugs and Crime (UNODC) also produced "Toolkits to Combat Trafficking in Persons and Smuggling of Migrants."
- The ILO holds multiple conventions on forced labor, the abolition of forced labor and child labor.
- The Financial Action Task Force (FATF) issued the typology report "Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants" in 2011.
- Other international, regional and sub-regional organizations that have issued laws and guidance for anti-human trafficking include:
    - African Union (AU)
    - Association of Southeast Asian Nations (ASEAN)
    - Commonwealth of Independent States (CIS)
    - Coordinated Mekong Ministerial Initiative against Trafficking (COMMIT)
    - Council of Europe (COE)
    - Economic Community of Central African States (ECCAS)
    - Economic Community of West African States (ECOWAS)
    - League of Arab States (LAS)
    - Organization for Security and Cooperation in Europe (OSCE)
    - Organization of American States (OAS)
    - Regional Conference on Migration Plan of Action by the Puebla Group
    - South Asian Association for Regional Cooperation (SAARC)
    - Southern African Development Community (SADC)

For an extensive list of organizations and their anti-human trafficking efforts, please refer to Annex E of FATF's "Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants."

Within the United States, the federal response to combating human trafficking involves multiple federal agencies tasked with the following key responsibilities:

- President's Interagency Task Force to Monitor and Combat Trafficking (PITF) – Coordinate federal efforts to combat human trafficking.
- Department of State (DOS) – Coordinate international anti-human trafficking programs and efforts.
- Department of Health and Human Services (HHS) – Identify, certify and assist victims of human trafficking.
- Department of Justice (DOJ) – Investigate cases of human trafficking and prosecute traffickers.
- Department of Defense (DOD) – As one of the largest buyers in the world, ensure that the U.S. military, its civilian employees and its contractors are aware of and adopt a zero-tolerance policy on human trafficking within its organization and supply chain.
- Department of Homeland Security (DHS) (U.S. Immigration and Customs Enforcement [ICE], U.S. Customs and Border Protection [CBP], U.S. Citizenship and Immigration Services [USCIS]) – Raise awareness, identify and protect victims, grant immigration relief to victims, disrupt human trafficking rings and investigate cases of human trafficking.

- Department of Labor (DOL) – Detect exploitative labor practices and provide assistance to victims of human trafficking, including job search, education and training services, transportation, childcare and housing.
- Department of Agriculture (USDA) – Reduce the likelihood that agricultural products produced with the use of child or forced labor are imported into the United States.
- Department of Education (ED) – Raise awareness to prevent human trafficking and increase victim identification of trafficked children in schools.
- U.S. Agency for International Development (USAID) – Fund international programs that prevent trafficking, protect and assist victims, and support prosecutions through training for police and criminal justice personnel.
- U.S. Equal Employment Opportunity Commission (EEOC) – Identify labor trafficking cases in addition to discriminatory cases based on race, color, national origin, sex, religion, age, disability and genetic information.

Some key initiatives by the U.S. federal government include, but are not limited to, the following:

- Together with the Office of Refugee Settlement (ORS), the HHS established the **Anti-Trafficking in Persons** (ATIP) program, which supports the following initiatives:
    - **Victim Identification and Public Awareness** through the "Rescue and Restore" campaigns, which establish state, local and regional coalitions composed of non-government organizations, law enforcement and other community members to address the problem of human trafficking.
    - **Assistance for Victims of Human Trafficking** through certification and eligibility letters that identify and verify victims of human trafficking who are eligible for federal benefits and services; service grants through the National Human Trafficking Victim Assistance Program; and the National Human Trafficking Resource Center (NHTRC), a national hotline that offers resources and tools for victims as well as service providers and community members who are attempting to identify and prevent human trafficking and assist victims of this crime.
- The **Office to Monitor and Combat Trafficking in Persons** (G/TIP) within the U.S. Department of State issues an annual "**Trafficking in Persons Report**" (TIP Report), similar to the Financial Action Task Force (FATF) Mutual Evaluation Reports (MERs), that evaluates each country on its compliance with the minimum standards of the Trafficking Victims Protection Act (TVPA). Countries are monitored for progress in adhering to TVPA minimum standards based on a "3P" paradigm: prosecution, protection and prevention.
- Within the U.S. Department of State, the **Human Smuggling and Trafficking Center** (HSTC) gathers information on illicit travel, including that of trafficking, and coordinates with foreign agencies and diplomats to monitor and fight trafficking on an international basis.
- The Bureau of Justice Assistance (BJA) and the Office for Victims of Crime (OVC) within the DOJ funds the establishment of **Anti-Human Trafficking Task Forces** and released an "**Anti-Human Trafficking Task Force Strategy and Operations e-Guide**." The DOJ issues periodic Bureau of Justice Statistics (BJS) reports titled "**Characteristics of Suspected Human Trafficking Incidents,**" which summarize data captured in the **Human Trafficking Reporting System** (HTRS) based on information collected from local and federal law enforcement cases involving human trafficking within the United States. Additionally, the DOJ also produces the "**Attorney General's Annual Report to Congress on U.S. Government Activities to Combat Trafficking in Persons**."
- The U.S. Department of Labor's "**List of Goods Produced by Child Labor or Forced Labor**" cites goods from countries that the agency believes are produced by child or forced labor in violation of international standards.
- Together with the Federal Law Enforcement Training Center (FLETC), the DHS developed web-based human trafficking training modules under the "**Blue Campaign**" to teach law enforcement how to recognize human trafficking, protect victims and initiate human trafficking investigations. The DHS also initiated Project STAMP (Smugglers' and Traffickers' Assets, Monies and Proceeds), an effort to attack and seize the assets of human trafficking organizations and identify and disseminate typologies and red flags related to money laundering by these organizations.
- The U.S. Department of Agriculture established the **"Consultative Group to Eliminate the Use of Child Labor and Forced Labor in Imported Agricultural Products**,**"** representing government, private sector, academic and non-government entities charged with developing recommendations to reduce the likelihood of importing agricultural products produced with the use of child or forced labor.

The Polaris Project is a nonprofit, non-governmental organization established in 2002 to combat human trafficking. It has been involved in the following initiatives:

- Administration of the **National Human Trafficking Resource Center** (NHTRC) in partnership with the Office of Refugee Settlement (ORS).
- Founding member of the **Alliance to End Slavery and Trafficking** (ATEST), launched by Humanity United, to strengthen U.S. laws and federal resources to fight human trafficking.
- Administration of the Polaris Project Annual State Ratings, an annual assessment of state trafficking legislation in the United States.

Examples of other organizations involved in anti-human trafficking efforts include the following:

- **The Nexus Institute** is an independent international human rights research and policy center.
- **Safe Horizon** is a victim assistance organization that provides services to victims and families affected by crime and abuse, including, but not limited to, child abuse, domestic violence and human trafficking.
- **The Global Alliance Against Traffic in Women** is an alliance of more than 100 non-governmental organizations founded to promote the rights of women migrant workers and trafficked persons.
- **The Pillars of Hope: Attorneys General Unite Against Human Trafficking** is an initiative by the National Association of Attorneys General focused on nationwide efforts to fight labor and sex trafficking.
- **The Human Trafficking Clinic** at the University of Michigan Law School is a clinical law program committed to advancing anti-human trafficking policy through interdisciplinary collaboration at the local, national and international levels.

Elder Financial Abuse

1611. What is elder abuse?

Elder abuse generally refers to intentional or negligent actions taken by a caregiver or other person presumed to be in a position of trust who causes harm or a serious risk of harm to a vulnerable, older adult. It can be a single act or a series of actions that causes harm or distress to an older person and may include physical, psychological or financial abuse, as well as neglect.

1612. What is elder financial abuse?

Elder financial abuse involves the exploitation of a relationship with an elder or dependent adult in order to steal, embezzle or improperly use the person's money, property or other resources. The exploitation may occur by deception, coercion, misrepresentation, undue influence or theft, and can include deprivation of money and/or property.

1613. Why is elder financial abuse so insidious?

The occurrence of elder financial abuse is becoming more frequent and yet, at the same time, the crime is often underreported. Victims may not recognize that they are being exploited, due to the nature of the relationship with the perpetrator and/or due to their own diminished capacity. Additionally, many elders are reluctant to report the crime for reasons that include embarrassment that they have fallen prey to a confidence scheme, fear of retribution from the perpetrator, and even a desire to protect the loved ones who exploit them.

Elder financial abuse is particularly devastating because victims may lose all of their life savings and may never recover financially. Elder victims' inability to provide for their own needs and uncertainty as to what will become of them can have a permanent effect on their mental state, with victims often suffering from depression.

1614. Who is at risk of being victimized?

Older persons with physical or mental health issues may be vulnerable because their dependence on other individuals for daily care isolates them and/or because a diminished capacity leaves them unaware of the abuse or limits their ability to provide informed consent or otherwise respond appropriately. However, any older adult, regardless of potential health concerns, may be at increased risk of exposure to unscrupulous individuals who specifically target elders. Characteristics that perpetrators may exploit include, but are not limited to, the following:

- The isolation of individuals who may not physically be able to leave or object to the treatment;
- The elder's need for interaction with other individuals;
- Vulnerable experiences, such as traumas suffered by the elder or a close loved one;
- The elder's naiveté in wanting to believe the perpetrator is telling the truth; and
- The elder's desire to help an individual in need.

With 70 percent of wealth in the United States under the control of persons over the age of 50, the pool of potential victims for elder financial abuse is substantial.

1615. Who are common perpetrators of elder financial abuse?

Perpetrators of elder financial abuse can include anyone in a position of trust, control or authority; often, these individuals are well known to the victims. These perpetrators can include family members, neighbors and friends, as well as paid service providers – such as attorneys, doctors and financial advisers – and other persons who befriend the elder specifically to exploit him/her in the future. Additionally, perpetrators may be con artists who impersonate people in a position of trust.

1616. What common schemes are used to perpetrate elder financial abuse scams?

Elder financial abuse can take many forms, depending on the nature of the relationship being exploited. It can be as simple as directly removing money or property from the elder's possession, such as taking it from a wallet, or it can involve a complex confidence scam designed specifically to prey upon certain vulnerabilities. It may involve a series of ongoing activities, or it can be a onetime transaction. It may involve persons well-known to the victim, or it could be perpetrated by con artists or other criminals who target elders. Common categories of schemes involve, but are not limited to, the following:

- **Exerting undue influence, misrepresentation or fraud to obtain money or property** – The perpetrator manipulates, intimidates or otherwise threatens the elder into giving or signing over assets.
- **Exploiting a power of attorney or fiduciary authority** – The perpetrator takes advantage of his/her role as power of attorney or fiduciary to alter the elder's will, borrow money in the elder's name, or dispose of an elder's assets or income.
- **Misappropriation of money or property** – The perpetrator obtains access to the elder's bank accounts, credit cards, pension, etc., or forges the elder's signature in order to take money or property and/or to use the elder's property or possessions without permission.
- **Overcharging for services or withholding services** – The perpetrator may provide services for basic needs, such as food or medicine, at an exorbitant or unreasonable fee when the elder is not in a position to obtain the services elsewhere. Also, the perpetrator may agree to perform work, such as household repairs or other home improvement projects, at a reasonable fee, but once the work is under way, refuses to complete the job until the elder pays more for it.
- **Confidence crimes** – The perpetrator gains the victim's confidence and deceives or tricks him/her into paying money. These scams may involve claims of lottery winnings or inheritances, where the victim is persuaded to provide an amount upfront as a show of good faith, or may involve fictitious accidents or stories of loved ones needing immediate medical treatment to induce the elder to send money quickly.
- **Telemarketing and mail fraud** – The perpetrator calls victims or sends flyers that use deception, scare tactics or exaggerated claims to induce them to send money and can be difficult to distinguish from legitimate calls or correspondence. The fraud may involve selling a valueless product, collecting donations to a fake charity, etc., and the perpetrator may make repetitive charges against victims' credit cards without authorization.
- **Predatory lending practices** – Elders may be pressured into high-interest loans they cannot repay, such as home equity loans to finance home repairs, debt consolidation or healthcare costs, or they may be coerced into a reverse mortgage transaction.

1617. What are the warning signs of elder abuse?

Victims of elder abuse often demonstrate changes in their behavior and patterns of financial activity. The financial institution may be unable to speak with the customer, despite repeated attempts to contact him/her. When the institution does have customer contact, the elder may be accompanied by another person who won't allow the elder to speak alone with personnel or make any independent decisions. This person could be a new caregiver to the elder,

a new “best friend” or someone known to the institution, such as a family member, but who may take excessive interest in the elder’s finances or who suddenly takes control of the elder’s financial decisions.

Behavioral warning signs may include:

- **Physical changes** – The elder’s appearance and grooming may deteriorate noticeably. Inadequately explained fractures, bruises, cuts or burns may appear. The elder may have unexplained sexually transmitted diseases;
- **Mood or personality changes** – The elder may increasingly become withdrawn or secretive, could be reluctant to engage in conversation, and may appear frightened of or submissive to an individual accompanying him/her; and
- **Changes in intellectual capacity** – The elder may appear disorientated or forgetful, or demonstrate a lack of understanding, and may repeatedly ask the same question. The elder may have no awareness of his/her finances and appear confused about past transactions or missing funds.

Elders who have recently lost a spouse or moved into a nursing home are particularly vulnerable because of the emotional stress these types of life changes can create.

Although the presence of warning signs is not conclusive evidence that the elder is the victim of abuse, these indicators could signify the customer is at heightened risk.

1618. What role can financial institutions play with regard to combating elder financial abuse?

Financial institutions may become aware of potential abuse through their regular interactions with customers within their branch locations, through call center activity and via routine transaction monitoring. Branch personnel who are familiar with specific customers may note behavioral changes or other oddities in how the customer conducts business, including the presence of third-party influencers. Call center representatives may receive complaints about missing funds and inquiries about unrecognized transactions. Back-office personnel may note increased activity or activity that deviates from the customer’s profile. Financial institutions should have escalation procedures to refer these types of anomalies for further investigation and for initiating reviews of customer activity.

1619. What are some common red flags of elder financial abuse?

If a financial institution notes the presence of warning signs for elder financial abuse, it should investigate or perform other due diligence to determine whether potentially suspicious activity is present. The following are examples of financial activity red flags:

- **Changes in transaction activity** – The elder’s spending pattern may change, including:
    - Decreased spending on essential items (e.g., food, medication, utilities, etc.);
    - Increased spending and purchases of unnecessary items or items he/she can’t use;
    - Numerous withdrawals, including the maximum ATM withdrawal;
    - Checks written out of sequence; and
    - Large wire transfers to third-party beneficiaries who have unclear relationships with the elder.
- **Unexplained activity** – The activity may not make logical sense, given known details about the customer:
    - ATM withdrawals when the elder is homebound;
    - The sudden presence of overdrafts, when previously there had been limited to no insufficient funds activity;
    - Numerous unpaid bills, when someone has been designated to pay them;
    - An appearance of checks or signed documents when the elder cannot write or lacks the capacity to understand what he/she is signing, or the signature on checks and documents may not resemble the elder’s signature.
- **Changes in account features** – The elder may request the addition of account features or changes to existing features, including:
    - Requesting the issuance of a credit or debit card for the first time;
    - Seeking to enroll in online banking;

    - Changing the account beneficiary; and
    - Requesting that statements be sent to an address besides his/her own.
- **Uncharacteristic requests** – The elder may seek to undertake a non-routine transaction, including:
    - Refinancing a mortgage;
    - Closing a certificate of deposit without regard to penalties for early withdrawal; or
    - Requesting to wire a large sum for no apparent purpose.

For guidance on additional red flags, please refer to the Suspicious Activity Red Flags section.

1620. What should a financial institution do if it suspects potential elder financial abuse?

Financial institutions should report suspected elder financial abuse to FinCEN through Suspicious Activity Reports (SARs). Institutions should select the appropriate characterization of suspicious activity in the Suspicious Activity Information section of the SAR form and specifically use the term "elder financial exploitation" in the SAR narrative. Institutions should also use the narrative to explain why the institution knows, suspects or has reason to suspect that the activity is suspicious. The potential victim of elder financial exploitation should not be reported as the subject of the SAR, but rather information on the victim should be included in the SAR narrative.

Many states have laws against elder financial abuse that may require financial institutions to contact state or local authorities and may impose additional requirements.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

1621. Are there instances in which a financial institution should notify law enforcement in advance of filing a SAR?

Whenever a violation is ongoing, financial institutions should immediately notify law enforcement, even before the SAR is filed.

1622. What can financial institutions do to help prevent elder financial abuse?

Financial institutions can play an important role in preventing elder financial abuse by establishing programs that increase awareness of the risks and offering account security features that consider the needs of elder customers. Steps that financial institutions can take include, but are not limited to, the following:

- Develop policies that communicate the financial institution's position on elder financial abuse and implement procedures for how it will detect, investigate and report elder financial abuse to the authorities;
- Train employees about elder financial abuse schemes so that they recognize when a customer may be a potential victim and are sensitive to the heightened risk of elder customers;
- Assign responsible persons within the institution to whom employees should refer potential suspected elder financial abuse for further investigation and who will maintain awareness of industry trends and disseminate prevention techniques; and
- Educate customers on how to recognize the signs of elder financial abuse and the availability of resources for victim assistance, including alerting customers to possible scams as they appear.

1623. What statistics and observations are available on elder financial abuse?

Following are some notable statistics and observations related to elder financial abuse:

- More than 70 percent of the wealth within the United States is controlled by individuals who are over 50 years of age.
- Multiple resources suggest that at least 20 percent of individuals over 65 years of age will be a victim of a financial crime.
- FinCEN has issued multiple advisories related to the rise in the targeting of elders in mortgage and healthcare fraud schemes, including but not limited to reverse mortgages and Medicare fraud.
- According to Issue 20 of FinCEN's "SAR Activity Review," of the approximately 1,700 SARs related to "elder financial exploitation" filed during the first half of 2011:

- The top states for elder abuse-related filings included California, Florida, Texas, New York, Washington and Hawaii;
- Of those SARs filed by banks, the most commonly reported activities included credit card fraud, check fraud and identity theft;
- Of those SARs filed by money services businesses (MSBs), commonly reported activities included wire transfer activity related to advance fee schemes, online dating scams, and scams involving individuals posing as friends or family members in need of emergency funds;
- Of those SARs filed by the securities and futures industries, commonly reported activities included embezzlement, wire fraud, forgery, identity theft and check fraud.

It is likely that these statistics do not truly reflect the magnitude of the problem of elder financial abuse, as many cases go unreported.

1624. What resources are available with respect to elder financial abuse?

FinCEN has issued the following guidance and advisories on elder financial abuse:

- Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation
- Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Home Equity Conversion Mortgage Fraud Schemes
- FinCEN Supports Efforts to Raise Awareness of Elder Financial Exploitation
- SAR Activity Review – Trends, Tips & Issues provides insight on suspected cases of elder financial abuse

The Elder Investment Fraud and Financial Exploitation (EIFFE) Prevention Program was established by the Investor Protection Trust (IPT), a nonprofit organization devoted to investor education, in partnership with the North American Securities Administrators Association (NASAA), the National Adult Protective Services Association (NAPSA), the American Academy of Family Physicians, the National Area Health Education Center Organization and the National Association of Geriatric Education Centers. Created by the Baylor College of Medicine and funded by IPT, the EIFFE Prevention Program trains physicians, adult protective service professionals and other caregivers on how to identify and assist elders who are at risk or are victims of investment fraud.

Another organization established to address elder abuse in general is the National Center on Elder Abuse (NCEA). Established by the U.S. Administration on Aging (AoA) in 1988, the NCEA serves as a national resource dedicated to the prevention of elder mistreatment. The NCEA partnered with the National Committee for the Prevention of Elder Abuse (NCPEA) to expand multidisciplinary efforts to address elder abuse and administer a database – called the Promising Practices Clearinghouse – of key research, news and policy updates as they relate to elder abuse. Recent efforts have included the following:

- Establishment of specialized elder abuse investigation and prosecution units
- Creation of multidisciplinary teams composed of law enforcement, ombudsman, health and adult protective services
- Creation of fatality (forensic) review teams to investigate suspected cases of abuse
- Establishment of fiduciary abuse specialist teams (FASTs) composed of accountants, FBI personnel, insurance claims detectives and other specialists to investigate suspected elder financial abuse cases

Additionally, the Health Care Fraud Prevention and Enforcement Action Team (HEAT), a joint effort between the U.S. Department of Health and Human Services and the U.S. Department of Justice, was established in 2009 to strengthen existing programs (e.g., Medicare, Medicaid), investigate fraud and invest in new resources to prevent future fraud, waste and abuse.

Foreign Account Tax Compliance Act

FATCA Basics

As of the date of this publication, the final regulations for implementation of the Foreign Account Tax Compliance Act (FATCA) had not been published. The following information on FATCA is based on the proposed regulations issued in February 2012 and other regulatory guidance from the Internal Revenue Service (IRS) available at the date of drafting.

1625. What is the Foreign Account Tax Compliance Act (FATCA)?

FATCA, enacted in 2010 as part of the Hiring Incentives to Restore Employment (HIRE) Act, is designed to combat tax evasion by U.S. taxpayers hiding money in offshore accounts. FATCA imposes new requirements on three primary groups:

- Foreign financial institutions (FFIs) that maintain accounts for U.S. account holders or foreign entities substantially owned by U.S. persons;
- U.S. taxpayers holding specified financial assets outside of the United States; and
- U.S. financial institutions acting as withholding agents.

Under FATCA, the obligations for FFIs that have signed an agreement with the IRS include:

- Registering with the IRS as a participating FFI (or certifying as a “deemed-compliant” FFI);
- Conducting customer due diligence to identify U.S. account holders or accounts held by foreign entities substantially owned by U.S. persons;
- Ensuring that a 30 percent tax on certain payments of U.S. source income is withheld when paid to non-participating FFIs and account holders who are unwilling to provide the required identification information or documentation;
- Closing of accounts in certain instances of noncompliance;
- Submitting annual reports to the IRS with information about U.S. account holders and accounts held by foreign entities substantially owned by U.S. persons;
- Conducting compliance reviews and certifying compliance with FATCA; and
- Providing additional information to the IRS in determining whether the FFIs’ obligations were met under FATCA.

FATCA also requires U.S. taxpayers to self-report assets held at FFIs in excess of a specific threshold, determined by residence and tax filing status (separate or joint) on IRS Form 8938: Statement of Specified Foreign Financial Assets.

1626. What is the stated primary objective of FATCA?

The central thrust of FATCA is to identify U.S. account holders who have assets outside of the United States and provide reporting of that information to the IRS. The stated policy objective of FATCA is to achieve reporting on U.S. accounts, rather than withholding.

1627. What are the effective dates for the various provisions of FATCA?

There are different effective dates for the various provisions of FATCA:

- **FFI Agreement –** FFIs must enter into an agreement with the IRS by June 30, 2013, to avoid withholding on payments received from U.S. withholding agents starting on January 1, 2014. The effective date of any agreement entered into before July 1, 2013, will be July 1, 2013 (important because the effective date becomes the deadline for other requirements), and the effective date of any agreement entered into after July 1, 2013, will be the actual date of the agreement.

- **Due Diligence –** Due diligence procedures for new accounts must be in place by the later of January 1, 2014, or the effective date of the FFI agreement. Pre-existing high-value accounts of individuals must be reviewed by the later of December 31, 2014, or one year after the effective date of the FFI agreement. All other pre-existing accounts for individuals must be reviewed by the later of December 31, 2015, or two years after the effective date of the agreement.
- **Reporting –** Reporting requirements will be phased in. The first report of U.S. account holders to the IRS will only cover identification information (covering 2013 data) and is due in 2014. Reporting on dividends, interest and other income will start in 2016, and reporting on gross sales and redemption proceeds will begin in 2017.
- **Withholding –** Withholding requirements will begin for payments of fixed, determinable, annual or periodical (FDAP) income on January 1, 2014, and for payments of gross income generated by certain asset sales on January 1, 2015. Withholding on foreign passthru payments will begin on January 1, 2017.

1628. What are the consequences of noncompliance with FATCA?

FFIs that do not report the required information on U.S. account holders will be subject to a 30 percent withholding on U.S. source income (e.g., interest, dividends, and proceeds from securities sales). FFI account holders that do not provide the necessary identification information or documentation are also subject to the same withholding.

U.S. taxpayers who do not report the required information are subject to a $10,000 penalty, with an additional penalty of up to $50,000 for continued failure to file after IRS notification. A 40 percent penalty on any understatement of taxes associated with non-disclosed assets can also be imposed. In some cases, filers may be subject to criminal penalties.

1629. Who is responsible for overseeing compliance with FATCA?

The IRS is responsible for writing and implementing regulations and overseeing participating FFIs' compliance with FATCA.

1630. Are FFIs required to report on non-U.S. account holders under FATCA?

Yes. Accounts owned by foreign entities in which U.S. taxpayers hold a substantial ownership interest are subject to FATCA reporting requirements. Substantial ownership interest has been defined as greater than or equal to a 10 percent direct or indirect ownership.

1631. Are there any exemptions to FATCA?

Withholding does not apply to payments when the beneficial owner of the payment is one of the following:

- Foreign governments, political subdivisions of a foreign government, and wholly owned instrumentalities and agencies of a foreign government;
- International organizations and wholly owned agencies or instrumentalities of an international organization;
- Foreign central banks of issue;
- Governments of U.S. territories; and
- Certain foreign retirement plans.

1632. How is the IRS facilitating information sharing with participating FFIs?

Published guidance on FATCA notes that the IRS, in order to address certain legal issues on information sharing directly with the IRS, is pursuing arrangements with foreign governments to provide for alternative reporting by FFIs to resident country governments, who would share this information with the IRS under a tax treaty or other agreement.

1633. What further steps is the U.S. taking to improve international compliance with FATCA?

At the time of this publication, the United States had entered into a bilateral agreement with the United Kingdom to implement the information reporting and withholding provisions of FATCA, and was in discussions with France, Germany, Italy and Spain regarding the exchange, on an automatic basis, of information on accounts held in U.S. financial institutions by residents of these countries. By entering into an agreement with the United States, the partner country ("FATCA partner") would eliminate the need for each FFI established within the FATCA partner to enter into a separate agreement with the IRS.

In July 2012 the U.S. Treasury Department published model intergovernmental agreements to implement the information sharing with the countries listed above as well as other partner countries. These agreements, when put in place, would address privacy restrictions and other concerns of FFIs on sharing customer information and would also provide for bilateral sharing of information between governments.

1634. What key steps should participating FFIs take to ensure compliance with FATCA?

Participating FFIs should take the following key steps to ensure compliance with FATCA:

- Assemble a multidisciplinary work group and project management office to direct compliance readiness efforts including, but not limited to:
    - Compliance
    - Legal
    - Treasury
    - Operations
    - IT
    - Systems
    - Audit
    - Private banking
    - Asset management
    - Risk management
- Brief senior management on the requirements for compliance and need for resources.
- Consider the following issues related to IT and systems when designing an efficient and effective due diligence process:
    - Identification of U.S. person indicia
    - “Tagging” accounts of U.S. persons
    - Identification of related accounts
    - Aggregation of account balances for account holders
    - Required changes to client on boarding and acceptance processes to incorporate FATCA status to facilitate reporting and withholding obligations
    - Inventory of electronically available information to target due diligence searches of electronic databases
    - Searching electronic documentation
    - Tracking compliance efforts including missing documentation
    - Assembling information for reporting, on an entity-level and enterprise-level, where applicable
- Consider potential conflicts and roadblocks to FATCA reporting requirements with applicable privacy restrictions, including the ability of customers to waive privacy rights.
- Establish capabilities and processes to identify incoming funds that are subject to possible withholding, apply proper withholding calculations, and maintain records for reporting purposes.
- Prohibit employees on advising clients on account identification avoidance.
- Develop an internal awareness and training program on FATCA.
- Develop a communication strategy for customers to address questions and concerns that may arise with the implementation of FATCA requirements.

1635. What key guidance has been published related to FATCA?

The following key guidance has been published related to FATCA:

- **Notice 2010-60: Notice and Request for Comments Regarding Implementation of Information Reporting and Withholding Under Chapter 4 of the Code** (2010) by the IRS
- **Notice 2011-34: Supplemental Notice to Notice 2010-60, Providing Further Guidance and Requesting Comments on Certain Priority Issues Under Chapter 4 of Subtitle A of the Code** (2011) by the IRS
- **Notice 2011-53: Implementation Notice** (describing the timeline for implementation of FATCA) (2011) by the IRS
- **Notice 2011-55: Suspension of Information Reporting Requirements Until the Internal Revenue Service Releases Form 8938** (2011) by the IRS
- **Announcement 2012-42: Timelines for Due Diligence and Other Requirements under FATCA** (2012)
- **Proposed Regulation 121647-10: Regulations Relating to Information Reporting by Foreign Financial Institutions and Withholding on Certain Payments to Foreign Financial Institutions and Other Foreign Entities** (2012) by the IRS
- **Proposed Regulation 130302-110: Regulations relating to Reporting of Specified Foreign Financial Assets under IRC 6038D by Certain Domestic Entities** (2012) by the IRS
- **TD 9567: Temporary regulations relating to reporting of Specified Foreign Financial Assets under IRC 6038D** (2012) by the IRS
- **Summary of Key FATCA Provisions** (2012) by the IRS
- **Details on the FATCA Registration Process for Foreign Financial Institutions (FFI)** by the IRS
- **Basic Questions and Answers on Form 8938** by the IRS
- **Comparison of Form 8938 and FBAR Requirements** by the IRS
- News Releases by the IRS:
    - **Treasury, United Kingdom Sign Bilateral Agreement to Improve Tax Compliance, Combat Offshore Tax Evasion and Implement FATCA** (2012)
    - **Treasury Releases Model Intergovernmental Agreement for Implementing the Foreign Account Tax Compliance Act to Improve Offshore Tax Compliance and Reduce Burden** (2012)
    - **Treasury and IRS Issue Proposed Regulations for FATCA Implementation** (2012)
    - **Treasury and IRS Issue Guidance Outlining Phased Implementation of FATCA Beginning in 2013** (2011)
    - **IRS Releases Guidance on Foreign Financial Asset Reporting** (2011)
- **Foreign Financial Institutions: Preparing for the FATCA Burden** (2012) by Protiviti

Participating Foreign Financial Institutions

1636. How is a “foreign financial institution” defined for the purposes of FATCA?

A foreign financial institution (FFI) is a non-U.S. entity that:

- Accepts deposits in the ordinary course of business (e.g., banks, credit unions, building societies);
- Holds financial assets for others (e.g., broker-dealers, trust companies, clearing organizations, custodians); or
- Engages primarily in the business of investing, reinvesting or trading in securities, partnerships or commodities (e.g., mutual funds, hedge funds, venture capital funds, private equity funds).

1637. How are “nonfinancial foreign entities” defined for the purposes of FATCA?

Nonfinancial foreign entities (NFFEs) are defined as foreign entities that are not financial institutions under the FATCA definition. NFFEs are subject to withholding under FATCA if they refuse to provide ownership information to participating FFIs or U.S. withholding agents.

1638. How is “U.S. source income” defined for the purposes of FATCA?

U.S. source income is defined by IRS rules and regulations and generally refers to interest, dividends and gains on asset sales from U.S. locations.

1639. How is FDAP income defined by the IRS?

The IRS defines FDAP income as all income, except:

- Gains derived from the sale of real or personal property (including market discount and option premiums, but not including original issue discount); and
- Items of income excluded from gross income, without regard to the U.S. or foreign status of the owner of the income, such as tax-exempt municipal bond interest and qualified scholarship income.

Income is fixed when it is paid in amounts known ahead of time. Income is determinable whenever there is a basis for figuring the amount to be paid. Income can be periodic if it is paid from time to time. It does not have to be paid annually or at regular intervals. Income can be determinable or periodic, even if the length of time during which the payments are made is increased or decreased.

FFI Agreement

1640. What is an “FFI Agreement” for the purposes of FATCA?

An FFI agreement is a signed commitment in which FFIs agree to identify U.S. account holders, report account holder information to the IRS, withhold on payments to certain account holders, and close accounts in certain instances of noncompliance in accordance with FATCA. Under the agreement, participating FFIs must also do the following:

- Adopt policies and procedures for FATCA compliance;
- Periodically conduct reviews of compliance;
- Designate a responsible officer (RO) to certify the participating FFI’s compliance to the IRS; and
- Periodically provide the IRS with certifications and other information that will assist the IRS in determining whether the participating FFI has met its obligations under the FFI agreement.

1641. What is a “participating FFI” for the purposes of FATCA?

A “participating FFI” is an FFI that signs an FFI agreement with the IRS.

1642. What is a “deemed-compliant FFI” for the purposes of FATCA?

“Deemed-compliant FFIs” are FFIs with a low risk of tax evasion, such as retirement plans and certain investment vehicles. FFIs that have applied for the “deemed-compliant” status from the IRS are not subject to the reporting and withholding requirements of FATCA. There are three categories of deemed-compliant FFIs – registered, certified and owner-documented.

Registered deemed-compliant FFIs must meet IRS definition requirements, agree to conditions and register with the IRS, and renew their IRS certification every three years. Examples of registered deemed-compliant FFIs might be non-reporting members of FFI groups, qualified investment vehicles and restricted funds.

Certified deemed-compliant FFIs certify directly to specific withholding agents using Form W-8, and examples might include retirement plans, nonprofit organizations and FFIs with only low-value accounts.

Owner-documented deemed-compliant FFIs certify directly to withholding agents, provide ownership information, do not maintain accounts for non-participating FFIs, maintain low-value accounts, and are not affiliated with certain other FFIs.

1643. Why would an FFI enter into an agreement with the IRS?

An FFI must enter into an agreement with the IRS to avoid a 30 percent withholding on U.S. source income payments to the FFI for its own account or the accounts of its customers.

1644. What are the expanded affiliated group requirements for participating FFIs?

All FFIs in an expanded affiliate group must be participating FFIs or deemed-compliant FFIs in order for any FFI to become a participating FFI. An expanded affiliate group must appoint a “lead” FFI for the group. The “lead” FFI can register and submit information and annual reports to the IRS on behalf of the expanded affiliate group.

Registration

1645. What are the registration requirements for participating FFIs and deemed-compliant FFIs under FATCA?

The registration process serves as the FFI agreement for participating FFIs and certification for deemed-compliant FFIs. As part of the registration, participating FFIs must do the following:

- Select a FATCA Responsible Officer (RO) (typically the individual who signs the FFI agreement);
- Select up to five Points of Contact (POCs) with at least one in-house POC (typically the RO). POCs may include third parties, located in the home country of the participating FFI or in the United States (e.g., employee of an affiliate, service provider);
- In instances where the RO or other in-house individual cannot register the FFI, delegate FATCA registration duties (including signing) by power of attorney to an authorized third party (ATP) (i.e., U.S.-licensed tax professional subject to U.S. regulatory jurisdiction);
- Submit an affirmative statement that the person signing the FFI agreement (or certification) has the authority to act for the FFI;
- Provide positive identity verification for the individual who will sign the agreement (or certification) on behalf of the FFI (e.g., RO, ATP); and
- Obtain a FATCA Individual Identification Number (FIIN) for the person signing the FFI agreement (or certification).

1646. When will the IRS begin accepting registrations?

The IRS will begin accepting registrations through its electronic submissions process no later than January 1, 2013.

1647. Why should an FFI register by June 30, 2013?

An FFI should register by June 30, 2013 to ensure that it will be identified as a participating FFI in sufficient time to allow U.S. withholding agents to refrain from withholding beginning January 1, 2014.

Due Diligence

1648. What is the objective of an FFI's due diligence on individual accounts?

The objective of an FFI's due diligence on individual accounts is to put account holders into one of three "buckets":

- U.S. account holders
- Recalcitrant account holders
- Non-U.S. account holders

Each of these buckets is subject to different withholding and reporting requirements, making a robust tracking and documentation system vital to compliance.

Identification of U.S. Account holders

1649. How can participating FFIs identify U.S. account holders?

Participating FFIs must conduct due diligence on their existing and new account holders (both individuals and entities) to identify U.S. accounts and their owners. FFIs are permitted to rely on electronic records to perform due diligence on the accounts of U.S. persons.

The following are indicia of U.S. person account ownership and should be used to identify accounts requiring further due diligence for final determination of U.S. account status:

- Identification of an account holder as a U.S. person;
- A U.S. birthplace;
- A U.S. telephone number;
- Standing instructions to transfer funds to an account maintained in the United States, or directions regularly received from a U.S. address;
- An "in care of" address or a "hold mail" address that is the sole address with respect to the client; and
- A power of attorney or signatory authority granted to a person with a U.S. address.

1650. What steps are required if indicia of U.S. account ownership is noted?

When indicia of U.S. account ownership is noted, additional steps and documentation are required to establish the status of the account holder (U.S. or non-U.S.), such as:

- Obtaining an IRS Form W-9, IRS Form W-8BEN and non-U.S. passport
- Explanation of renunciation of U.S. citizenship or other specified documentation

Based on the review of the additional documentation requested, account holders will be classified as U.S. or non-U.S. persons. Account holders who refuse to provide documentation will be classified as "recalcitrant account holders."

Pre-Existing Individual Accounts

1651. What date should be used by participating FFIs to distinguish pre-existing and new individual accounts?

The effective date of an FFI agreement should be used to distinguish pre-existing accounts from new individual accounts.

1652. What steps does FATCA outline for reviewing pre-existing individual accounts?

FATCA suggests the following approach to identify U.S. classification for pre-existing individual accounts:

- **Step One**: Accounts with an aggregate balance or value of less than $50,000 do not need to be reviewed, unless the FFI elects otherwise. This threshold must include the aggregated balances of all accounts owned by an

individual to the extent that an FFI's systems can link accounts through common client numbers, identification numbers or other means. Each joint holder of an account will be attributed the total account balance for purposes of this aggregation.

- **Step Two**: Certain cash value insurance and annuity contracts held by individuals in pre-existing accounts with a value or balance of $250,000 or less are exempt from review, unless the FFI elects otherwise.
- **Step Three**: Accounts with a balance or value greater than $50,000 but less than $1,000,000, are subject to a review of electronically searchable information for U.S. person indicia. If no indicia are found, the account is classified as a non-U.S. account.
- **Step Four**: Accounts with a balance or value exceeding $1,000,000 are subject to a search of both electronic and non-electronic file information for U.S. person indicia, and inquiries of the relationship manager(s) must also be made. If no indicia are noted, the account is classified as a non-U.S. account.

If indicia are present in Steps Three or Four, additional steps and documentation are required to determine whether the account holder is a U.S. person, such as:

- Obtaining an IRS Form W-9, IRS Form W-8BEN and non-U.S. passport
- Explanation of renunciation of U.S. citizenship or other specified documentation

Based on the review of the additional documentation requested, account holders will be classified as U.S. or non-U.S. persons. Account holders who refuse to provide documentation will be classified as "recalcitrant account holders."

1653. How often are participating FFIs required to review pre-existing individual accounts?

After going through this exercise to classify pre-existing individual account holders, FFIs must annually re-test individual accounts with year-end balances that exceed $500,000 and were not previously subject to a review of account files.

New Individual Accounts

1654. How are "new" individual accounts defined?

New individual accounts are those opened after the effective date of the participating FFI's agreement with the IRS, and they include accounts opened by individuals who already have an existing account with the FFI.

1655. What steps does FATCA outline for reviewing new individual accounts?

Participating FFIs should take the following steps to determine U.S./non-U.S. classification of new individual accounts:

- Review the information provided at the opening of the account, including identification and any documentation collected under anti-money laundering/Know Your Customer (AML/KYC) rules.
- If U.S. indicia are identified as part of that review, obtain additional documentation to determine U.S. ownership, or treat the account as held by a recalcitrant account holder.

Pre-Existing Entity Accounts

1656. What date should be used by participating FFIs to distinguish pre-existing and new entity accounts?

The effective date of an FFI agreement should be used to distinguish pre-existing accounts from new entity accounts.

1657. What steps does FATCA outline for reviewing pre-existing entity accounts?

FATCA suggests the following approach to identify U.S./non-U.S. classification for pre-existing entity accounts:

- **Step One:** Pre-existing entity accounts with aggregate account balances of $250,000 or less are exempt from review until the account balance exceeds $1,000,000. These thresholds are based on the aggregated balances of all accounts owned by an entity to the extent that an FFI's system can link accounts through common client numbers, identification numbers or other means.

- **Step Two:** For remaining pre-existing entity accounts, electronically searchable information will need to be reviewed to determine U.S./non-U.S. classification. Generally, participating FFIs can rely on AML/KYC records and other existing account information to determine account status. For accounts identified as U.S. accounts or passive investment entities, all substantial U.S. owners (generally, 10 percent direct or indirect ownership) will need to be identified.

Entities reviewed in the above process must be put into one of the following "buckets":

- U.S. accounts (those with one or more "substantial" U.S. owners – defined generally as a 10 percent direct or indirect ownership)
- Foreign financial institutions:
    - Participating
    - Deemed-compliant
    - Non-participating
- Excepted entities (under Section 1471(f))
    - Foreign governments or political subdivisions of foreign governments
    - International organizations and their wholly owned agencies
    - Foreign central banks
- Recalcitrant account holders
- Non-financial foreign entities (NFFEs):
    - Excepted entity
    - Passive investment entity

Similar to the process for individual accounts, pre-existing entity accounts should be reviewed in a structured manner to determine their proper classification. Accounts already identified as U.S. accounts for other U.S. tax purposes are considered U.S. accounts.

Pre-Existing New Entity Accounts

1658. How are "new" entity accounts defined?

New entity accounts are those opened after the effective date of the participating FFI's agreement with the IRS, and they include accounts opened by individuals who already have an existing account with the FFI.

1659. What steps does FATCA outline for reviewing new entity accounts?

For new entity accounts, the same process described above for pre-existing entity accounts may be followed, except all information obtained in the account opening process must be considered, not just the electronically searchable information. This includes all information gathered for purposes of opening and maintaining the account, corresponding with the account holder and complying with regulatory requirements, including AML/KYC requirements.

Recalcitrant Account holders

1660. How is a "recalcitrant account holder" defined for the purposes of FATCA?

A recalcitrant account holder is any holder of an account maintained by a participating FFI if the account holder is not an FFI and the account holder either:

- Fails to comply with the participating FFI's request for documentation or information to establish whether the account is a U.S. account;
- Fails to provide a valid Form W-9 upon the request of the participating FFI;

- Fails to provide a correct name and TIN upon request of the FFI after the participating FFI receives notice from the IRS indicating a name/TIN mismatch; or
- Fails to provide a valid and effective waiver of foreign law if foreign law prevents reporting with respect to the account holder by the participating FFI.

1661. What actions are participating FFIs required to take with respect to recalcitrant account holders?

The U.S. Treasury Department and the IRS intend to require a participating FFI to report the number and aggregate value of financial accounts held by the following:

- Recalcitrant account holders;
- Related or unrelated non-participating FFIs; and
- Recalcitrant account holders who have U.S. indicia.

Recalcitrant account holders will be subject to a 30 percent withholding tax.

Withholding

1662. What are the withholding obligations of FFIs?

Participating FFIs agree to withhold a tax equal to 30 percent of withholdable and passthru payments of U.S. source income to the following account holders:

- FFIs that have not signed agreements with the IRS and that do not fall under an exception. The IRS intends to publish a list of participating FFIs and deemed-compliant FFIs to facilitate compliance.
- Individuals and entities that fail to provide sufficient information to determine whether or not they are a U.S. person (recalcitrant account holders) or fail to agree to waive applicable restrictions on the reporting of their information to the IRS.

1663. Are any entities exempt from withholding?

Yes. Withholding requirements do not apply to payments to the following beneficial owners of such payments:

- Any foreign government, any political subdivision of a foreign government, or any wholly owned agency or instrumentality of these entities;
- Any international organization or any wholly owned agency or instrumentality of an international organization;
- Any foreign central bank; or
- Any other class of persons identified by the Secretary of the U.S. Treasury Department as posing a low risk of tax evasion.

1664. How are “passthru payments” defined for the purposes of FATCA?

A passthru payment is defined as any withholdable payment or other payment to the extent attributable to a withholdable payment. The IRS indicates that passthru payments to nonparticipating FFIs and recalcitrant account holders are subject to withholding, and additional guidance should be forthcoming in future publications from the IRS.

1665. How are “custodial payments” defined for the purposes of FATCA?

A custodial payment is a payment with respect to which an FFI acts as a custodian, broker, nominee, or otherwise as an agent for another person. A custodial payment that is a withholdable payment will be treated as a withholdable payment (and thus as a passthru payment), and the FFI must apply the appropriate withholding unless the withholding obligation has been satisfied by another withholding agent.

1666. How can account holders request refunds of withheld funds?

The U.S. Treasury Department and the IRS intend to issue future guidance regarding the requirements necessary for claiming a refund.

Certification

1667. What certification requirements are participating FFIs required to provide under FATCA?

Participating FFIs must provide certifications of the following:

- Compliance with the provisions of FATCA to the IRS;
- Required due diligence on pre-existing accounts were completed by required deadlines; and
- Formal or informal practices or procedures were not in place at any time from August 6, 2011, forward to assist account holders in the avoidance of U.S. account identification.

1668. Are certifications required to be verified through third-party audits?

No. Verification of such compliance through third-party audits is not mandated, but may be required by the IRS in certain cases.

Reporting

1669. What are the annual reporting requirements of participating FFIs?

Participating FFIs are required to report annually the following to the IRS for its specified U.S. accounts:

- Name, address and taxpayer identification number (TIN);
- Account number;
- Account balance or value at year-end;
- Gross receipts from the account;
- Gross amount of dividends paid or credited to the account;
- Gross amount of interest paid or credited to the account;
- Other income paid or credited to the account; and
- Gross proceeds from the sale or redemption of property paid or credited to the account with respect to which the FFI acted as an agent for the account holder.

Reporting on the first four items in the list will begin in 2014; reporting on dividends, interest and other income will begin in 2016; and reporting on gross proceeds will start in 2017.

1670. When are annual reports due?

The IRS will specify in future guidance the date by which participating FFIs must file annual reports.

1671. What are the reporting requirements for an organization with multiple FFIs?

As with registration requirements, in an organization with multiple FFIs, a “lead” FFI must be appointed, and each affiliate in the group must execute an FFI agreement in order for all FFIs to be considered participating FFIs or deemed-compliant FFIs. The lead FFI can then submit required annual reports on behalf of the organization with multiple FFIs.

1672. Are participating FFIs required to include closed accounts in their annual reports to the IRS?

In the case of a U.S. account closed or transferred in its entirety by an account holder during the year, the participating FFI will be required to report the income paid or credited to the account for the year until the date of transfer or closure, and will also be required to report the amount or value withdrawn or transferred from the U.S. account as a gross withdrawal. The FFI will also be required to report the U.S. account as closed or transferred.

1673. What additional reporting requirements must participating FFIs submit under FATCA?

Reporting of recalcitrant account holders identified by participating FFIs by June 30, 2014, will be required to be filed with the IRS by September 30, 2014.

U.S. Financial Institutions/Withholding Agents

1674. What are the obligations for U.S. financial institutions as a withholding agent under FATCA?

To comply with its obligations as a withholding agent, a U.S. financial institution will be required to determine whether to treat entities to which it makes withholdable payments as:

- U.S. persons;
- Participating FFIs;
- Deemed-compliant FFIs;
- Non-participating FFIs;
- Entities described in Section 1471(f); or
- Excepted NFFEs or other NFFEs.

INTERNATIONAL PERSPECTIVES AND INITIATIVES

International Perspectives

1675. How do U.S. regulations compare to international AML regulations?

The United States' role as a leader in the fight against money laundering and terrorist financing dates back 40 years to the passage of the Bank Secrecy Act in 1970. Through the ensuing decades and especially following the terrorist activities of September 11, 2001, the United States has reinforced its commitment through the passage of a number of additional money laundering-related laws, issuance of extensive regulatory guidance and aggressive enforcement.

That said, the United States, as with many other major jurisdictions, is not in full compliance with the FATF Recommendations. In fact, FATF in its most recent assessment of the United States' anti-money regime, identified several areas in need of improvement, including: customer due diligence relating to beneficial owners, authorized signers, legal persons and trusts; ongoing due diligence; and general requirements for designated nonfinancial businesses and professions (DNFBPs) (e.g., casinos, accountants, attorneys, dealers in precious metals and stones, real estate agents). For additional guidance, please refer to the Financial Action Task Force and Mutual Evaluations sections.

1676. How are individual country standards monitored for conformity to international AML standards?

The Financial Action Task Force (FATF) performs mutual evaluations of countries based on its recently updated Recommendations (formerly the "Forty plus Nine Recommendations," now consolidated and referred to as simply the "Recommendations").

Since the end of 2002, the World Bank (WB) and International Monetary Fund (IMF) also have been involved in the effort to assess global AML standards using the standards set forth in the Recommendations.

For additional guidance on FATF and the Recommendations, please refer to the Financial Action Task Force section.

1677. How can multinational financial conglomerates manage their AML compliance efforts?

For multinational financial conglomerates subject to different AML requirements for each of their diverse business areas, as well as each jurisdiction in which they operate, the coordination of AML compliance efforts can be particularly challenging.

Institutions will benefit from AML compliance efforts being as consistent as possible throughout their global operations. While full consistency cannot be achieved due to the differing business and jurisdictional requirements, the most efficient AML program can be developed by an institution's headquarters to incorporate as many common characteristics as possible. The program then can be further customized across different businesses and jurisdictions to include the specific requirements of those businesses/countries.

Where possible, institution-wide AML compliance efforts should incorporate common Customer Identification Program (CIP) requirements, automated transaction-monitoring systems and risk-assessment methodologies. Whenever possible, centralization of key monitoring functions, or at least internal sharing of monitoring results among global compliance departments, allows an institution to take a holistic approach to the AML program.

1678. What are some obstacles to establishing a global AML program?

One of the biggest challenges in establishing a global AML program is adopting one global standard that meets the specific requirements of each country's AML laws and regulations. Although the overarching goal is very similar, the individual requirements are different. Global institutions typically implement a global policy with minimum requirements, often dictated by the location of the head office, and adopt local procedures at international locations. It can be difficult for the other offices to meet minimum standards if they are set too high, especially if local resources lack the requisite experience and knowledge and if their local competitors are not implementing such tight controls.

Multinational institutions also are facing the challenge of implementing transaction-monitoring systems on an enterprise level. Systems may need to accommodate different time zones and currencies, and apply custom rules/parameters to each jurisdiction.

Another potential obstacle that multinational institutions must consider is the different privacy laws and regulations that may exist in the jurisdictions in which the company operates. In some cases, these privacy regulations restrict the use of information and/or cross-border movement of information.

Key International Groups and Initiatives

1679. What key international groups have played an important role in the development and implementation of global AML standards?

Recognizing the international focus on money laundering and terrorist financing, many groups have become active in issuing guidance and driving AML efforts, including:

- The **Financial Action Task Force (FATF)** is an intergovernmental policy-making body composed of more than 30 countries whose purpose is to establish and promote international legislative and regulatory standards in the areas of money laundering and terrorist financing, and to monitor members' progress in adhering to these standards. FATF works to identify trends to disseminate to the global community for combating money laundering and terrorist financing. For additional guidance on FATF, please refer to the Financial Action Task Force section.
- **Egmont Group (Egmont)**, formed in 1995, has been the leading international association of financial intelligence units. As of 2010, there are 120 member countries that meet annually to discuss global issues of importance with regard to money laundering as well as terrorist financing. The group acts as a conduit for information sharing and, when pertinent, passes information on to the corresponding law enforcement agency to investigate. Examples of members are FinCEN (United States), TRACFIN (France), and FINTRAC (Canada).
- The **Wolfsberg Group of Banks (Wolfsberg)** is an association of 11 member international banks that creates industry best practices. Formed in 2000, the member banks include Banco Santander, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale and UBS. The group has produced work products in the areas of Know Your Customer (KYC), AML and counterterrorist financing. More recently, Wolfsberg Group released a work paper highlighting steps that financial institutions can take to prevent internal corruption.
- The **Basel Committee on Banking Supervision** (BCBS) is a committee of central banks and bank supervisors and regulators from major industrialized countries that meets to discuss issues relating to banking supervision at the Bank for International Settlements (BIS) in Basel, Switzerland. BCBS was formed in 1974 by the Governors of the central banks of the G10. BCBS operates under the expectation that member nations will take into account, and then implement, the guidance that comes out of these meetings. The goal of BCBS is to create uniform international standards of banking best practices.
- The **World Bank (WB)**, established in 1945, was founded to help countries recover from natural disasters, humanitarian crises and other conflicts that plague the developing world. With 187 member countries, the WB primarily works on reducing global poverty by the distribution of grants for development projects. The WB also has a group whose primary purpose is to curb money laundering and terrorist financing through FATF as its vehicle for change. In recent years, the WB has adopted FATF Recommendations for internal use.
- The **International Monetary Fund (IMF)** is an international body like the World Bank. It oversees the global monetary system and offers aid and assistance to countries as situations arise. The IMF, along with the WB, have created the Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) program to help the global community better improve AML regimes to prevent the flow of terrorist dollars into the global monetary infrastructure. This group works by providing technical assistance to countries in need.

- The **United Nations' (UN)** purpose is to maintain international peace and security; develop friendly relations among nations; cooperate in solving international economic, social, cultural and humanitarian problems; promote respect for human rights and fundamental freedoms; and be a center for harmonizing the actions of nations in attaining these ends.
- The **European Commission (EC)**, formally known as the Commission of the European Communities, is the executive branch of the European Union (EU) responsible for proposing legislation, implementing decisions, and upholding the EU's treaties. It also is responsible for the general day-to-day running of the EU.
- **Europol,** the European Law Enforcement Agency, was established in 1992 with the aim of improving the effectiveness and cooperation of law enforcement authorities in the EU Member States in preventing and combating terrorism, unlawful drug trafficking, and other serious forms of organized crime.
- **Organisation for Economic Cooperation and Development (OECD)** uses its wealth of information on a broad range of topics to help governments foster prosperity and fight poverty through economic growth and financial stability. The OECD helps ensure the environmental implications of economic and social development are taken into account.
- **International Organization of Securities Commissions (IOSCO)**, established in 1983, is a global cooperative body recognized as the international standard setter for securities markets. With a membership that regulates more than 95 percent of the world's securities markets in over 100 jurisdictions, IOSCO is the primary international cooperative forum for securities market regulatory agencies.
- **Asia/Pacific Group on Money Laundering (APG)** is an autonomous and collaborative international organization that was founded in 1997 in Bangkok, Thailand. It consists of 40 member jurisdictions, and a number of international and regional observers who assess compliance by APG member jurisdictions with the global AML/CFT standards and contribute to the global policy development of anti-money laundering and counterterrorism financing standards through active Associate Membership status in the FATF.
- **Eastern and South Africa Anti-Money Laundering Group (ESAAMLG)**, an organization with 14 members located in the Eastern and Southern African Region, was established at an inaugural Meeting of the Council of Ministers held in Arusha, Tanzania, on August 27, 1999. The objectives of ESAAMLG are to adopt and implement FATF's Forty plus Nine Recommendations and implement any other measures contained in multilateral agreements.
- **Organization of American States (OAS)**, an international organization headquartered in the United States in Washington, D.C., includes 35 independent states of the Americas. The OAS is the region's principal multilateral forum for strengthening democracy, promoting human rights and confronting shared problems such as poverty, terrorism, illegal drugs and corruption. It plays a leading role in carrying out mandates established by the hemisphere's leaders through the Summits of the Americas.
- **INTERPOL**, established in 1923, is the world's largest international police organization with 188 member countries. Its mission is to prevent or combat international crime by facilitating cross-border police cooperation and assisting all organizations, authorities and services within the limits of existing laws in different countries.
- **MONEYVAL**, the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, formerly known as PC-R-EV, was established in 1997 by the Council of Europe. With 28 permanent members, two temporary members and numerous observers, MONEYVAL's objective is to ensure its members implement effective systems to counter money laundering and terrorist financing in accordance with international standards.
- **Transparency International,** founded in 1993, is a global civil society organization with more than 90 chapters. Its mission is to fight against corruption by bringing together relevant players from government, civil society, business and media.

1680. What guidance has the Bank of International Settlements provided?

The Bank of International Settlements (BIS) has provided the following guidance:

- **Basel Committee: Banking Secrecy and International Cooperation in Banking Supervision** – A publication created in December 1981 that discusses the need to overcome bank secrecy impediments that hinder the flow of information between different foreign jurisdictions in an effort to establish an effective, internationally coordinated infrastructure to supervise banks.
- **Basel Committee: Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering** – A publication created in December 1998 that encourages banks to implement effective

procedures to properly identify customers with whom they are conducting business to prevent their institutions from being used to conduct criminal activity.

- **Initiatives by the BCBS, IAIS and IOSCO to Combat Money Laundering and the Financing of Terrorism** – A joint note created in June 2003 between the Basel Committee on Banking Supervision (BCBS), International Association of Insurance Supervisors (IAIS), and the International Organization of Securities Commissions (IOSCO) that discusses the initiatives taken by each sector to combat money laundering and terrorist financing. The first part of the note provides an overview of common AML/CFT standards applicable to all three sectors and assesses whether there are serious gaps or inconsistencies in approaches and recommendations. The second part of the note covers the relationships between the institutions and their customers, focusing on products or services particularly vulnerable to money laundering, how each committee has sought to address those vulnerabilities, and a description of ongoing and future work, broken out by each of the three sectors.
- **Customer Due Diligence for Banks** – A publication created in October 2001, establishing standards for Know Your Customer (KYC) programs to manage the reputational, operational, legal and concentration risks of banks and nonbank financial institutions and professional intermediaries (e.g., attorneys, accountants) effectively.
- **General Guide to Account Opening and Customer Identification** – A publication created in February 2003 as an attachment to "Customer Due Diligence for Banks," which was published in October 2001. This publication focuses on some mechanisms banks can use to develop an effective Customer Identification Program (CIP).
- **Sharing of Financial Records between Jurisdictions in Connection with the Fight against Terrorist Financing** – A publication created in April 2002 that focuses on the official gateways, such as financial intelligence units (FIUs), for cross-border information sharing as well as information flow from a financial entity to its head office or parent.
- **Survey of Developments in Electronic Money and Internet and Mobile Payments** – A publication created in March 2004 in cooperation with the Committee on Payment and Settlement Systems (CPSS) that focuses on two categories of emerging payment products and services: reloadable electronic money instruments and Internet and mobile payments.
- **General Principles for International Remittance Services** – A publication created in January 2007 jointly with the World Bank (WB) that discusses the payment system aspect of remittances and how to safely and efficiently send and receive international payments. The January 2007 edition was an update to the original publication issued in March 2006.
- **Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-Border Wire Transfers** – A publication created in May 2009 that provides guidance for situations in which one or more intermediary banks are located in a jurisdiction other than where the bank of the originator and the bank of the beneficiary are located.

1681. What guidance has the Wolfsberg Group provided?

Key publications issued by the Wolfsberg Group include, but are not limited to, the following:

- **The Wolfsberg Statement Against Corruption** (2007) – A statement written to generally describe the Wolfsberg Group's and financial institutions' roles in dealing with corruption. It also identifies some measures that may be used by financial institutions to prevent corruption in their own operations and protect themselves against the misuse of their operations in relation to corruption.
- **Wolfsberg Statement – Guidance on a Risk-Based Approach for Managing Money Laundering Risks** (2006) – Guidance to assist institutions with managing money laundering risks and prevent the use of their institutions for criminal purposes; focuses on using a risk-based approach.
- **Wolfsberg Statement – Anti-Money Laundering Guidance for Mutual Funds and Other Pooled Investment Vehicles** (2006) – Guidance to assist mutual funds and other pooled investment vehicles with managing their money laundering risk.
- **Wolfsberg Statement on AML Monitoring, Screening and Searching** (2009) – This guidance supersedes the 2003 paper on the same topic. The statement provides more guidance on the design, implementation and ongoing maintenance of transaction monitoring frameworks for real-time screening, transaction monitoring and retroactive searches.
- **Wolfsberg AML Principles for Correspondent Banking** (2002) – Guidance concerning the establishment and ongoing maintenance of correspondent banking relationships.

- **Wolfsberg Frequently Asked Questions on Correspondent Banking** (2006) – A follow-up guide to the Wolfsberg AML Principles for correspondent banking addressing frequently asked questions concerning correspondent banking based upon the Wolfsberg Group's views on current best practices and how it believes those practices should evolve over time.
- **The Wolfsberg Group and the Clearing House Association: Cover Payments: Some Practical Questions Regarding the Implementation of the New Payments Messages** (2009) – Guidance issued by the Wolfsberg Group regarding the implementation of the new SWIFT payment messages for cover payments, the MT 202 COV, and the MT 205 COV.
- **Wolfsberg Statement on the Suppression of the Financing of Terrorism** (2002) – Guidance describing the role financial institutions have in preventing the flow of terrorist funds through the world's financial systems.
- **Wolfsberg AML Principles on Private Banking** (2012) – Guidance tailored toward assisting financial institutions with combating money laundering in the private banking industry.
- **Wolfsberg Frequently Asked Questions on Selected Anti-Money Laundering Issues in the Context of Investment and Commercial Banking** (2006) – Guidance addressing specific money laundering concerns in the investment and commercial banking industries.
- **Wolfsberg FAQs on Beneficial Ownership** (2012) – A guide addressing questions concerning "Beneficial Ownership" that arose from the Wolfsberg AML Principles on Private Banking.
- **Wolfsberg FAQs on Politically Exposed Persons** (2008) – A guide addressing frequently asked questions about politically exposed persons (PEPs).
- **Wolfsberg FAQs on Intermediaries** (2012) – A guide addressing frequently asked questions about intermediaries.
- **Wolfsberg AML Guidance on Credit/Charge Card Issuing and Merchant Acquiring Activities** (2009) – A guide addressing the vulnerabilities of credit/charge card issuing activities and merchant acquiring activities in and methods of managing these risks.
- **The Wolfsberg Trade Finance Principles** (2011) – A guide on the vulnerabilities of trade finance and recommendations on methods for managing these risks.

1682. What guidance has the World Bank provided?

Key publications issued by the World Bank include, but are not limited to, the following:

- **Money Laundering and Terrorist Financing: A Practical Guide for Banking Supervisors** – A publication created in 2009 that summarizes various models, suggested tools, and methodologies for developing comprehensive supervisory systems.
- **New Technologies, New Risks? Innovation and Countering the Financing of Terrorism** – A publication created in 2009 that details the vulnerabilities of value cards, mobile financial services, online banking/payments and digital currencies, and recommendations on developing more effective preventive measures.
- **Stolen Asset Recovery: Politically Exposed Persons, A Policy Paper on Strengthening Preventive Measures** – A publication created in 2009 that summarizes key obstacles in identifying and mitigating the risks of politically exposed persons (PEPs) and recommendations on developing more effective preventive measures.
- **Stolen Asset Recovery: A Good Practices Guide on Non-Conviction Based (NCB) Asset Forfeiture** – A publication created in 2009 that provides guidance on Non-Conviction Based (NCB) forfeiture, a legal regime that provides for the seizure and forfeiture of the proceeds of serious crime, including corruption, without the need for a criminal conviction.
- **Correspondent Account KYC Toolkit: A Guide to Common Documentation Requirements** – A publication created in 2009 by the International Finance Corporation (IFC), the private sector arm of the World Bank Group, that provides information and guidance relating to the application process for opening a correspondent bank account or responding to an inquiry from a counterparty bank undertaking a Know Your Customer (KYC) compliance review.
- **Alternative Remittance Systems and Terrorism Financing: Issues in Risk Management** – A publication created in 2009 that summarizes more than a hundred recommendations on issues relating to terrorist financing, including, but not limited to, new technologies, nonprofit organizations, informal remittance providers, and international cooperation.

- **Mobile Phone Financial Services Paper** – A publication created in 2008 that summarizes fieldwork from seven economies on the vulnerabilities of mobile financial services and recommendations on methods for managing these risks.
- **Counter-Terrorism Implementation Task Force Report** – A publication created in 2009 that details the findings and recommendations of the meetings of the "United Nations Working Group on Tackling the Financing of Terrorism" task force led by the World Bank with the IMF and the UN Office on Drugs and Crime with support from INTERPOL, the Al-Qaida/Taliban Monitoring Team, and the Counter-Terrorism Committee.
- **Financial Intelligence Units: An Overview** – A publication created in 2004 that provides examples from multiple countries on how to establish financial intelligence units (FIUs).
- **Effective Regimes to Combat Money Laundering and the Financing of Terrorism, Strengthening the Collaborative Process: Lessons Learned** – A publication created in 2004 that describes best practices for developing an effective AML infrastructure consistent with international standards.
- **The World Bank in the Global Fight Against Money Laundering and Terrorist Financing** – A publication created in 2003 that describes the magnitude and impact of money laundering and terrorist financing on the global financial system and the role of the World Bank in combating it.
- **Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism: Second Edition and Supplement on Special Recommendation IX** – A guide created in January 2006 that provides practical solutions to establishing a comprehensive AML infrastructure.
- **AML/CFT Regulation: Implications for Financial Service Providers that Serve Low-Income People** – A guide published in July 2005 that summarizes the implications of the AML requirements for financial service providers working with low-income people and possible solutions to minimize adverse impacts.
- **Money Laundering in Cyberspace** – A document published in November 2004 that details the vulnerabilities and trends of Internet-based payment mechanisms and recommendations on methods for managing these risks.
- **Bilateral Remittance Corridor Analysis (BRCA)** – A series of publications that focuses on payment corridors between two or more countries. The reports provide insight into the players (e.g., remittance senders and receivers), market dynamics, vulnerabilities, and regulatory frameworks of select remittance corridors.
- **Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide** – A seven-part training guide published in January 2009 on developing comprehensive institutional, legal, and regulatory frameworks for combating money laundering and terrorist financing consistent with international standards:
    - Volume 1: Effects on Economic Development and International Standards
    - Volume 2: Legal Requirements to Meet International Standards
    - Volume 3a: Regulatory and Institutional Requirements for AML/CFT
    - Volume 3b: Compliance Requirements for Financial Institutions
    - Volume 4: Building an Effective Financial Intelligence Unit
    - Volume 5: Domestic (Inter-Agency) and International Cooperation
    - Volume 6: Combating the Financing of Terrorism
    - Volume 7: Investigating Money Laundering and Terrorist Financing

1683. What guidance has the International Monetary Fund provided?

Key publications issued by the International Monetary Fund (IMF) include, but are not limited to, the following:

- **Fiscal Transparency, Accountability, and Risk** – A publication created in 2012 that highlights fiscal transparency as a critical element of effective fiscal policymaking and risk management. The focus is on the ongoing efforts to enhance international standards for transparency and monitoring, and revitalizing various efforts to prevent risk management shortcomings.
- **Money Laundering and Terrorism Financing: An Overview** – A publication created in 2005 that examines why and how criminal and terrorist organizations use financial institutions to move and store assets, and the legal and regulatory responses in developing preventive measures.

- **Recent Developments in International Monetary Fund Involvement in Anti-Money Laundering and Combating the Financing of Terrorism Matters** – A publication created in 2005 summarizing recent developments in the fight against money laundering and terrorist financing, including, but not limited to, the expanded role of the IMF, the Offshore Financial Center (OFC) Program, the Financial Services Assessment Program (FSAP), and revisions to FATF's Forty plus Nine Recommendations.
- **Financial Section Assessment Program (FSAP)** – The FSAP is a voluntary, comprehensive and in-depth analysis of a country's financial sector designed to help increase the effectiveness of efforts to promote the soundness of financial systems in member countries which result in Reports on Observance of Standards and Codes (ROSC). In 2008, the **Offshore Financial Center (OFC) Assessment Program** was integrated into the FSAP Program. The OFC Assessment Program executes detailed assessments of the extent to which OFCs meet international standards.
- **Financial Intelligence Units: An Overview** – A publication created in 2004 that provides an overview of financial intelligence units (FIUs), including, but not limited to, information on how to establish an FIU, core functions and international assessments of FIUs.
- **The Impact of Terrorism on Financial Markets** – A publication created in 2005 that details how financial markets have reacted to terrorism.
- **Suppressing the Financing of Terrorism – A Handbook for Legislative Drafting** – A publication created in 2003 that summarizes international measures to combat terrorist financing and provides guidance on topics such as criminalizing the financing of terrorism; freezing, seizing and confiscating terrorist assets; establishing jurisdiction; international cooperation; alternative remittance systems; and nonprofit organizations.
- **Regulatory Frameworks for Hawalas and Other Remittance Systems** – A publication created in 2005 that summarizes the regulatory frameworks for hawalas and other informal remittance systems. For additional guidance on informal value transfer systems (IVTS), please refer to the Money Services Businesses and Informal Value Transfer Systems sections.

1684. What guidance has the United Nations provided?

The United Nations has provided the following key model laws and treaties on money laundering and related offenses, including confiscation, proceeds of crime, mutual assistance in criminal matters and the financing of terrorism:

- Money Laundering
    - United Nations Convention Against Illicit Traffic In Narcotic Drugs And Psychotropic Substances (1988)
    - United Nations Convention Against Transnational Organized Crime (2000)
    - Political Declaration and Action Plan Against Money Laundering (1988)
    - Naples Political Declaration and Global Action Plan Against Organized Transnational Crime (1994)
- Terrorist Financing
    - Convention on Offences and Certain Other Acts Committed on Board Aircraft (1963)
    - Convention for the Suppression of Unlawful Seizure of Aircraft (1970)
    - Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971)
    - Convention on the Prevention and Punishment of Offences against Internationally Protected Persons, Including Diplomatic Agents (1973)
    - International Convention against the Taking of Hostages (1979)
    - Convention on the Physical Protection of Nuclear Material (1980)
    - Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988)
    - Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988)
    - Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf (1988)
    - Convention on the Marking of Plastic Explosives for the Purpose of Detection (1991)

    - International Convention for the Suppression of Terrorist Bombings (1997)
    - International Convention for the Suppression of the Financing of Terrorism (1999)
- Mutual Assistance and Criminal Matters
    - United Nations Model Mutual Assistance in Criminal Matters Bill (2000)
    - United Nations Model Foreign Evidence Bill (2000)
    - United Nations Model Extradition (Amendment) Bill (2000)
    - United Nations Model Witness Protection Bill (2000)
    - United Nations Model Legislation on Laundering, Confiscation and International Cooperation in Relation to the Proceeds of Crime (1999)
    - United Nations Model Law on International Cooperation (Extradition and Mutual Legal Assistance) with regard to Illicit Traffic in Narcotic Drugs, Psychotropic Substances and Precursors
    - United Nations Model Treaty on Extradition (1990) and amendment, United Nations International Cooperation in Criminal Matters (1997)
    - United Nations Model Treaty on Mutual Assistance in Criminal Matters, 1990, and amendment, United Nations Mutual Assistance and International Cooperation in Criminal Matters (1998)

Additionally, the United Nations has hosted a series of conferences, conventions and forums related to combating money laundering and the financing of terrorism:

- United Nations Convention against Corruption (UNCAC) (2004)
- Conventions Against Terrorism
- International Convention for the Suppression of the Financing of Terrorism (adopted in 1999 and enforced in 2002)
- The International Convention against Transnational Organized Crime and its Protocols, 2000
- United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988
- Report and Recommendations of the International Conference on Preventing and Controlling Money-Laundering and the Use of the Proceeds of Crime: A Global Approach, 1994
- Report of the World Ministerial Conference on Organized Transnational Crime, 1994 (which included the Naples Political Declaration and Global Action Plan against Organized Transnational Crime)
- Twentieth Special Session of the General Assembly, 1998: Transcript from the panel discussion on “Attacking the Profits of Crime: Drugs, Money and Laundering” and the General Assembly Political Declaration and Action Plan against Money Laundering
- Money Laundering and the Financing of Terrorism: The United Nations Response, 2004 (Excerpts from the main legal instruments and resolutions against money laundering and the financing of terrorism adopted under the auspices of the United Nations)
- United Nations Global Programme against Money Laundering (GPML) Forum Framework of Minimum Standards, 2000

The UN also has issued several publications, including, but not limited to, the following:

- **An Overview of the UN Conventions and Other International Standards Concerning Anti-Money Laundering and Countering the Financing of Terrorism** – A publication first compiled in February 2004 and then updated in January 2007 by UNODC’s Anti-Money Laundering Unit/Global Programme Against Money Laundering, which provides an overview of various international laws and standards on anti-money laundering and counter-financing of terrorism.
- **Financial Havens, Banking Secrecy and Money Laundering** – A publication created in 2008 featuring the results of a study designed to explore the issues of banking secrecy and financial havens in the context of the global fight against money laundering. The study was prepared on behalf of the United Nations under the auspices of the Global Programme Against Money Laundering, Office for Drug Control and Crime Prevention.

- **Countering Money Laundering** – This publication, created in 1997, provides a comparative analysis of major international conventions against money laundering.
- **Publications Related to Terrorism**
    - **Digest of Terrorist Cases** – A publication created in 2010 that provides practical ideas and expert insights on how to deal with cases of terrorism. Topics include, but are not limited to, the following:
        - Violent Offences Not Requiring a Specific Terrorist Intent
        - Association for the Purpose Of Preparing Terrorist Acts
        - Relationship Between Terrorism and Other Forms of Crime (e.g., corruption, narcotics trafficking, organized crime, using minor offences to catch major criminals, false identity and immigration offences)
        - The Statutory Framework for Terrorism Prosecutions
        - Investigation and Adjudication Issues
        - International Cooperation
        - Innovations and Proposals
    - **Legislative Guide to the Universal Anti-Terrorism Conventions and Protocols** – A publication created in 2004 that provides a summary of the development and requirements of the international terrorism conventions to assist those responsible for incorporating anti-terrorism conventions in national legislation.
    - **Guide For Legislative Incorporation of the Provisions of the Universal Legal Instruments Against Terrorism** – A publication created in 2006 that provides guidance on how anti-terrorism conventions and protocols can be integrated and harmonized with domestic law and other international standards.
    - **Preventing Terrorist Acts: A Criminal Justice Strategy Integrating Rule of Law Standards in Implementation of United Nations Anti-Terrorism Instruments** – A publication created in 2006 that provides guidance on topics including, but not limited to, the responsibility to protect against terrorism, scope and elements of a preventive criminal justice strategy against terrorism, offenses, procedural improvements and mechanisms for international cooperation.
    - **Criminal Justice Responses to Terrorism Handbook** – A publication created in 2009 that provides guidance on the key components of an effective criminal justice response to terrorism and criminal justice accountability and oversight mechanisms.
    - **Counter-Terrorism Legislation Database** – An online resource of legal resources on international terrorism established in 2009.
    - **Frequently Asked Questions on International Law Aspects of Countering Terrorism** – A publication created in 2009 that provides an overview of the international law framework in which counter-terrorism works, including general principles of international criminal law, humanitarian law, refugee law and human rights law, which may be relevant in a counter-terrorism context.
- **Publications Related to Corruption**
    - **Assessment of the Integrity and Capacity of the Justice System in Three Nigerian States** – A publication created in 2006 that presents statistics and data drawn from live interviews held with specific groups within the justice system.
    - **Compendium of International Legal Instruments on Corruption, 2nd Edition** – A publication created in 2005 that contains all the major relevant international and regional treaties, agreements, resolutions and other instruments related to corruption.
    - **Global Action Against Corruption: The Mérida Papers** – A publication highlighting the key topics addressed in the United Nations Office on Drugs and Crime in Merida, Mexico, in 2003, including, but not limited to, the following:
        - Preventive Measures against Corruption: the Role of the Private and Public Sectors
        - The Role of Civil Society and the Media in Building a Culture against Corruption
        - Legislative Measures to Implement the United Nations Convention against Corruption
        - Measures to Combat Corruption in National and International Financial Systems

        - International Group for Anti-Corruption Coordination: Report of the Fifth Meeting
    - **Technical Guide to the United Nations Convention Against Corruption** – A publication created in 2009 by the UNODC and the United Nations Interregional Crime and Justice Research Institute (UNICRI) to promote the implementation of the United Nations Convention against Corruption (UNCAC) Convention, the first global legally binding instrument in the fight against corruption, which was adopted by the United Nations in 2003.

The UNODC also provides guidance on the following related topics:

- Strategy on Human Trafficking and Migrant Smuggling
- Criminal Justice, Prison Reform and Crime Prevention
- Organized Crime
- Piracy Under International Law

For further information, please visit the United Nations Office on Drug and Crime's website at www.unodc.org.

1685. What is the International Money Laundering Information Network (IMoLIN)?

The International Money Laundering Information Network (IMoLIN) is a network of the following international organizations:

- Asia/Pacific Group on Money Laundering (APG)
- Caribbean Financial Action Task Force (CFATF)
- Commonwealth Secretariat, Council of Europe – MONEYVAL
- Eurasian Group (EAG)
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
- Financial Action Task Force (FATF)
- Financial Action Task Force on Money Laundering in South America (GAFISUD)
- Intergovernmental Action Group Against Money Laundering in West Africa (GIABA)
- INTERPOL
- Organization of American States (OAS/CICAD)

Key resources provided by IMoLIN include the following:

- **Anti-Money Laundering International Database (AMLID)** – A centralized resource center administered by the Law Enforcement, Organized Crime and Anti-Money-Laundering Unit (LEOCMLU) of the United Nations Office on Drugs and Crime (UNODC) that contains analyses of AML/CFT laws and regulations from its member organizations.
- **Legislations and Regulations** – List of legislation and regulations by country.
- **International Norms and Standards** – Model laws for common law and civil law systems.
- **Research and Analysis** – Publications from governments and international organizations.
- **Bibliography** – A list of books, articles and other publications issued by governments and international organizations addressing all aspects of anti-money laundering, countering the financing of terrorism, and governance.
- **Calendar of Events** – A list of current national, regional and international training events and conferences.

1686. What AML guidance has the International Organization of Securities Commissions (IOSCO) provided?

Key publications issued by the International Organization of Securities Commissions (IOSCO) include, but are not limited to, the following:

- **Anti-Money Laundering Guidance For Collective Investment Schemes** – Final Report (October 2005) – This publication lays out the principles endorsed by IOSCO to address the application of the client due diligence process in the securities industry and describes the FATF's Forty Recommendations on combating money laundering and the financing of terrorism.
- **Initiatives by the BCBS, IAIS and IOSCO to Combat Money Laundering and the Financing of Terrorism** (January 2005) – This report offers guidance to address vulnerabilities in combating money laundering and the financing of terrorism in the banking, insurance and securities sectors.
- **Report on Money Laundering** – This report, created in 1992, summarizes the growing concerns of money laundering in the securities sector and recommendations to combat money laundering including, but not limited to, the FATF's Forty Recommendations.
- **Reports on Various Topics:**
    - **Special Purpose Entities (SPEs)**:
        - Special Purpose Entities (2007)
        - Report on Special Purpose Entities, Joint Forum (IOSCO, BCBS and IAIS) (2009)
    - **Beneficial Ownership**: Principles on Client Identification and Beneficial Ownership for the Securities Industry
    - **Information Sharing**: Multi-jurisdictional Information Sharing – Final Report
    - **Internet-Based Activities**: Report on Securities Activity on the Internet (Three Part Series: I, II and III) (1998, 2001 and 2003 respectively)

1687. What AML guidance has Transparency International (TI) provided?

Key publications issued or recommended by TI include, but are not limited to, the following:

- **Survey, Indices and Assessments**
    - The **Corruption Perceptions Index** (CPI) measures the perceived level of public-sector corruption in 180 countries and territories around the world based on multiple surveys. The CPI shows a country's ranking (score is based on a scale of 1 to 10, with 10 being the least corrupt), the number of surveys used to determine the score, and the confidence range of the scoring. In 2009, New Zealand, Denmark, Singapore, Sweden and Switzerland ranked as the least corrupt; Somalia, Afghanistan, Myanmar, Sudan and Iraq ranked as the most corrupt; the United States ranked as the 19th least corrupt country out of 180 jurisdictions.
    - The **Bribe Payers' Index** (BPI) assesses the supply side of corruption and ranks corruption by source country and industry sector.
    - The **Global Corruption Barometer** (GCB) is a public opinion survey that assesses the general public's perception and experience of corruption in more than 60 countries.
    - **National Integrity System Assessments** (NIS) country reports present the results of the NIS assessment in the form of a comprehensive analysis of the anti-corruption provisions and capacities in a country, including recommendations for key areas of anti-corruption reform.
- **Working Papers** includes a series of reports on various topics related to corruption and anti-corruption practices including, but not limited to, the following:
    - **Corporate Responsibility and Anti-Corruption: the Missing Link?** (2010)
    - **Making Government Anti-Corruption Hotlines Effective** (2009)
    - **Corruption and Local Government** (2012)
    - **Corruption in the [Middle East and North Africa] MENA Region: A Declining Trend or More of the Same?** (2008)

    - **Corruption and Sport: Building Integrity and Preventing Abuses** (2009)
    - **Recovering Stolen Assets: A Problem of Scope and Dimension** (2011)
    - **Corruption and (In)security** (2008)
    - **Accountability and Transparency in Political Finance** (2008)
- **Global Corruption Reports** includes a series of reports that detail corruption risks and solutions in various sectors, including, but not limited to, the following:
    - **Corruption and the Private Sector** (2009)
    - **Corruption in Judicial Systems** (2007)
    - **Political Corruption** (2004)
- **Policy Positions** includes a series of publications that provide guidance in developing anti-corruption policies, including, but not limited to, the following:
    - **Controlling Corporate Lobbying and Financing of Political Activities** (2009)
    - **Building Corporate Integrity Systems to Address Corruption Risks** (2009)
    - **Making Anti-Corruption Regulation Effective for the Private Sector** (2009)
    - **Countering Cartels to End Corruption and Protect the Consumer** (2009)
    - **Strengthening Corporate Governance to Combat Corruption** (2009)
    - **Political Finance Regulations: Bridging the Enforcement Gap** (2009)
    - **Effectively Monitoring the United Nations Convention against Corruption (UNCAC)** (2011)
    - **Standards on Political Funding and Favours** (2009)
- The **Anti-Corruption Research News** provides users with insights and activities in anti-corruption research on knowledge gaps and emerging risks, curriculum development, jobs, funding opportunities and research events on a quarterly basis.
- The **Anti-Corruption Plain Language Guide** provides standardized definitions for key terms commonly used by the anti-corruption movement.

1688. What guidance has the Egmont Group provided?

Egmont has provided the following guidance:

- **The Role of FIUs in Fighting Corruption and Recovering Stolen Assets** – An FIU can be an important element of fighting corruption-related offences, and preventing the laundering of illicit funds which stem from corruption activities. Published in 2012, this report details the results of a study aimed at increasing awareness of corruption and asset recovery among FIUs, and presents case scenarios and best practices. It also describes the position and the role of the FIU in the asset recovery process.
- **Enhancing International AML/CFT Information Exchange through Strengthening FIU Channels** – Published in 2011, this report introduces the concept of "diagonal" exchange of information through enhanced international cooperation, and focuses on the Egmont Group's ongoing efforts to strengthen international sharing of information in areas where current international standards do not call for, or may not fully support, cross-border sharing.
- **Statement of Purpose of the Egmont Group of Financial Intelligence Units** – A statement of purpose written for the organization in June 1997 and revised as of June 2004. Full compliance with the Egmont definition of a financial intelligence unit (FIU) is an essential component of being admitted into the Egmont Group.
- **Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases** – Basic principles, written in June 2001, outlining how the exchange of information between FIUs should be conducted.
- **Interpretive Note Concerning the Egmont Definition of a Financial Intelligence Unit** – A document explaining the Egmont Group's stance on the definition of an FIU. The definition was originally stated in 1996 and amended in 2004 to include terrorism financing.

- **"Countering of Terrorism Financing" Complementary Interpretive Note** – A document created in 2004 intended to complement the Interpretive Note Concerning the Egmont Definition of an FIU, which further clarifies the definition of an FIU by also explaining the minimum requirements of an FIU to comply with the Egmont Group's definition of an FIU.
- **Executive Summary of The Final Report on Survey of FIU Governance Arrangements** – A document created by the Egmont Group and World Bank Project in January 2010 that summarizes baseline information on governance arrangements among FIUs.
- **Best Practices for the Exchange of Information Between Financial Intelligence Units** – A document developed to enhance the exchange of information between FIUs by documenting principles that relate to the conditions for the exchange of information, the permitted uses of information, and confidentiality.
- **Information Paper on Financial Intelligence Units and the Egmont Group** – A brief paper published in 2004 describing the history and purpose of FIUs and the Egmont Group.
- **Egmont Meetings at a Glance** – A document that describes the main focus or outcomes of each of the Egmont Plenary Meetings, current as of August 2005.
- **International Bulletin** – A bulletin produced from time to time that outlines the current accomplishments and ongoing workings of the Egmont Group.
- **Library of Sanitized Cases** – A library of cases submitted by member FIUs of the Egmont Group, in which the information was sanitized so others can use the cases as training material to assist all FIUs and institutions with fighting the global problem of money laundering and terrorist financing. The library is broken down into categories such as Cross-Border Activities, Gambling, and Terrorist Financing.
- **FIUs in Action: 100 Cases from the Egmont Group** – A compilation of 100 sanitized cases published to assist FIUs and institutions with fighting the global problem of money laundering and terrorist financing, compiled by Egmont from submissions from member FIUs. These cases can be used as training material.
- **The Egmont Group – Financial Intelligence Units of the World** – A listing of all current member FIUs of the Egmont Group.

1689. How does an FIU become a member of Egmont?

FIUs become a member of the Egmont Group by completing a questionnaire that collects contact details and interest from the unit, and by undergoing site visits and a written assessment that focuses on the operational and legal aspects of the FIU. The heads of the member FIUs discuss the candidate's application, provide their recommendations at the annual meeting, and provide a written commitment, if endorsed.

1690. How many FIUs are members of the Egmont Group?

As of October 2012, over 130 FIUs were members of the Egmont Group. Following is a partial list:

- **Armenia** – Financial Monitoring Center (FMC)
- **Afghanistan** – Financial Transactions and Reports Analysis Center of Afghanistan
- **Australia** – Australian Transaction Reports and Analysis Centre (AUSTRAC)
- **Brazil** – Conselho de Controle de Atividades Financeira (Council for Financial Activities Control) (COAF)
- **Canada** – Financial Transactions and Reports Analysis Centre of Canada/Centre d'analyse des opérations et déclarations financières du Canada (FINTRAC/CANAFE)
- **Cayman Islands** – Financial Reporting Authority (CAYFIN)
- **Colombia** – Unidad de Informacion y Analisis Financiero (UIAF)
- **Côte d'Ivoire** – National Unit for the Processing of Financial Information in Côte d'Ivoire (CENTIF-CI)
- **Czech Republic** – Financní analytický útvar (Financial Analytical Unit) (FAU – CR)
- **Dominica** – Financial Intelligence Unit (FIU)
- **Egypt** – Egyptian Money Laundering Combating Unit (EMLCU)
- **France** – Traitement du Renseignement et Action Contre les Circuits Financiers Clandestins (TRACFIN)

- **Germany** – Zentralstelle für Verdachtsanzeigen – Financial Intelligence Unit
- **Hong Kong** – Joint Financial Intelligence Unit (JFIU)
- **India** – Financial Intelligence Unit – India (FIU-IND)
- **Ireland** – An Garda Síochána/Bureau of Fraud Investigation (MLIU)
- **Israel** – Israel Money Laundering Prohibition Authority (IMPA)
- **Italy** – Unità di Informazione Finanziaria (UIF)
- **Japan** – Japan Financial Intelligence Center (JAFIC)
- **Korea (Republic of)** – Korea Financial Intelligence Unit (KoFIU)
- **Netherlands** – Financial Intelligence Unit (FIU) – Nederland
- **Poland** – Generalny Inspektor Informacji Finansowej (General Inspector of Financial Information) (GIIF)
- **Slovakia** – Spravodajská jednotka finacnej polície Úradu boja proti organizovanej kriminalite (Financial Intelligence Unit of the Bureau of Organised Crime) (SJFP UBPOK)
- **Switzerland** – Meldestelle für Geldwäscherei, Bureau de communication en matière de blanchiment d'argent, Ufficio di comunicazione in materia di riciclaggio di denaro (Money Laundering Reporting Office) (MROS)
- **United Kingdom** – Serious Organised Crime Agency (SOCA)
- **United States** – Financial Crimes Enforcement Network (FinCEN)

For a full list of FIUs, please visit Egmont's website at www.egmontgroup.org.

Financial Action Task Force

FATF Basics

1691. What is the Financial Action Task Force (FATF)?

The FATF is an intergovernmental policy-making body composed of more than 30 countries whose purpose is to establish and promote international legislative and regulatory standards in the areas of money laundering and terrorist financing, and to monitor members' progress in adhering to these standards. Among other things, FATF works to identify trends to disseminate to the global community for combating money laundering and terrorist financing.

Additional information on FATF membership standards and current members is included below.

1692. Who leads FATF?

FATF is led by an appointed president who is chosen from among the member countries and supported by the FATF Secretariat, which is housed in Paris, France, at the headquarters of the Organisation for Economic Co-operation and Development (OECD). The FATF president serves one 12-month term.

1693. How does FATF establish international standards for combating money laundering and terrorist financing?

FATF achieves this by creating awareness through its publications, such as *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferations* (which has replaced the "Forty plus Nine Recommendations"), various typology and methodology reports, and Mutual Evaluation Reports (MERs) of member nations.

1694. How are decisions made within FATF?

All decisions are made by consensus in plenary meetings by members of FATF. The plenary meetings are assisted by the FATF Secretariat and chaired by the FATF president.

1695. What does FATF hope to achieve by developing these standards and issuing the Recommendations?

FATF has several goals including, but not necessarily limited to:

- Supporting legal/criminal justice systems and law enforcement
- Creating consistency in institutional/regulatory systems for combating money laundering and terrorist financing
- Developing preventive measures that should be taken by financial institutions and certain businesses and professionals
- Fostering international cooperation

1696. With what bodies has FATF collaborated to assist in implementing the Recommendations?

FATF collaborates with four FATF associate members and four FATF-style regional bodies (FSRBs) that are involved with combating money laundering and terrorist financing.

FATF associate members are:

- Asia/Pacific Group on Money Laundering (APG)
- Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) (formerly PC-R-EV)
- Grupo de Acción Financiera de Sudamerica (GAFISUD)
- Middle East and North Africa Financial Action Task Force (MENAFATF)

FATF-style regional bodies are:

- Caribbean Financial Action Task Force (CFATF)
- Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG)
- Eastern and South African Anti-Money Laundering Group (ESAAMLG)
- Intergovernmental Anti-Money Laundering Group in Africa (GIABA)

FATF also has close partnerships with the Offshore Group of Banking Supervisors (OGBS), the International Monetary Fund (IMF), the World Bank (WB), the United Nations, the Egmont Group and other international organizations.

1697. What is included in the updated FATF Recommendations?

The updated FATF Recommendations address the following general areas of a country's AML infrastructure:

- Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) policies and coordination
- Money laundering and confiscation
- Terrorist financing and financing of proliferation
- Preventive measures
- Transparency and beneficial ownership of legal persons and arrangements
- Powers and responsibilities of competent authorities and other institutional measures
- International cooperation

The Recommendations have been recognized by the IMF, the WB and other international organizations as setting international standards for combating money laundering and the financing of terrorism. For further guidance, please refer to the section Analysis of the FATF Recommendations.

1698. How are FATF and the Recommendations relevant to U.S. financial institutions?

The United States is a founding member of FATF; therefore, a number of U.S. AML statutes and regulations are influenced by the Recommendations.

In addition, FATF has the authority to issue a MER of the United States, as a FATF member.

The results of the MERs may serve as a catalyst for additional AML-related rulemaking and/or regulatory guidance.

1699. Why did FATF consolidate the Forty plus Nine Recommendations?

FATF, since its inception, has continually adapted its guidance to address new and emerging threats. FATF and other FSRBs determined that consolidation of the Forty plus Nine Recommendations was required in order to clarify and strengthen many existing obligations, increase consistency among jurisdictions' application and implementation of AML/CFT measures, as well as to enforce the Recommendations.

1700. What are the new consolidated Recommendations called?

The newly consolidated Recommendations are simply referred to as "The FATF Recommendations." A specific Recommendation may be referred to by its new consolidated number (e.g., consolidated Recommendation #12). A conversion table of the Recommendations is available in the Analysis of the FATF Recommendations section.

1701. What are the benefits of implementing the FATF Recommendations?

There are a number of benefits that a country derives from adherence to the Recommendations including, but certainly not limited to, the following:

- Securing a more transparent and stable financial system;
- Reducing volatility of international capital flows and exchange rates, market disparities and stabilizing investment and trade flows;
- Reducing vulnerabilities to infiltration, exploitation or abuse by organized crime groups;
- Implementing tools and resources that support the facilitation of tracking and monitoring illicit funds;
- Supporting international cooperation through participation in binding international obligations;
- Avoiding the risk of sanctions or other actions by the international community; and
- Protecting a country's financial system from becoming a haven for criminals.

1702. Does FATF have the authority to enforce the Recommendations or investigate suspicious activity?

No. FATF has no enforcement or investigative authority. FATF's Recommendations are not rules but rather policies aimed to set international AML standards. While many countries have made a political commitment to fight money laundering and terrorist financing by implementing the Recommendations, and FATF may assess a country's adherence to the Recommendations, the MERs are not reports which a country has an obligation to respond to or address. As a practical matter, however, companies may use the results of the MERs to assess a country's risk of money laundering and terrorist financing, which does exert some pressure on countries to address shortcomings.

All potentially suspicious activity should be reported to local investigative authorities (e.g., FinCEN), not to FATF.

1703. How does FATF monitor new money laundering and terrorist financing methods and trends?

Annually, FATF invites experts from law enforcement and regulatory authorities of member countries to share information on significant money laundering and terrorist financing cases and operations. This exercise helps to identify and describe current money laundering trends and effective countermeasures. Findings are summarized and then released in periodic reports made available on FATF's website.

1704. What guidance has FATF provided?

Key publications issued by FATF in the last two years include:

- **International Standards on Combating Money Laundering and The Financing of Terrorism & Proliferation** – Recommendations that are aimed at establishing AML best practices for jurisdictions, regulators and market participants. For additional guidance, please refer to the Analysis of the FATF Recommendations section.
- **Mutual Evaluation Reports (MERs)** – The mutual evaluation process is designed to measure and evaluate the implementation progress of the Forty plus Nine Recommendations. It involves FATF members conducting evaluations of each other's AML infrastructures in accordance with the Forty plus Nine Recommendations. MERs detail the findings of each country's mutual evaluation. For additional guidance on the mutual evaluation process, please refer to the Mutual Evaluations section.
- **AML/CFT Evaluations and Assessments: Handbook for Countries and Assessors** – Guidance created in 2007 providing an overview of assessment methodology used in evaluations/assessments, descriptions of what is necessary for an effective AML/CFT program, and guidance and interpretation concerning the methodology.
- **FATF Annual Report** – A publication created annually that summarizes the key achievements of FATF and its members, a summary of emerging risks, and strategic outcomes in the fight against money laundering and terrorist financing.
- **FATF Public Statements on High-Risk Jurisdictions of Concern** – Public statements that identify jurisdictions with strategic deficiencies after reviews of the AML/CTF infrastructure are conducted by FATF or a member organization. Public statements include suggested measures for mitigating risks associated with transactions involving identified jurisdictions.
- **Typologies Report** – A publication created annually that summarizes recent studies on various topics relating to money laundering and terrorist financing and conclusions of the annual meeting of select money laundering and terrorist financing experts.
- **Guidance on International Best Practices**
    - **Best Practices Paper: Confiscation (Recommendations 3 and 38)** – Guidance related to Recommendation 3 – Provisional Measures and Confiscation, and Recommendation 38 – Mutual Legal Assistance and Extradition, created in 2010, that summarizes methods of effective tracing and confiscation within each jurisdiction and internationally.
    - **International Best Practices: Detecting and Preventing the Illicit Cross-Border Transportation of Cash and Bearer Negotiable Instruments** – Guidance related to Special Recommendation IX, created in 2010, that summarizes the best preventive measures with regard to cross-border transport of monetary instruments.
    - **International Best Practices: Freezing of Terrorist Assets** – Guidance related to Special Recommendation III – Freezing and Confiscating Terrorist Assets, created in 2009, that summarizes effective methods of freezing terrorist-related funds or other assets.
    - **Combating the Abuse of Alternative Remittance Systems: International Best Practices Paper** – Guidance related to Special Recommendation VI: Alternative Remittance, created in 2004, that summarizes best practices to managing the risks of alternative remittance systems.
    - **Combating the Abuse of Non-Profit Organizations: International Best Practices Paper** – Guidance related to Special Recommendation VIII – Non-Profit Organizations, created in 2002, that summarizes best practices to managing the risks of nonprofit organizations.
- **Guidance on a Risk-Based Approach to Combat Money Laundering and Terrorist Financing**
    - **Operational Issues Financial Investigations Guidance** – A publication created in June 2012 that provides guidance on how to enhance the functions, responsibilities, powers and tools of law enforcement to effectively conduct money laundering, terrorist financing and asset-tracing investigations.
    - **Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing** – A publication created in July 2007 that provides high-level guidance for developing a risk-based approach to combating money laundering and terrorist financing.

- **Money Laundering and Terrorist Financing Risk Assessment Strategies** – A publication created in June 2008 that provides guidance on developing a risk-based approach to combating money laundering and terrorist financing.
- **RBA Guidance for Trust and Company Service Providers (TCSPs)** – A publication created in June 2008 that provides guidance on developing a risk-based approach to combating money laundering and terrorist financing for TCSPs (e.g., acting as a formation agent of legal persons; acting as [or arranging for another person to act as] a director or secretary of a company; providing a registered office; acting as [or arranging for another person to act as] a trustee of an express trust; acting as [or arranging for another person to act as] a nominee shareholder for another person).
- **RBA Guidance for Real Estate Agents** – A publication created in June 2008 that provides guidance on developing a risk-based approach to combating money laundering and terrorist financing for real estate agents.
- **RBA Guidance for Accountants** – A publication created in June 2008 that provides guidance on developing a risk-based approach to combating money laundering and terrorist financing for accountants.
- **High Level Principles and Procedures for Dealers in Precious Metals and Dealers in Precious Stones** – A publication created in July 2008 that provides guidance on developing a risk-based approach to combating money laundering and terrorist financing in the precious metals and precious stones industries.
- **Risk-Based Approach Guidance for Legal Professionals** – A publication created in October 2008 that provides guidance on the development of a risk-based approach to combating money laundering and terrorist financing for legal professionals.
- **Risk-Based Approach for Casinos** – A publication created in December 2008 that provides guidance on the development of a risk-based approach to combating money laundering and terrorist financing for casinos.
- **Guidance for Money Services Businesses** – **Risk-Based Approach** – A publication created in July 2009 that provides guidance on the development of a risk-based approach to combating money laundering and terrorist financing in money services businesses (MSBs).
- **Risk-Based Approach for the Life Insurance Sector** – A publication created in October 2009 that provides guidance on the development of a risk-based approach to combating money laundering and terrorist financing in the insurance sector.

- **Reports on Specific Industries**
  - **Illicit Tobacco Trade** – A report released in June 2012 to FATF and related international governing bodies detailing the risks posed by the global illicit tobacco trade.
  - **Specific Risk Factors in the Laundering of Proceeds of Corruption – Assistance to Reporting Institutions** – A publication created in June 2012 specifically to help reporting institutions in better analyzing and understanding risk factors for corruption-related money laundering, including politically exposed persons (PEPs).
  - **Laundering the Proceeds of Corruption** – A publication created in July 2011 that describes links between corruption and money laundering drawn from publically available expert resources and identifies key vulnerabilities within the current AML/CFT framework.
  - **Organized Maritime Piracy and Related Kidnapping for Ransom** – A publication created in July 2011 that examines the financial impact of these crimes, and current challenges with tracing the illicit flows associated with maritime piracy and kidnapping for ransom.
  - **Money Laundering Risks Arising from Trafficking of Human Beings and Smuggling of Migrants** – A study published in July 2011 describing the money flows from these issues and their potential scale.
  - **Money Laundering Using Trust and Company Service Providers** – A publication created in October 2010 that provides comprehensive analysis and evaluation of the effectiveness of FATF's Forty plus Nine Recommendations in relation to TCSPs, their role in the detection, prevention and prosecution of money laundering and terrorist financing, and the potential need for additional international requirements or sector-specific international standards.

- **The Misuse of Corporate Vehicles, Including Trust and Company Service Providers** – A publication created in October 2006 that details the methods of abusing corporate vehicles in money laundering and terrorist financing.
- **Money Laundering and Terrorist Financing Through the Real Estate Sector** – A publication created in May 2008 that details the vulnerabilities of the real estate sector.
- **Money Laundering of Casinos and Gaming Sector Report** – A publication created in March of 2009 that details the vulnerabilities of casinos and the gaming sector.
- **Money Laundering through the Football Sector** – A publication created in July 2009 that details the vulnerabilities of major sports organizations (e.g., football).
- **Money Laundering and Terrorist Financing in the Securities Sector** – A publication created in October 2009 that details the vulnerabilities of securities firms.

- **Reports Related to Various Payment Methods**
  - **Money Laundering Using New Payment Methods** – A publication created in 2010 that summarizes key risk factors that can be used to assess new payment methods (NPM), case studies and typologies involving NPMs and the ongoing challenges faced in developing appropriate legislation and regulations.
  - **Trade-Based Money Laundering** – A publication created in June 2006 that details the vulnerabilities of the international trade system.
  - **Report on New Payment Methods** – A publication created in October 2006 that details the vulnerabilities of emerging payment methods, including prepaid cards, Internet payment systems, mobile payments and digital precious metals.
  - **Money Laundering (ML) and Terrorist Financing (TF) Vulnerabilities of Commercial Websites and Internet Banking Systems** – A publication created in July 2008 that details the vulnerabilities of electronic commerce.
  - **Money Laundering Vulnerabilities of Free Trade Zones** – A publication created in March 2010 that details the vulnerabilities of more than 3,000 “free trade zones” – designated areas within countries that offer a free trade environment with minimal regulation – in more than 130 countries.
- **Reports Related to Terrorism**
  - **FATF Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion** – A publication released in June 2012 providing guidance on how governments can balance their national goal of financial inclusion of financially underserved populations without compromising measures taken to combat money laundering and terrorist financing efforts.
  - **Global Money Laundering and Terrorist Financing Threat Assessment** – A publication released in 2010 that presents a global overview of the systematic ML and TF threats, their potential negative impacts, and suggested steps for governments to take to mitigate the harm caused by these threats.
  - **Guidance for Financial Institutions in Detecting Terrorist Financing** – A publication created in 2002 that provides guidance to financial institutions in detecting terrorist financing, including, but not limited to, account opening and transaction red flags, common sources of funds for terrorist organizations (e.g., kidnapping, extortion, use of nonprofit organizations as front companies, skimming from legitimate businesses).
  - **FATF Terrorist Financing Report** – A publication created in February 2008 that analyzes the methods of raising and moving funds between terrorist organizations. The report also covers suggested controls for mitigating the risks of this activity.
  - **Typologies of Proliferation Financing** – A publication created in August 2008 that analyzes the threat of “proliferation financing” – financing that facilitates the movement and development of proliferation-sensitive items (e.g., weapons of mass destruction) by exploiting global commerce by masking acquisitions as legitimate trade, abusing free trade zones and operating in countries with weak export controls. The report covers methods of financing and suggested controls for mitigating the risks of this activity.

FATF Recommendations

1705. What are the key sections of the FATF's Updated Recommendations?

FATF's Recommendations are organized into seven main categories:

A. AML/CTF Policies and Coordination (Recommendations 1 and 2):

- Assessing risks and applying a risk-based approach
- National cooperation and coordination

B. Money Laundering and Confiscation (Recommendations 3 and 4):

- Money laundering offense
- Confiscation and provisional measures

C. Terrorist Financing and Financing of Proliferation (Recommendations 5 through 8):

- Terrorist financing offense and sanctions related to terrorism, terrorist financing and proliferation
- Nonprofit organizations

D. Preventive Measures (Recommendations 9 through 23):

- Financial institution secrecy laws
- Customer due diligence and recordkeeping
- Additional measures for specific customers and activities (e.g., high-risk customers)
- Reliance, controls and financial groups
- Reporting of suspicious transactions
- Designated nonfinancial businesses and professions (DNFBPs)

E. Transparency and Beneficial Ownership of Legal Persons and Arrangements (Recommendations 24 and 25):

- Transparency and beneficial ownership of legal persons

F. Powers and Responsibilities of Competent Authorities and Other Institutional Measures (Recommendations 26 through 35):

- Regulation and supervision of financial institutions
- Operational and law enforcement
- General requirements
- Sanctions

G. International Cooperation (Recommendations 36 through 40):

- International instruments
- Mutual legal assistance, freezing and confiscation, extradition and other forms of international cooperation

1706. What were the major changes between the Forty plus Nine Recommendations and the revised FATF Recommendations?

There were no significant changes to the content or objectives of the Recommendations. The changes were a consolidation of the Forty plus Nine Recommendations, and reorganization into categories that are more consistent with emerging money laundering and terrorist financing trends.

Number	Old Number	Recommendations	Section	Subtopic
1	NA	Assessing risks and applying a risk-based approach	A	AML/CFT POLICIES AND COORDINATION
2	R.31	National cooperation and coordination	A	AML/CFT POLICIES AND COORDINATION
3	R.1 and R.2	Money laundering offense	B	MONEY LAUNDERING AND CONFISCATION
4	R.3	Confiscation and provisional measures	B	MONEY LAUNDERING AND CONFISCATION
5	SRII	Terrorist financing offense	C	TERRORIST FINANCING AND FINANCING OF PROLIFERATION
6	SRIII	Targeted financial sanctions related to terrorism and terrorist financing	C	TERRORIST FINANCING AND FINANCING OF PROLIFERATION
7	NA	Targeted financial sanctions related to proliferation	C	TERRORIST FINANCING AND FINANCING OF PROLIFERATION
8	SRVIII	Nonprofit organizations	C	TERRORIST FINANCING AND FINANCING OF PROLIFERATION
9	R.4	Financial institution secrecy laws	D	PREVENTIVE MEASURES
10	R.5	Customer due diligence	D	PREVENTIVE MEASURES
11	R.10	Recordkeeping	D	PREVENTIVE MEASURES
12	R.6	PEPs	D	PREVENTIVE MEASURES
13	R.7	Correspondent banking	D	PREVENTIVE MEASURES
14	SRVI	Money or value transfer services	D	PREVENTIVE MEASURES
15	R.8	New technologies	D	PREVENTIVE MEASURES
16	SRVII	Wire transfers	D	PREVENTIVE MEASURES
17	R.9	Reliance on third parties	D	PREVENTIVE MEASURES
18	R.15 and R.22	Internal controls and foreign branches and subsidiaries	D	PREVENTIVE MEASURES
19	R.21	Higher-risk countries	D	PREVENTIVE MEASURES
20	R.13 and SRIV	Reporting of suspicious transactions	D	PREVENTIVE MEASURES
21	R.14	Tipping-off and confidentiality	D	PREVENTIVE MEASURES
22	R.12	DNFBPs: Customer due diligence	D	PREVENTIVE MEASURES
23	R.16	DNFBPs: Other measures	D	PREVENTIVE MEASURES
24	R.33	Transparency and beneficial ownership of legal persons	E	TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS
25	R.34	Transparency and beneficial ownership of legal arrangements	E	TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS
26	R.23	Regulation and supervision of financial institutions	F	POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES

Number	Old Number	Recommendations	Section	Subtopic
27	R.29	Powers of supervisors	F	POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
28	R.24	Regulation and supervision of DNFBPs	F	POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
29	R.26	Financial Intelligence Units	F	POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
30	R.27	Responsibilities of law enforcement and investigative authorities	F	POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
31	R.28	Powers of law enforcement and investigative authorities	F	POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
32	SRIX	Cash couriers	F	POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
33	R.32	Statistics	F	POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
34	R.25	Guidance and feedback	F	POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
35	R.17	Sanctions	F	POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
36	R.35 and SRI	International instruments	G	INTERNATIONAL COOPERATION
37	R.36 and SRV	Mutual legal assistance	G	INTERNATIONAL COOPERATION
38	R.38	Mutual legal assistance: Freezing and confiscation	G	INTERNATIONAL COOPERATION
39	R.39	Extradition	G	INTERNATIONAL COOPERATION
40	R.40	Other forms of international cooperation	G	INTERNATIONAL COOPERATION

1707. Are the Recommendations applicable only to financial institutions?

No. The Recommendations are applicable to DNFBPs and regulatory and law enforcement authorities in addition to financial institutions.

1708. Which of the Recommendations are applicable to financial institutions?

All of the Recommendations affect financial institutions, either directly through specific guidance for customer due diligence (CDD) programs, recordkeeping and suspicious transaction reporting or indirectly by establishing the legal and regulatory frameworks in which financial institutions must operate. The Recommendations related directly to CDD, recordkeeping and suspicious transaction reporting are Recommendations 4 through 25.

Definitions

1709. Has the definition of "financial institution" by FATF changed?

No. FATF still defines the term "financial institution" as any person or entity who/that conducts, as a business, one or more of the following activities or operations for, or on behalf of, a customer:

- Acceptance of deposits and other repayable funds from the public (inclusive of private banking)
- Lending (e.g., consumer credit, mortgage credit, factoring)
- Financial leasing (not including financial leasing arrangements in relation to consumer products)
- The transfer of money or value, in both the formal and informal or underground sectors (i.e., informal value transfer systems)
- Issuing and managing means of payment (e.g., credit and debit cards, checks, traveler's checks, money orders, banker's drafts, electronic money)
- Financial guarantees and commitments
- Trading in:
    - Money market instruments (e.g., checks, bills, CDs, derivatives)
    - Foreign exchange
    - Exchange, interest rate and index instruments
    - Transferable securities
    - Commodity futures trading
- Participation in securities issues and the provision of financial services related to such issues
- Individual and collective portfolio management
- Safekeeping and administration of cash or liquid securities on behalf of other persons
- Otherwise investing, administering or managing funds or money on behalf of other persons
- Underwriting and placement of life insurance and other investment-related insurance (applies to both insurance undertakings and to insurance intermediaries [e.g., agents, brokers])
- Money and currency changing

1710. Has the definition of "designated nonfinancial business and profession" by FATF changed?

No. FATF still defines designated nonfinancial businesses and professions (DNFBPs) as the following:

- Casinos (including online casinos)
- Real estate agents
- Dealers in precious metals
- Dealers in precious stones
- Lawyers, notaries, other independent legal professionals and accountants
    - Refers to sole practitioners, partners or employed professionals within professional firms; it is not meant to refer to professionals who are employees of other types of businesses, nor to professionals working for government agencies who already may be subject to measures that would combat money laundering and terrorist financing
- Trust and company service providers
    - Refers to all persons or businesses who are not covered elsewhere under the Recommendations, and which, as a business, provide any of the following services to third parties:

- Acting as a formation agent of legal persons
- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons
- Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement
- Acting as (or arranging for another person to act as) a trustee of an express trust
- Acting as (or arranging for another person to act as) a nominee shareholder for another person

1711. Should all financial institutions and DNFBPs described above be subject to the Recommendations?

A country may decide that the application of a measure is not necessary, either fully or partially, to a particular type or size of financial institution. For example, in the United States, quantitative thresholds are included in some of the definitions of financial institutions that are subject to AML requirements (e.g., an MSB must conduct US$1,000 or more in MSB activity with the same person ([in one type of activity] on the same day to be subject to AML requirements).

However, if a country decides to limit the scope of financial institutions obligated to comply with AML requirements, the reasoning must be justified and risk-based (i.e., low risk for money laundering and terrorist financing). For additional guidance on how the United States applies AML requirements to the various types of financial and nonfinancial institutions, please refer to the Bank Secrecy Act, USA PATRIOT Act, and Nonbank Financial Institutions and Nonfinancial Businesses sections.

1712. Has the definition for "politically exposed person" (PEP) by FATF changed?

Yes. FATF has expanded the definition of a PEP by breaking it down into two categories: foreign PEPs and domestic PEPs.

Foreign PEPs are defined as individuals who are or have been entrusted with prominent public functions in a foreign country (e.g., heads of state, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials). FATF also states that business relationships with family members or close associates of PEPs have similar reputational risks to PEPs themselves, and therefore should be included in the definition of PEP, as well.

FATF advises that the definition of PEP was not meant to include junior- or middle-ranking individuals in the categories mentioned above. FATF also suggests that persons who are or have been entrusted with a prominent function by an international organization (e.g., deputy directors, and members of the board or equivalent functions) be considered in the definition of PEP.

Domestic PEPs are individuals who are, or have been, entrusted domestically with prominent public functions (e.g., heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials).

1713. Did FATF amend the "designated categories of offenses for money laundering"?

Yes. As part of its ongoing efforts to identify new methods of money laundering and the associated sources of illicit funds, in 2012 FATF added "Tax Offenses" to the list of potential predicate crimes. Otherwise, the term "designated categories of offenses for money laundering" is defined as activities that should be considered as predicate crimes to money laundering. FATF's designated categories of offenses include the following:

- Participation in an organized criminal group and racketeering
- Terrorism, including terrorist financing
- Trafficking in human beings and migrant smuggling
- Sexual exploitation, including sexual exploitation of children
- Illicit trafficking in narcotic drugs and psychotropic substances
- Illicit arms trafficking
- Illicit trafficking in stolen and other goods

- Corruption and bribery
- Fraud
- Counterfeiting currency
- Counterfeiting and piracy of products
- Environmental crime
- Murder, grievous bodily injury
- Kidnapping, illegal restraint and hostage-taking
- Robbery or theft
- Smuggling (including in relation to customs and excise duties and taxes)
- Tax crimes (related to direct taxes and indirect taxes)
- Extortion
- Forgery
- Piracy
- Insider trading and market manipulation

1714. Should all categories of offenses be included within a country's definition of predicate offenses?

Each country may decide, in accordance with its domestic law, the range of offenses to be covered as predicate offenses under each of the above categories. Some countries have opted to define these offenses by listing activities designated as serious offenses, by minimum penalty of imprisonment (e.g., one year imprisonment), or by a combination of these approaches.

1715. Does FATF provide guidance on "thresholds" for determining when due diligence is required?

FATF defines the designated threshold as the minimum amount of a transaction or a series of transactions that should prompt CDD, recordkeeping and/or suspicious activity reporting requirements.

FATF suggests the following designated thresholds:

- For transactions conducted by financial institutions under Recommendation 10: USD/EUR 15,000
- For transactions conducted by casinos under Recommendation 22: USD/EUR 3,000
- For transactions conducted by dealers in precious metals and stones when engaged in any cash transaction under Recommendations 22 and 23: USD/EUR 15,000

High-Risk and Non-Cooperative Jurisdictions

1716. What are "Non-Cooperative Countries and Territories"?

Non-Cooperative Countries and Territories (NCCT) was a term used to describe jurisdictions designated by FATF that had detrimental rules and practices that seriously hampered the international fight against money laundering and terrorist financing. Since FATF revised its International Co-operation Review Group (ICRG) procedures in 2010, the term was changed from "Non-Cooperative Countries and Territories" to "High-Risk and Non-Cooperative Jurisdictions."

1717. How does FATF define “High-Risk and Non-Cooperative Jurisdictions”?

High-Risk and Non-Cooperative Jurisdictions describe two primary groups:

- Group 1: Jurisdictions with strategic AML/CFT deficiencies subject to a FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the ongoing and substantial money laundering and terrorist financing risks emanating from the jurisdictions; and
- Group 2: Jurisdictions with strategic AML/CFT deficiencies that either:
    - Have not made sufficient progress in addressing the deficiencies; or
    - Have not committed to an action plan developed with FATF to address the deficiencies.

1718. Why did FATF change from “Non-Cooperative Countries and Territories” to “High-Risk and Non-Cooperative Jurisdictions”?

In 2006, FATF removed the last country from the NCCT designation (Myanmar, formerly Burma). From 2007 through 2010, FATF continued to evaluate countries and jurisdictions, but without any being considered “non-cooperative” the focus shifted to ensuring that existing programs were effective and efficient.

In 2009, FATF issued procedures for the ICRG at the request of member countries, and in 2010 released its identification of “High-Risk Jurisdictions and Non-Cooperative Territories.”

1719. What is the difference between a “High-Risk Jurisdiction” and a “Non-Cooperative Jurisdiction”?

FATF has not articulated a clear distinction between the two designations. It appears, however, that the level of engagement and degree of cooperation demonstrated by the jurisdiction under review will determine if a jurisdiction is identified as “high-risk” or as “non-cooperative.”

1720. When and where does FATF identify “High-Risk and Non-Cooperative Jurisdictions”?

FATF provides updates on designated “High-Risk and Non-Cooperative Jurisdictions” in two public documents:

- FATF Public Statements, published three times a year: in February, June and October; and
- “Improving Global AML/CFT Compliance: Ongoing Process,” which is released once a year and focuses specifically on jurisdictions that have deficiencies but also a political commitment to improvement.

A list of these jurisdictions is available on the FATF website: http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/

1721. What are the consequences of being a FATF designated High-Risk or Non-Cooperative Jurisdiction?

FATF’s previous Recommendation 21 recommended that countries exercise caution and conduct enhanced due diligence when developing business relationships or conducting transactions with any person, company or financial institution from a country or territory listed as NCCTs, now referred to as “High-Risk or Non-Cooperative.”

Today, the same principle applies under the new Recommendation 19: Higher-Risk Countries. As a result, a jurisdiction’s designation by FATF can cause significant adverse consequences for its financial development as businesses and financial institutions will have limited access to financial world markets. Additionally, FATF calls for countries to take “countermeasures” against any listed jurisdiction not taking the necessary steps to correct their AML/CFT deficiencies.

A financial institution in the United States should review the FATF Public Statements on High-Risk and Non-Cooperative Jurisdictions to determine whether the customer located in such country or doing business in such country should be considered high-risk for purposes of its AML Compliance Program.

1722. What additional countermeasures did FATF suggest member countries take against "High-Risk or Non-Cooperative Jurisdictions" beyond Recommendation 19?

FATF suggests reviewing the public reports to identify the specific deficiencies of each country, and developing countermeasures accordingly. However, in general, FATF advises that effective countermeasures include:

- Enhanced due diligence (EDD) requirements on customers and beneficial owners of individuals or businesses within designated countries before establishing account relationships
- More intensive monitoring of transactions involving designated countries
- Consideration of location of relevant designated countries' financial institutions when approving establishment of subsidiaries, branches or representative offices in member countries
- Informing nonfinancial sector businesses of the heightened money laundering and terrorist financing risk of entities within designated countries

1723. When did the process for designating countries as "High-Risk or Non-Cooperative" begin?

FATF began assessing select nonmember countries and territories in 1998. It was not until 2000 that the NCCT process was formalized by the issuance of reports listing NCCTs as well as the framework, procedures and criteria used to designate NCCTs. After the last NCCT country was removed in 2006, FATF continued using MERs to assess countries based on their effectiveness and efficiency in implementing laws and sustaining measures to mitigate money laundering and terrorist financing. Additionally, FATF began issuing public statements expressing concerns over some jurisdictions. In 2009, the Group of 20 (G20) formally requested that FATF resume the process of designating high-risk jurisdictions. This process resumed in 2010, after issuing formal ICRG procedures in 2009.

1724. What is the process of designating a jurisdiction as "High-Risk or Non-Cooperative"?

In 2009, FATF established the ICRG, which produces procedures governing the reviews of select countries and territories. The review of countries by the ICRG begins with the results of a country's MER. Those with identified deficiencies are referred to the ICRG. The ICRG procedures are not published for the public; however, the MER details are outlined in the section below, and it is known that FATF continues to assess countries against the Forty plus Nine Recommendations, even though the new FATF Recommendations have been released.

1725. How are countries and territories selected for review?

Countries are selected for review based on a number of factors. The primary factor is the result of a country's MER, but in addition, FATF may consider a member's experience and the interests of other member nations when determining which countries to refer to the ICRG. Generally, larger financial centers and countries with a history of being uncooperative are reviewed first. However, FATF cautions that certain jurisdictions with deficient AML regimes may not be immediately selected for review because they are not prioritized by FATF members.

1726. Who conducts the reviews of selected "High-Risk or Non-Cooperative Jurisdictions"?

FATF established the International Cooperation Review Group (ICRG), which is a specialized body with the designated responsibility of reviewing "High-Risk or Non-Cooperative Jurisdictions." The ICRG may include representatives from FATF and other regional groups (e.g., the Review Group on Asia/Pacific, the Review Group on the Americas, Europe and Africa/Middle East) consisting of representatives from FATF member governments that act as a conduit of information between the reviewed country or territory and FATF.

1727. What countries have been designated as "High-Risk or Non-Cooperative Jurisdictions"?

As of October 19, 2012, two countries were placed in Group 1: jurisdictions with strategic AML/CFT deficiencies subject to a FATF call on its members and other jurisdictions to apply countermeasures to protect the international financial system from the ongoing and substantial money laundering and terrorist financing risks emanating from the jurisdictions:

- Iran
- Democratic People's Republic of Korea (DPRK)

Seventeen jurisdictions were placed in Group 2: jurisdictions with strategic AML/CFT deficiencies that either have not made sufficient progress in addressing the deficiencies, or have not committed to an action plan developed with FATF to address the deficiencies:

- Bolivia
- Cuba
- Ecuador
- Ethiopia
- Indonesia
- Kenya
- Myanmar
- Nigeria
- Pakistan
- São Tomé and Príncipe
- Sri Lanka
- Syria
- Tanzania
- Thailand
- Turkey
- Vietnam
- Yemen

1728. What other countries have been designated by FATF as requiring additional consideration of risk by other member nations?

As of October 19, 2012, FATF identified 22 jurisdictions currently undergoing ongoing processes to improve global AML/CFT compliance as requiring consideration of additional risk. These jurisdictions are currently being closely monitored by FATF (or an appropriate FSRB) to help ensure appropriate implementation of corrective action:

- Afghanistan
- Albania
- Algeria
- Angola
- Antigua and Barbuda
- Argentina
- Bangladesh
- Brunei Darussalam
- Cambodia
- Ghana
- Kuwait
- Kyrgyzstan
- Mongolia
- Morocco
- Namibia
- Nepal
- Nicaragua
- Philippines
- Sudan
- Tajikistan
- Trinidad and Tobago
- Venezuela

1729. How is a country or territory removed from designation as a "High-Risk or Non-Cooperative Jurisdiction"?

Once designated, a jurisdiction must periodically report on its progress in plenary meetings (e.g., recent AML reforms, implementation plans), and submit to ongoing monitoring by the ICRG in order to first be designated as making progress in its efforts to remediate deficiencies.

FATF then performs on-site visits to ensure effective implementation of the recent AML reforms. Once the ICRG is satisfied that sufficient steps have been taken, recommendations for delisting are made at plenary meetings, and jurisdictions are identified as no longer requiring ongoing monitoring (e.g., Trinidad and Tobago in 2012).

1730. Can a financial institution assume that a country is compliant with the FATF Recommendations or has a strong AML infrastructure if it's not listed as an NCCT or a "High-Risk or Non-Cooperative Jurisdiction"?

No. While FATF's designations help member nations to identify the countries and jurisdictions with particularly weak AML/CFT programs, the mutual evaluation process may identify instances of compliance with the Recommendations of member countries. However, if a jurisdiction is not designated by FATF as "High-Risk or Non-Cooperative," a U.S. financial institution may want to assess the volume of business activity such jurisdiction conducts with other member nations to determine the specific level of risk to which it is exposed.

1731. How does FATF deal with noncomplying members?

FATF's actions include:

- Sending a letter from the FATF president or high-level mission to the noncomplying member country to apply peer pressure so that the jurisdiction takes action to tighten its AML system
- Requiring that the noncomplying member country deliver progress reports at plenary meetings
- Referral to the ICRG for the development of corrective action plans, and continued monitoring
- Calling upon international financial institutions to perform scrutiny on business relations and transactions with persons, companies and financial institutions in the noncomplying member country
- Suspending membership

Members and Observers

1732. What criteria must be met for a country to become a member of FATF?

In order to qualify for membership in FATF, a country must:

- Be strategically important
- Be a full and active member of a relevant FSRB
- Provide a letter from a minister or a person who is of equal political level, making a political pledge to implement the Recommendations within a reasonable time frame and to be able to undergo the mutual evaluation process
- Effectively criminalize money laundering and terrorist financing
- Make it mandatory for financial institutions to identify their customers, maintain customer records and report suspicious transactions
- Establish a Financial Intelligence Unit (FIU)

1733. What is the benefit of becoming a member of FATF?

Countries and territories listed as being FATF members are recognized as being compliant, or largely compliant, with international AML and counterterrorist financing practices. Membership in FATF, therefore, provides comfort that a jurisdiction is operating under a sound AML regime; however, it is not a guarantee that all of the companies operating in that jurisdiction are fully compliant with all requirements.

1734. Which jurisdictions are currently members of FATF?

As of October 2012, there were 36 members of FATF, 34 member jurisdictions and two regional organizations. This includes the following:

- Argentina
- Australia
- Austria
- Belgium
- Brazil
- Canada
- China
- Denmark
- European Commission
- Finland
- France
- Germany
- Greece
- Gulf Cooperation Council
- Hong Kong
- Iceland
- India
- Ireland
- Italy
- Japan
- The Kingdom of the Netherlands
- Luxembourg
- Mexico
- New Zealand
- Norway
- Portugal
- Republic of South Korea
- Russian Federation
- Singapore
- South Africa
- Spain
- Sweden
- Switzerland
- Turkey
- United Kingdom
- United States

1735. What is an observer of FATF?

Being an observer can be the first step on the path toward becoming a member of FATF. Observers include FSRBs with similar functions to FATF. Some FATF members are also members of these organizations. Some are international organizations that have specific money laundering missions or functions.

1736. How does a country or territory become an observer of FATF?

To receive observer status, a country or territory must first make a request to FATF for consideration. The potential observer must have an AML infrastructure (e.g., criminal and regulatory framework) in place or plans for the development of such an infrastructure. The observer status can only be granted by the consensus of FATF members at one of the organization's three annual meetings.

1737. Which countries and regional organizations are currently observers of FATF?

As of October 2012, the following countries and regional organizations are observers of FATF:

- African Development Bank
- Anti-Money Laundering Liaison Committee of the Franc Zone
- INTERPOL
- INTERPOL/Money Laundering

- Basel Committee on Banking Supervision (BCBS)
- Commonwealth Secretariat
- Egmont Group of Financial Intelligence Units
- European Bank for Reconstruction and Development (EBRD)
- European Central Bank (ECB)
- Eurojust
- Europol
- Inter-American Development Bank (IDB)
- International Association of Insurance Supervisors (IAIS)
- International Monetary Fund (IMF)
- International Organisation of Securities Commissions (IOSCO)
- Organization of American States/Inter-American Committee Against Terrorism (OAS/CICTE)
- Organization of American States/Inter-American Drug Abuse Control Commission (OAS/CICAD)
- Organisation for Economic Co-operation and Development (OECD)
- Offshore Group of Banking Supervisors (OGBS)
- Task Force on Money Laundering in Central Africa
- United Nations (UN)
- UN Office on Drugs and Crime (UNODC)
- Counter-Terrorism Committee of the Security Council (UNCTC)
- The Al-Qaida and Taliban Sanctions Committee (1267 Committee)
- World Bank (WB)
- World Customs Organization (WCO)

1738. How can a country transition from being an observer to membership in the FATF?

The process of an observer obtaining member status takes approximately two years and depends on the results of a mutual evaluation. For additional guidance on mutual evaluations, please see the Mutual Evaluations section.

1739. Who are the associate members of FATF?

As of October 2012, associate members of FATF include the following regional bodies that share FATF's goals:

- The Asia/Pacific Group on Money Laundering (APG)
- Caribbean Financial Action Task Force (CFATF)
- Eurasian Group (EAG)
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
- The Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) – formerly PC-R-EV
- The Financial Action Task Force on Money Laundering in South America (GAFISUD)
- Intergovernmental Anti-Money Laundering Group in Africa (GIABA)
- Middle East and North Africa Financial Action Task Force (MENAFATF)

1740. What are FSRBs?

FSRBs are international bodies and organizations that have observer status with FATF. Some FATF members are also members of FSRBs.

As of October 2012, FSRBs include the following:

- The Asia/Pacific Group on Money Laundering (APG)
- Caribbean Financial Action Task Force (CFATF)
- Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG)
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
- Intergovernmental Anti-Money Laundering Group in Africa (GIABA)
- The Financial Action Task Force on Money Laundering in South America (GAFISUD)
- Middle East and North Africa Financial Action Task Force (MENAFATF)
- The Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) – formerly PC-R-EV

Mutual Evaluations

1741. How does FATF ensure that all of its member countries are in compliance with the FATF Recommendations?

FATF relies heavily on the various enforcement agencies within each country (e.g., within the United States, it would be FinCEN and the federal financial regulators such as the Office of the Comptroller of the Currency). In addition, FATF members agree to conduct mutual evaluations of their AML/CFT systems to ensure compliance with the Forty plus Nine Recommendations. Each member agrees to be evaluated by an internationally accepted assessment methodology.

Within FATF, the Working Group on Evaluations and Implementation (WGEI) administers the mutual evaluation process. They monitor, coordinate and review the mutual evaluation procedures, develop interpretation and provide guidance to the Recommendations, develop and coordinate the training of new assessors, and serve as the point of contact between FATF, the OGBS, the IMF and the WB.

1742. Has FATF released guidance on the mutual evaluation process?

Yes. FATF has issued the *AML/CFT Evaluations and Assessments: Handbook for Countries and Assessors*, April 2009. This guidance provides an overview of the assessment methodology used in evaluations/assessments, descriptions of what is necessary for an effective AML/CFT program, and guidance and interpretation concerning the methodology.

1743. Does the MER assess or evaluate anything besides compliance with the Recommendations?

Yes. Through assessment of adherence to the Recommendations, FATF is also able to perform an in-depth evaluation of a country's system for preventing criminal abuse of the financial system; it helps FATF to quantify each country's risk exposure to money laundering and terrorist financing, among other financial crimes.

1744. Did the process for mutual evaluations change along with the new Recommendations?

The mutual evaluation process is designed to measure and evaluate the implementation progress of the Recommendations. Since the Recommendations were consolidated, and fundamentally remain unchanged, the evaluation process largely remains the same. It still involves the following:

- The completion of a mutual evaluation questionnaire, a self-assessment exercise in which each member country provides information on the status of its implementation of the Forty plus Nine Recommendations

- An on-site visit, in which each member country is examined for compliance by a select team of legal, financial and law enforcement experts from other member governments
- The preparation of a MER describing the findings and the effectiveness of the member country's AML/CFT system, which is made available on the FATF website
- Submission of follow-up reports two years after the evaluation indicating the member country's progress since the mutual evaluation, with particular focus on the areas of improvement identified in the mutual evaluation

For some countries that have already received a MER, FATF is now issuing a "Follow-Up Report to the Mutual Evaluation Report," which frequently highlights a country's progress in implementing corrective action to address deficiencies and further develop enhancements to laws, regulatory expectations, control processes and so forth, for adherence to the Recommendations.

1745. How long does the mutual evaluation process take?

The mutual evaluation process takes approximately 10 months to one year to complete per country. This includes the time it takes for the jurisdiction to complete the pre-on-site self-assessment questionnaire, and for the reviewers to conduct the on-site visit, draft the preliminary and final reports and discuss findings with FATF and the country under review. The timeline varies slightly from one evaluation to the next. It may be affected by factors such as the date at which the plenary will next meet and endorse the final draft report.

1746. Who conducts the mutual evaluation?

Mutual evaluations are conducted by FSRBs, the IMF and the WB. Each evaluation team consists of a minimum of four experts, plus two members of the FATF Secretariat. This includes:

- One member with legal expertise (e.g., judge, prosecutor)
- Two members with financial sector expertise (e.g., regulator) and experience with both financial institutions and nonfinancial DNFBPs
- One law enforcement professional (e.g., police, customs, FIU)

Additional experts may be added, depending on the size or complexity of the country under review.

The evaluation team typically consists of members drawn from countries that have a history, understanding and close relationship with the country being evaluated.

1747. How are the assessors trained to conduct mutual evaluations?

A five-day training session is provided for prospective assessors by FATF, FSRBs, the IMF and the WB to ensure assessors have the same level of knowledge to conduct the assessment.

1748. Who is interviewed by the assessors? How are they selected?

The FATF Evaluation Team interviews representatives from ministries, criminal justice and operational entities, and financial sector bodies selected across geographic regions as well as industry lines (e.g., casinos, insurance industry). A detailed program for the on-site visit portion of a mutual evaluation is devised in consultation with the country being evaluated. The details of the meeting (e.g., timing, interviewees) are determined with consideration to the particular nature of the country, its risks and industries.

1749. Are the results of the mutual evaluation available to the public?

Yes. In 2005, FATF began publishing the MERs on its website: www.fatf-gafi.org. Today, FATF is publishing the "Follow-Up Report to the Mutual Evaluation Report" for countries already reviewed at least once, and continues to publish MERs for countries that have not previously been evaluated (e.g., new member countries).

1750. What are key factors used when assessing compliance with the Recommendations?

While the categories have changed slightly with the consolidation of the Recommendations, the key factors used when assessing compliance largely remain the same. It is important to note that the FATF Recommendations are applicable to criminal justice systems and regulatory authorities in addition to financial institutions. Different factors are considered when assessing applicable Recommendations relevant to each area.

The following factors may be considered to assess overall compliance of a country's AML infrastructure with the Recommendations:

- Range of money laundering and terrorist financing predicate offenses
- Evidentiary standards applied to money laundering/terrorist financing offenses
- Number and nature of precondition(s) required prior to providing mutual assistance (e.g., dual criminality, treaty, secrecy provisions)
- Quantity and quality of Suspicious Transaction Reports (STRs)
- Number of money laundering/terrorist financing investigations initiated
- Number of prosecutions
- Number of convictions
- Existence of penalties for failures of compliance
- Number and amount of penalties
- Existence of mechanisms to freeze/seize criminal proceeds
- Existence of sanctions for failure to freeze/confiscate assets
- Number of cases where sanctions have been applied
- Number and amount of frozen/seized assets
- Number of resources within regulatory and law enforcement authorities
- Expertise of resources
- Number, frequency and duration of examinations conducted by regulatory authorities
- Failures identified in financial institutions in examinations by regulatory authorities
- Information sharing (e.g., between FIU, financial institutions, law enforcement)
- Quality of coordination between financial institutions, regulatory and law enforcement authorities

With the consolidation of the Recommendations, FATF will now be able to determine how effectively a country may be at the following:

- Facilitating international cooperation;
- Leveraging existing processes to increase transparency around customer and transaction information; and
- Preventing the proliferation of money laundering and terrorist financing.

1751. Have there been any changes to the rating scale used to assess compliance with the new Recommendations?

No. FATF still uses the following rating scale to assess compliance with the Recommendations:

- **Compliant** – The Recommendation is fully observed with respect to all criteria.
- **Largely Compliant** – There are only minor shortcomings, with a large majority of the essential criteria being fully met.
- **Partially Compliant** – The country has taken some substantive steps and complies with some of the essential criteria.
- **Noncompliant** – There are major shortcomings with a large majority of essential criteria not being met.
- **Not Applicable** – A requirement, or part of the requirement, does not apply due to structural, legal or institutional features of the country.

1752. What have been the results of MERs conducted in recent years?

Based on the most recent MERs conducted between 2008 and 2010 on 34 member countries – Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Finland, France, Germany, Greece, Hong Kong, Iceland, India, Ireland, Italy, Japan, Kingdom of Denmark, Kingdom of the Netherlands, Luxembourg, Mexico, New Zealand, Norway, Portugal, Republic of Korea, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom and the United States – the overall ratings were as follows:

No.	Recommendation	Compliant	Largely Compliant	Partially Compliant	Noncompliant	N/A
R1	Money Laundering Offense	9%	68%	24%	0%	0%
R2	Money Laundering Offense – Mental Element and Corporate Liability	18%	62%	21%	0%	0%
R3	Confiscation and Provisional Measures	21%	56%	24%	0%	0%
R4	Secrecy Laws Consistent with Recommendations	74%	18%	9%	0%	0%
R5	Customer Due Diligence	0%	32%	50%	18%	0%
R6	Politically Exposed Persons	0%	35%	24%	41%	0%
R7	Correspondent Banking	9%	35%	18%	38%	0%
R8	New Technologies and Non-Face-to-Face Business	18%	41%	32%	9%	0%
R9	Third Parties and Introducers	3%	18%	24%	32%	24%
R10	Recordkeeping	41%	47%	12%	0%	0%
R11	Unusual Transactions	12%	38%	41%	9%	0%
R12	Designated Nonfinancial Businesses and Professions – R.5,6,8-11	0%	12%	29%	59%	0%
R13	Suspicious Transaction Reporting	6%	62%	29%	3%	0%
R14	Protection and No Tipping-Off	62%	24%	15%	0%	0%

No.	Recommendation	Compliant	Largely Compliant	Partially Compliant	Noncompliant	N/A
R15	Internal Controls, Compliance and Audit	0%	56%	35%	9%	0%
R16	Designated Nonfinancial Businesses and Professions – R. 13-15, 21	0%	15%	38%	47%	0%
R17	Sanctions	0%	38%	56%	6%	0%
R18	Shell Banks	26%	35%	35%	3%	0%
R19	Other Forms of Reporting	88%	6%	3%	3%	0%
R20	Other Nonfinancial Businesses and Professions and Secure Transaction Techniques	68%	24%	6%	3%	0%
R21	Special Attention for Higher Risk Countries	9%	35%	32%	24%	0%
R22	Foreign Branches and Subsidiaries	6%	41%	26%	26%	0%
R23	Regulation, Supervision and Monitoring	0%	50%	47%	3%	0%
R24	Designated Nonfinancial Businesses and Professions – Regulation, Supervision and Monitoring	0%	15%	29%	56%	0%
R25	Guidelines and Feedback	12%	38%	44%	6%	0%
R26	Financial Intelligence Unit	12%	74%	15%	0%	0%
R27	Law Enforcement Unit	35%	53%	12%	0%	0%
R28	Powers of Competent Authorities	71%	29%	0%	0%	0%
R29	Supervisors	6%	59%	29%	6%	0%
R30	Resources, Integrity and Training	3%	56%	35%	6%	0%

No.	Recommendation	Compliant	Largely Compliant	Partially Compliant	Noncompliant	N/A
R31	National Cooperation	18%	74%	9%	0%	0%
R32	Statistics	0%	56%	35%	9%	0%
R33	Legal Persons - Beneficial Owners	3%	9%	56%	32%	0%
R34	Legal Arrangements - Beneficial Owners	0%	6%	41%	21%	32%
R35	Conventions	6%	59%	35%	0%	0%
R36	Mutual Legal Assistance	21%	68%	12%	0%	0%
R37	Dual Criminality	65%	29%	6%	0%	0%
R38	Mutual Legal Assistance on Confiscation and Freezing	24%	59%	18%	0%	0%
R39	Extradition	26%	65%	9%	0%	0%
R40	Other Forms of International Cooperation	44%	53%	0%	3%	0%
SR1	Implement United Nations Instruments	3%	41%	53%	3%	0%
SR2	Criminalize Terrorist Financing	15%	53%	29%	3%	0%
SR3	Freeze and Confiscate Terrorist Assets	3%	26%	56%	15%	0%
SR4	Suspicious Transaction Reporting	12%	59%	21%	9%	0%
SR5	International Cooperation	9%	68%	24%	0%	0%
SR6	AML Requirements for Money/Value Transfer Services	6%	47%	32%	15%	0%

No.	Recommendation	Compliant	Largely Compliant	Partially Compliant	Noncompliant	N/A
SR7	Wire Transfer Rules	12%	32%	32%	24%	0%
SR8	Nonprofit Organizations	9%	38%	35%	18%	0%
SR9	Cross-Border Declaration and Disclosure	9%	35%	35%	21%	0%

The following areas are some of the common deficiencies that have been identified in the MERs:

- Ineffective CDD programs that are inconsistent with FATF standards, not tailored to particular customer types, exempt a significant number of customers, and fail to identify ultimate beneficial ownership in legal persons and legal arrangements
- Inadequate processes to manage risks associated with correspondent banking customers
- Inadequate processes to identify and manage risks associated with PEPs
- Inadequate processes to manage risks associated with trade-based money laundering (e.g., insufficient customer due diligence; poor sharing of information among financial institutions, regulatory authorities, trade authorities and investigative authorities, domestically and internationally)
- Poor extension of AML/CFT requirements to all categories of nonfinancial DNFBPs
- Inadequate processes to freeze and confiscate terrorist assets and/or proceeds from foreign corruption
- Ineffective application of sanctioning powers for breaches of AML/CFT obligations
- Insufficient collection of statistics and provision of guidance and feedback to financial institutions
- Inadequate systems and controls to identify and report suspicious activity or to maintain adequate records within financial institutions
- Poor coordination among government agencies, especially among financial supervisors and regulators, investigators, law enforcement authorities and the public
- Inadequate skills, training and resources within regulatory and law enforcement authorities
- Shortcomings in international cooperation/mutual assistance due to the existence of various limiting factors (e.g., strong secrecy provisions, restrictions placed on counterparty's use of information, precondition of treaty, dual criminality stipulation)

1753. What were the key findings of the most recent mutual evaluation of the United States?

The most recent MER issued for the United States was performed in 2006 and was based on the Forty plus Nine Recommendations prior to the update in 2012. The results of the U.S. MER were as follows:

- Compliant: 15 out of 49 (31 percent)
- Largely Compliant: 28 out of 49 (57 percent)
- Partially Compliant: 2 out of 49 (4 percent)
- Noncompliant: 4 out of 49 (8 percent)

The United States made significant structural changes/statutory amendments with the passage of the USA PATRIOT Act and experienced an increase in prosecutions, seizures and enforcement actions since the mutual evaluation conducted in 1999. The United States also developed its efforts in improving coordination and information sharing between the financial community and regulatory authorities, both domestically and internationally, and assisting state and local governments with investigating and prosecuting money laundering and financial crimes and increasing penalties for money laundering.

The mutual evaluation completed on the United States in 2006 highlighted specific areas as needing improvement including, but not limited to, customer due diligence relating to beneficial owners, authorized signers, legal persons and trusts, ongoing due diligence and general requirements for DNFBPs (e.g., casinos, accountants, attorneys, dealers in precious metals and stones, real estate agents). Full details of the U.S. MER are available at the FATF website: http://www.fatf-gafi.org/.

ACRONYMS AND GLOSSARY

Acronyms	
ABA	American Bankers Association
ACH	Automated Clearing House
ACSSS	American Council of State Savings Supervisors
AEDPA	Antiterrorism and Effective Death Penalty Act of 1996
AFMLS	Asset Forfeiture and Money Laundering Section, Criminal Division
AI	Artificial Intelligence
AMEX/ASE	American Stock Exchange
AML	Anti-Money Laundering
AMLID	Anti-Money Laundering International Database
ANPR	Advanced Notice of Proposed Rulemaking
APG	Asia/Pacific Group on Money Laundering
AoA	U.S. Administration on Aging
APO	Army Post Office
APT	Asset Protection Trust
ASEAN	Association of Southeast Asian Nations
ATA	Anti-Terrorism Assistance Program
ATEST	Alliance to End Slavery and Trafficking
ATIP Program	Anti-Trafficking in Persons Program
ATM	Automated Teller Machine
ATP	Authorized Third Party
AU	African Union
BASCAP	Business Action to Stop Counterfeiting and Piracy
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
BIS	Bureau of Industry and Security
BJA	Bureau of Justice Assistance
BMPE	Black Market Peso Exchange
BOE	Bank of England
BPI	Bribe Payers Index

Acronyms	
BRCA RULE	Books and Records Customer Accounts Rule
BSA	Bank Secrecy Act
BSAAG	Bank Secrecy Act Advisory Group
BXA	Bureau of Export Administration
C&D	Cease and Desist
CBETF	Cross-Border Electronic Transmittal of Funds
CBP	Customs and Border Protection
CBT	Computer-Based Training
CCL	The Commerce Control List
CCS	Commercial Crime Services
CDD	Customer Due Diligence
CEA	Commodity Exchange Act
CFATF	Caribbean Financial Action Task Force
CFPB	Consumer Financial Protection Bureau
CFR	Code of Federal Regulations
CFTC	Commodity Futures Trading Commission
CIA	Central Intelligence Agency
CIBO	Customer Identification Beneficial Ownership
CIP	Customer Identification Program
CIS	Commonwealth of Independent States
CISADA	Comprehensive Iran Sanctions, Accountability and Divestment Act
CMIR	Report of International Transportation of Currency or Monetary Instruments
CMP	Civil Money Penalty
COE	Council of Europe
COMMIT	Coordinated Mekong Ministerial Initiative against Trafficking
CPA	Certified Public Accountant
CPI	Corruption Perceptions Index
CPO	Commodity Pool Operator
CPRC	Consumer Payments Research Center (Federal Reserve Bank of Boston)
CRF	Criminal Referral Form
CSBS	Conference of State Bank Supervisors
CSV	Comma-Separated Values
CTA	Commodities Trading Adviser
CTF	Counterterrorist Financing
CTR	Currency Transaction Report
CTR-C	Currency Transaction Report for Casinos
CTS	Counterterrorism Section, Criminal Division
DBA	Doing Business As

Acronyms	
DDA	Demand Deposit Account
DEA	Drug Enforcement Administration
DFAT	Australian Department of Foreign Affairs and Trade
DHS	Department of Homeland Security
DNFBP	Designated Nonfinancial Businesses and Professions
DOB	Date of Birth
DoD	U.S. Department of Defense
DOEP	Designation of Exempt Person
DOJ	U.S. Department of Justice
DOL	U.S. Department of Labor
DOS	U.S. Department of State
DOT	U.S. Department of the Treasury
DPA	Deferred Prosecution Agreement
DPL	Denied Persons List
EAG	Eurasian Group on Combating Money Laundering and Financing of Terrorism
EAR	Export Administration Regulation
EB	Bureau of Economic and Business Affairs
ECCAS	Economic Community of Central African States
ECOWAS	Economic Community of West African States
ED	U.S. Department of Education
EDD	Enhanced Due Diligence
EIA	U.S. Energy Information Administration
EIFFE	Elder Investment Fraud and Financial Exploitation
EIN	Employer Identification Number
EPN	Electronic Payments Network
ERISA	Employee Retirement Income Security Act
ESAAMLG	Eastern and South Africa Anti-Money Laundering Group
ESW	Egmont Secure Web
EU	European Union
FAQ	Frequently Asked Question
FAST	Fiduciary Abuse Specialist Team
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FBAR	Report of Foreign Bank and Financial Account
FBI	Federal Bureau of Investigation
FCM	Futures Commission Merchant
FCPA	Foreign Corrupt Practices Act
FCS	FINRA Contact System

Acronyms	
FDAP Income	Fixed, Determinable, Annual, Periodical Income
FDIC	Federal Deposit Insurance Corporation
FEST	Foreign Emergency Support Team
FFETF	Financial Fraud Enforcement Task Force
FHB	Federal Home Loan Bank
FFI	Foreign financial institution
FFIEC	Federal Financial Institutions Examination Council
FHFA	Federal Housing Finance Authority
FI	Financial Institution
FICO	Financing Corporation
FINCEN	Financial Crimes Enforcement Network
FINRA	Financial Industry Regulatory Authority
FIU	Financial Intelligence Unit
FLETC	Federal Law Enforcement Training Center
FPO	Fleet Post Office
FRB	Federal Reserve Board
FSRB	FATF-Style Regional Bodies
FTC	Federal Trade Commission
FTO	Foreign Terrorist Organization
FTZ	Free Trade Zones
FWP	Foreign Withholding Partnership
FWT	Foreign Withholding Trust
GAFISUD	Financial Action Task Force of South America Against Money Laundering
GAO	Government Accountability Office
GCB	Global Corruption Barometer
GDP	Gross Domestic Product
GHRAVITY E.O.	Blocking the Property and Suspending Entry into the United States of Certain Persons with Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology
GPR cards	General purpose reloadable cards
GTFP	The Global Trade Finance Program
GIABA	Groupe Inter-Gouvernemental D'action Contre Le Blanchiment En Afrique
GSE	Government sponsored enterprise
GTO	Geographic Targeting Order
GUI	Graphical User Interface
HEAT	Health Care Fraud Prevention and Enforcement Action Team
HHS	Department of Health and Human Services
HIDTA	High Intensity Drug Trafficking Area
HIFCA	High Risk Money Laundering and Related Financial Crimes Area

Acronyms	
HKMA	Hong Kong Monetary Authority
HSTC	Human Smuggling and Trafficking Center
HTRS	Human Trafficking Reporting System
IAIS	International Association of Insurance Supervisors
IB	Introducing Broker
IBC	International Business Corporation
ICC	International Chamber of Commerce
ICE	Immigration and Customs Enforcement
ICRG	International Cooperation Review Group
IFC	International Finance Corporation
IFSR	Iranian Financial Sanctions Regulations
IEEPA	International Emergency Economic Powers Act
IGRE ACT	Internet Gambling Regulation and Enforcement Act
ILO	International Labour Office
IMF	International Monetary Fund
INCSR	International Narcotics Control Strategy Report
INL	Bureau of International Narcotics and Law Enforcement Affairs
IOLTA	Interest on Lawyer's Trust Account
IOSCO	International Organization of Securities Commissions
IPT	Investor Protection Trust
IRGC	Islamic Revolutionary Guard Corps
IRS	Internal Revenue Service
IRS-CI	Internal Revenue Service Criminal Investigations Division
IRS-SB/SE	Internal Revenue Service – Small Business and Self Employment Division
IRS-TE/GE	Internal Revenue Service – Tax Exempt and Government Entities Division
ISA	Iran Sanctions Act of 1996
ISDCA	International Security and Development Cooperation Act of 1985
ISO	Independent Sales Organization
IT	Information Technology
ITAR	International Traffic In Arms Regulations
ITPP	Identity Theft Prevention Program
ITR	Iranian Transaction Regulations
ITRSHRA	Iran Threat Reduction and Syria Human Rights Act of 2012
IVTS	Informal Value Transfer System
JFIU	Joint Financial Intelligence Unit (Hong Kong)
KYC	Know Your Customer
LAS	League of Arab States
LC	Letter of Credit

Acronyms	
LEFIIS	Law Enforcement and Financial Institution Information Sharing System
LSSP	Lost and Stolen Securities Program
MAS	Monetary Authority of Singapore
MENA	Middle East and North Africa
MENAFATF	Middle East & North Africa Financial Action Task Force
MER	Mutual Evaluation Report
MFA	Managed Funds Association
ML	Money Laundering
MLCA	Money Laundering Control Act of 1986
MLSA	Money Laundering Suppression Act of 1994
MLTA	U.S. Money Laundering Threat Assessment
MMDA	Money Market Deposit Accounts
MONEYVAL	The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (Formerly Pc-R-Ev)
MOU	Memorandum of Understanding
MSB	Money Services Business
MSRB	Municipal Securities Rule Board
MTL	Multiple Transaction Logs
MTRA	Money Transmitter Regulators Association
NAIC	National Association of Insurance Commissioners
NAICS	North American Industry Classification System
NARCC	North American Regional Clearing Center
NASAA	North American Securities Administration Association
NAPSA	National Adult Protective Services Association
NASCUS	National Association of State Credit Union Supervisors
NASD	National Association of Securities Dealers
NASDAQ	National Association of Securities Dealers Automated Quotations
NBFI	Nonbank Financial Institution
NBPCA	Network Branded Prepaid Card Association
NCCT	Non-Cooperative Countries and Territories
NCEA	National Center on Elder Abuse
NCPEA	National Committee for the Prevention of Elder Abuse
NCTC	National Counterterrorism Center
NCUA	National Credit Union Association
NDAA	National Defense Authorization Act
NDIC	National Drug Intelligence Center
NDIP	Non Deposit Investment Product
NFA	National Futures Association
NFC	Near field communication

Acronyms	
NFFE	Nonfinancial foreign entity
NGA	National Geospatial – Intelligence Agency
NGO	Nongovernmental Organization
NHTRC	National Human Trafficking Resource Center
NIGC	National Indian Gaming Commission
NIS	Nominee Incorporation Services
NIS	National Integrity System Assessments
NMLS	National Money Laundering Strategy
NPR	Notice of Proposed Rulemaking
NPWMD	Nonproliferation of Weapons of Mass Destruction
NRA	Nonresident Aliens
NSF	Nonsufficient Fund
NSL	National Security Letter
NS-PLC	Non-Specially Designated National Palestinian Council
NYCH	New York Clearing House Association
NYSE	New York Stock Exchange
NZP	New Zealand Police
OAS	Organization of American States
OCC	Office of the Comptroller of the Currency
OCDETF	Organized Crime Drug Enforcement Task Force
ODFI	Originating Depository Financial Institutions
OEA	Office of Enforcement Analysis
OECD	Organisation for Economic Cooperation and Development
OFAC	Office of Foreign Assets Control
OFC	Offshore Financial Center
OGBS	Offshore Group of Banking Supervisors
OIA	Office of International Affairs
OIA	Office of Intelligence and Analysis, Criminal Division
ONDCP	Office of National Drug Control Policy
ORS	Office of Refugee Settlement
OSFI	Office of the Superintendent of Financial Institutions
OTP	One Time Passwords
OTS	Office of Thrift Supervision
OVC	Office for Victims of Crime
PASPA	Professional and Amateur Sports Protection Act of 1992
PEP	Politically Exposed Person
PIC	Private Investment Company
PIN	Personal Identification Numbers

Acronyms	
PITF	President's Interagency Task Force to Monitor and Combat Trafficking
POB	Place of Birth
POC	Point of Contact
POS	Point of Sale
PTA	Payable Through Account
PUPID	Payable Upon Proper Identification
RBA	Reserve Bank of Australia
RDC	Remote Deposit Capture
RDFI	Receiving Depository Financial Institutions
REIT	Real Estate Investment Trust
RMSB	Registration for Money Services Businesses
RMLO	Residential mortgage lender or originator
RO	Responsible Officer
S/CT	State's Office of the Coordinator for Counterterrorism
SAARC	South Asian Association for Regional Cooperation
SADC	Southern African Development Community
SAR	Suspicious Activity Report
SAR-C	Suspicious Activity Report by Casinos
SAR-DI	Suspicious Activity Report by Depository Institutions
SAR-IC	Suspicious Activity Report by Insurance Companies
SAR-MSB	Suspicious Activity Report by Money Services Business
SAR-SF	Suspicious Activity Report by the Securities and Futures Industries
SDGT	Specially Designated Global Terrorists
SDN	Specially Designated National
SDNT	Specially Designated Narcotics Traffickers
SDNTK	Specially Designated Narcotics Traffickers – Kingpins
SDT	Specially Designated Terrorists
SEC	U.S. Securities and Exchange Commission
SIA	Securities Industry Association
SLC	State Liaison Committee
SPE	Special Purpose Entity
SPV	Special Purpose Vehicle
SRO	Self-Regulatory Organization
SSN	Social Security Number
STR	Suspicious Transaction Report
SVC	Stored-Value Cards
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TAR	Terrorist Asset Report

Acronyms	
TBML	Trade Based Money Laundering
TBML/TF	Trade Based Money Laundering/Terrorist Financing
TCSP	Trust and Companies Service Providers
TEOAF	The Executive Office for Asset Forfeiture and Treasury Forfeiture Fund
TF	Terrorist Financing
TI	Transparency International
TFI	Office of Terrorism and Financial Intelligence
TFFC	Office of Terrorist Financing and Financial Crime
TIC	Trade Information Center
TIN	Taxpayer Identification Number
TIP Report	Trafficking in Persons Report
TOPOFF	Top Officials
TPPP	Third-Party Payment Processors
TPSP	Third-Party Service Provider
TSRA	Trade Sanctions Reform and Export Enhancement Act of 2000
TTU	Trade Transparency Units
TVPA	Trafficking Victims Protection Reauthorization Act
TWEA	Trading with the Enemy Act of 1917
UIGEA	Unlawful Internet Gambling Enforcement Act Of 2006
UN	United Nations
USAID	U.S. Agency for International Development
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
USC	United States Code
USDA	U.S. Department of Agriculture
USML	U.S. Munitions List
USSS	United States Secret Service
WB	World Bank
WCO	World Customs Organization
WGEI	Working Group on Evaluations and Implementation
WMD	Weapons of Mass Destruction
WTO	World Trade Organization

Glossary of Select Key Terms	
Account	Account is defined differently for various types of institutions (e.g., bank, broker-dealer and casino). For example, for depository institutions, an "account" is a formal relationship in or through which financial transactions or services are provided. Examples of products and services where a formal relationship would normally exist include deposit accounts, extensions of credit, a safe deposit box or other safekeeping services, and cash management, custodian or trust services. For other definitions of "account," please see the Broker-Dealers and Casinos or Card Clubs sections.
Alert	An "alert" is an indicator of unusual or potentially suspicious activity based on such factors as expected activity thresholds, account history, customer types, product types and geography in an automated monitoring system. An "alert" may be generated from a transaction monitoring system or via internal referrals, subpoenas and 314(a)/(b) matches. Regardless of its source, an alert is not necessarily an automatic indicator of suspicious activity. For further guidance, please refer to the sections: Transaction Monitoring, Investigations and Red Flags and Investigating Potential Matches.
Beneficial owner	FinCEN's advanced notice of proposed rulemaking (ANPR) on "Customer Due Diligence Requirements for Financial Institutions" considers the following as a limited definition of beneficial ownership: Either: • Each of the individual(s) who, directly or indirectly, through any contract, arrangement, understanding, relationship, intermediary, tiered entity, or otherwise, owns more than 25 percent of the equity interests in the entity; or • If there is no individual who satisfies the above, then the Individual who, directly or indirectly, through any contract, arrangement, understanding, relationship, intermediary, tiered entity, or otherwise, has at least as great an equity interest in the entity as any other individual; and • The individual with greater responsibility than any other individual for managing or directing the regular affairs of the entity. For further guidance, please refer to the Beneficial Owners section.
Business day	Business day is defined differently for various types of institutions (e.g., depository institutions, casinos): • For depository institutions, a business day is the reporting period on which transactions are routinely posted to customers' accounts each day. • For casinos, the term "business day" is the gaming day by which they keep their books and records for business, accounting and tax purposes. It is also important to note that some AML requirements use calendar days as opposed to business days.
Business line risk assessment (BLRA)	A business line risk assessment is an evaluation of each business line's level of vulnerability to money laundering and terrorist financing risk. This assessment is accomplished by evaluating, for a specific business line, among other factors, the inherent risk of products/services, the customer base (e.g., type, location) and geography (e.g., customers, transactions, operations) at a macro level and the controls (e.g., policy and procedures, customer acceptance and maintenance standards, transaction monitoring, management oversight, training, personnel) mitigating those risks at the business line level. For further guidance, please refer to the Business Line Risk Assessment section.
Casa de cambio	A casa de cambio, the Spanish term for currency exchange, money exchange, bureau de change, is a business whose customers exchange one currency for another. For further guidance, please refer to the Money Services Businesses section.

Glossary of Select Key Terms	
Commodity Trading Adviser (CTA)	A CTA is a person who directs (i.e., is given decision-making authority over) account activities, client commodity futures and options accounts, and is registered or required to be registered as a CTA with the CFTC under the CEA. Generally, the CEA has defined a CTA as any person who is in the business of directly or indirectly advising others as to the value or advisability of trading futures contracts or commodity options for compensation or profit. For further guidance, please refer to the Commodity Trading Advisers and Commodity Pool Operators section.
Concentration Account	Within the industry, a concentration account is an account that a financial institution uses to aggregate funds from different customers' accounts. Concentration accounts are also known as collection, intraday, omnibus, settlement, special-use or sweep accounts. For further guidance, please refer to the Concentration Accounts section.
Correspondent account	A correspondent account is defined broadly to include any account or formal relationship established by a financial institution to receive deposits from, make payments to or other disbursements on behalf of a foreign financial institution, or to handle other financial transactions related to the foreign financial institution. For further guidance, please refer to the sections: Correspondent Banking and Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts.
Cover payment	Cover payments are used in correspondent banking to facilitate international transactions. A cover payment involves two separate transactions: one credit transfer message that travels a direct route from the originating bank to the ultimate beneficiary's bank, and a second credit transfer that travels through a chain of correspondent banks to settle or "cover" the first credit transfer message. For further guidance, please refer to the Due Diligence for Correspondent Accounts section.
Cross channel alert	A cross channel alert involves the sharing of information between groups that has utility for all involved groups (e.g., AML and anti-fraud units). For further guidance, please refer to the Convergence of Anti-Money Laundering and Anti-Fraud Programs section.

Currency/cash	Currency and cash are defined differently for Currency Transaction Reports (CTR) and Form 8300 reporting requirements.
	• For CTRs, currency means the coin and paper money of the United States or any other country, which is circulated and customarily used and accepted as money.
	• "Cash" is defined, for Form 8300 purposes, as:
	  o U.S. and foreign coin and currency received in any transaction
	  o A cashier's check, money order, bank draft or traveler's check having a face amount of $10,000 or less received in a designated reporting transaction, or received in any transaction in which the recipient knows that the instrument is being used in an attempt to avoid reporting requirements
	For further guidance, please refer to the sections: Currency Transactions, Currency Transaction Reports and Form 8300.

Customer	"Customer" is defined differently for various types of institutions (e.g., depository institution, broker-dealer and casino). For example, for depository institutions, a customer is any person who opens a new account or enters into another formal relationship after October 1, 2003. "Person" in this context includes individuals, corporations, partnerships, trusts or estates, joint stock companies, joint ventures or other incorporated organizations or groups. For other definitions of customer, please see the Broker-Dealers and Casinos or Card Clubs sections.
Customer due diligence (CDD)	CDD is information obtained for all customers. Information obtained for CDD should enable a financial institution to verify the identity of a customer and assess the risks associated with that customer. For further guidance, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence section.

Glossary of Select Key Terms	
Customer risk assessment	A customer risk assessment is a process that identifies the level of money laundering and terrorist financing risk inherent in a financial institution's customer base, either on an individual customer or customer segment basis. For further guidance, please refer to the Customer Risk Assessment section.
Date of detection	The date of detection that triggers the time period for filing a SAR begins when the financial institution, during its review of transaction or account activity or because of other factors, knows, or has reason to suspect, that the activity or transactions under review meet one or more of the definitions of suspicious activity. For further guidance on the date of detection, please see the SAR Filing Time Frame and Date of Initial Detection section.
Depository institution	Depository institutions include banks, savings associations, thrift institutions and credit unions.
Deferred prosecution agreement (DPA)	A DPA is an agreement entered into between a prosecutor and a defendant in a criminal case whereby in exchange for successful completion of agreed-upon commitments, the criminal charges against the defendant will be dismissed in their entirety by the prosecutor.
Elder abuse	Elder abuse generally refers to intentional or negligent actions taken by a caregiver or other person presumed to be in a position of trust who causes harm or a serious risk of harm to a vulnerable, older adult. It can be a single act or a series of actions that causes harm or distress to an older person and may include physical, psychological or financial abuse, as well as neglect.
Elder financial abuse	Elder financial abuse involves the exploitation of a relationship with an elder or dependent adult in order to steal, embezzle or improperly use the person's money, property or other resources. The exploitation may occur by deception, coercion, misrepresentation, undue influence or theft, and can include deprivation of money and/or property. For further guidance, please refer to the Elder Financial Abuse section.
Enhanced due diligence (EDD)	EDD refers to additional information that would be collected for those customers deemed to be of higher risk. For further guidance, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence section.
Enterprise-wide Risk Assessment	An enterprise-wise risk assessment is an exercise intended to identify systemic money laundering risk that may not be apparent in a risk assessment focused on a business line or other assessment unit. In other words, it is the big picture view of an organization's money laundering risks that aggregates the results of other risk assessment exercises. For further guidance, please see the Enterprise-Wide Risk Assessment section.

Glossary of Select Key Terms	
Financial institution	The term "financial institution" is defined differently for various regulations (e.g., USA PATRIOT Act, identity theft). The definition in the USA PATRIOT Act includes: • Insured banks • Commercial banks • Trust companies • Private banks • Agency or branch of a foreign bank in the United States • Credit unions • Thrift and saving institutions • Broker-dealers registered or required to register with the SEC • Securities/commodities broker-dealers • Futures commission merchants (FCM), introducing brokers (IB), commodity pool operators (CPO) and commodity trading advisers (CTA) registered or required to register under the Commodity Exchange Act (CEA) • State-licensed or Indian casinos with annual gaming revenue of more than $1 million • Investment bankers • Investment companies • Currency exchanges • Issuer or seller of traveler's checks, money orders or similar instruments • Licensed sender of money or any other person who engages as a business in the transmission of funds, formally or informally • Operators of credit card systems • Insurance companies • Dealers in precious metals, stones or jewels • Pawnbrokers • Loan or finance companies • Travel agencies • Telegraph companies • Businesses engaged in vehicle sales, including automobile, airplane and boat sales • Persons involved in real estate closings and settlements • The U.S. Postal Service • Agencies of the federal government or any state or local government, carrying out a duty or power of a business described in the definition of a "financial institution" • Any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any of the above entities are authorized to engage • Any other business designated by the Secretary of the Treasury whose cash transactions have a high degree of usefulness in criminal, tax or regulatory matters For further guidance, please refer to the sections: Overview of the USA PATRIOT Act and Overview of the BSA.

Financial interest	The term "financial interest" in a bank, securities or other financial account in a foreign country means an interest as described below:
	• A U.S. person has a financial interest in each account for which such person is the owner of record or has legal title, regardless of whether the account is maintained for the U.S. person's own benefit or for the benefit of others, including non-U.S. persons.
	• A U.S. person has a financial interest in each bank, securities or other financial account (including credit and debit cards) in a foreign country for which the owner of record or holder of legal title is:
	  o A person acting as an agent nominee, attorney, or in some other capacity on behalf of the U.S. person with respect to the account;
	  o A corporation in which the U.S. person owns directly or indirectly more than 50 percent of the total value of shares of stock or more than 50

Glossary of Select Key Terms	
	percent of the voting power of all shares of stock; o A partnership in which the U.S. person owns an interest in more than 50 percent of the profits (distributive share of income) or an interest in more than 50 percent of the partnership capital; o A trust of which the U.S. person is the trust grantor and has an ownership interest in the trust for U.S. federal tax purposes; o A trust in which the U.S. person either has a present beneficial interest in more than 50 percent of the assets or from which such person receives more than 50 percent of the current income; or o Any other entity in which the U.S. person owns directly or indirectly more than 50 percent of the voting power, total value of equity interests or assets, or interest in profits. For further guidance, please refer to the Report of Foreign Bank and Financial Accounts section.
Foreign and domestic	The terms "foreign" and "domestic" may be used to describe the home country of an organization or the jurisdiction in which the business is authorized to conduct business depending on the specific AML requirement. For example, in some instances, "domestic institution" refers to all financial institutions authorized to do business in the United States, including U.S. offices of foreign financial institutions.
Free trade zones	Free trade zones are designated areas within countries that offer a free trade environment with minimal regulation. According to FATF, free trade zones are now located in over 130 countries. Financial institutions may consider conducting enhanced due diligence on parties and transactions associated with free trade zones. For additional guidance, please refer to the Trade Finance Activities section.
Funds transfer	The term "funds transfer" means a series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order. Funds transfers governed by the Electronic Funds Transfer Act of 1978 as well as any other funds transfers made through an ACH, ATM or a point-of-sale (POS) system are excluded from this definition.
Futures Commission Merchant (FCM)	An FCM is a person or entity registered, or required to register, as an FCM with the Commodity Futures Trading Commission (CFTC) under the Commodity Exchange Act (CEA), except a person who registers pursuant to 4(f)(a)(2) of the CEA. FCMs conduct transactions in the futures market in a manner similar to that of brokers in the securities market. For further guidance, please refer to the Futures Commission Merchants and Introducing Brokers section.
Government sponsored enterprise (GSE)	A government sponsored enterprise (GSE) is a financial services organization created and regulated by the U.S. government (specifically, by Congress) and functioning to increase the availability and reduce the cost of credit to targeted sectors such as education, agriculture and home finance. GSEs that target home finance are called Housing GSEs. For further guidance, please refer to the Housing Government Sponsored Enterprise section.
Hawala	Hawala is one type of informal value transfer system (IVTS). Hawala is an Arabic word that means "a bill of exchange or promissory note." For further guidance, please refer to the sections: Informal Value Transfer Systems and Money Services Businesses.
Household	A household is generally defined as a grouping consisting of two or more distinct customers that share a common factor such as an address, phone number or business owner.

Glossary of Select Key Terms	
Human trafficking	Human trafficking is sometimes defined as modern slavery. It is the illegal trade of human beings for sexual exploitation or forced labor or services. Further, the physical transportation of victims from one location to another is not required for the crime to fall within the definition of human trafficking. For further guidance, please refer to the Human Trafficking section.
Human smuggling	Human smuggling involves the covert transportation of individuals across international borders with the consent of the transported individuals. Human smuggling occurs during the "transportation" stage of human trafficking and typically ends after the transfer is complete.
International Automated Clearing House Transaction (IAT)	An IAT is a new standard entry class (SEC) code used to identify cross-border ACH transactions. For further guidance, please refer to the section: Automated Clearing House Transactions and IATs.
Informal value transfer system (IVTS)	IVTS refers to any system, mechanism or network of people operating outside of the traditional financial system that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, regardless of whether the funds are in the same form. For further guidance on these systems, please refer to the Informal Value Transfer Systems section.
Inherent risk	Inherent risk is the risk to an entity in the absence of any actions management might take (e.g., controls) to alter either the risk's likelihood or impact. For further guidance, please refer to the Risk Assessments section.
Investigation	An investigation is the review of transactions/conduct in order to classify the alert as a "false positive" or a "true positive," which will require further analysis and could result in the filing of a SAR. For further guidance, please refer to the Transaction Monitoring, Investigations and Red Flags section.
Junket representative	A "junket representative" is the organizer of a group of well-known players; a "junket" who travel together for the purpose of gambling. For further guidance, please refer to the Casinos or Card Clubs section.
Knowingly	"Knowingly" means actual knowledge or constructive knowledge (i.e., the person should have known) within the context of select Iranian and Syrian sanctions. For further guidance, please refer to the Iranian Sanctions Overview section.
KYC/CIP/CDD/EDD	KYC, or "know your customer," generally refers to all of the steps taken by a financial institution to establish the identity of a customer and be satisfied that the source of the customer funds is legitimate. This includes: • Customer identification program (CIP) • Customer due diligence (CDD) • Enhanced due diligence (EDD) For further guidance, please refer to the sections: Know Your Customer, Customer Due Diligence and Enhanced Due Diligence and Section 326 – Verification of Identification.
Microstructuring	Microstructuring is a form of structuring that involves breaking transactions into small amounts, typically ranging from $500 to $1,500, and more frequent depositing of currency into a higher number of bank accounts than is done in classic structuring schemes. For further guidance on microstructuring, please see the CTR Evasion section.
Monetary instrument	Monetary instruments include bank checks or drafts, foreign drafts, cashier's checks, money orders or traveler's checks. For further guidance, please refer to the Monetary Instruments section. Monetary Instruments

Glossary of Select Key Terms	
Money laundering	Money laundering is the attempt to disguise the proceeds of illegal activity, so that it appears to come from legitimate sources or activities. For further guidance, please refer to the Anti-Money Laundering Fundamentals section.
Money services business (MSB)	FinCEN defines an MSB as "a person wherever located doing business, whether or not on a regular basis or as an organized or licensed concern, wholly or in substantial part within the United States, in one or more capacities" listed below: • Issuer or seller of money orders or traveler's checks • Check casher • Dealer in foreign exchange • Provides or sells prepaid access • Money transmission (domestic or international) For further guidance, please refer to the Money Services Businesses section.
Mutual Fund	A mutual fund is an open-ended investment company that is registered or required to register with the Securities and Exchange Commission (SEC) under Section 5 of the Investment Company Act. For further guidance, please refer to the Mutual Funds section.
National Security Letter (NSL)	National Security Letters (NSLs) are written investigative demands that may be issued by the local Federal Bureau of Investigation (FBI) office and other federal governmental authorities in counterintelligence and counterterrorism investigations to obtain the following: • Telephone and electronic communications records from telephone companies and Internet service providers • Information from credit bureaus • Financial records from financial institutions For further guidance, please refer to Section 505 - Miscellaneous National Security Authorities.
Nonbank financial institution (NBFI)	For purposes of this guide, NBFIs include all entities excluding depository institutions that are considered financial institutions under the USA PATRIOT Act. For further guidance, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.
OFAC risk assessment	An OFAC risk assessment identifies an organization's level of vulnerability to noncompliance with economic sanctions administered by OFAC. This is accomplished by evaluating, among other factors, the inherent risk of products and services, customer types and the geographic origin and destination of transactions, and the controls mitigating those risks. For further guidance, please refer to the OFAC Risk Assessment section.
Offshore financial center (OFC)	OFCs are jurisdictions that have a relatively large number of financial institutions engaged primarily in business with nonresidents.
Payable through account (PTA)	A PTA, also known as a "pass through" or "pass-by" account, is an account maintained for a respondent that permits the respondent's customers to engage, either directly or through a subaccount, in banking activities (e.g., check writing, making deposits), usually in the United States. For further guidance, please refer to the Payable Through Accounts section.
Pharming	Pharming is a method of fraudulently obtaining identity or other sensitive information (e.g., passwords, security answers) by secretly redirecting users from legitimate websites to websites created by scammers. For further guidance, please refer to the CIP vs. Identity Theft Prevention Program section.

Glossary of Select Key Terms	
Phishing	Phishing is a method of fraudulently obtaining identity or other sensitive information (e.g., passwords, security answers) by masquerading as a legitimate entity in an electronic communication (e.g., e-mail, spyware). For example, an individual may receive an e-mail that appears to be from his or her bank that requests identity and/or password information under the guise of "verification" purposes. For further guidance, please refer to the CIP vs. Identity Theft Prevention Program section.
Politically exposed person (PEP)	PEP has been defined by multiple sources (e.g., USA PATRIOT Act, FATF and the Wolfsberg Group). Under the USA PATRIOT Act, a "politically exposed person" (PEP) is a senior foreign political figure, such as a current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned commercial enterprise; a corporation, business or other entity formed by or for the benefit of any such individual; an immediate family member of such an individual; or any individual publicly known (or actually known by the financial institution) to be a close personal or professional associate of such an individual. For further guidance on PEPs, please see sections: Politically Exposed Persons and Enhanced Due Diligence for Private Banking Accounts.
Pouch activity	Pouch activity, also known as "pouch services" or "cash letters," is the use of a courier to transport currency, monetary instruments, loan payments and other financial documents to a financial institution. Pouches can be sent by another financial institution or by an individual and are commonly offered in conjunction with correspondent banking services. For further guidance, please refer to the Pouch Activity section.
Prepaid access	Prepaid access is defined by FinCEN's final rule "Definitions and Other Regulations Relating to Prepaid Access" as the access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number or personal identification number. Prepaid access applies to a very broad range of prepaid services, including but not limited to open-loop prepaid access, closed-loop prepaid access, prepaid access given for the return of merchandise, many prefunded employee programs such as a Health Savings Account, etc. For further guidance, please refer to the sections: Prepaid Access, Stored-Value, and E-Cash and Providers and Sellers of Prepaid Access.
Prepaid access provider	A provider of prepaid access is defined as the participant within a prepaid program that agrees to serve as the principal conduit for access to information from its fellow program participants. The participants in each prepaid access program (which may be one or more) must determine a single participant within the prepaid program to serve as the provider of prepaid access ("provider"). The provider also will be the primary contact and source of information for FinCEN, law enforcement and regulators for the particular prepaid program. For further guidance, please refer to the sections: Prepaid Access, Stored-Value, and E-Cash and Providers and Sellers of Prepaid Access.
Prepaid access seller	A seller of prepaid access is defined as any person who receives funds or the value of funds in exchange for an initial or subsequent loading of prepaid access if: • That person either sells prepaid access offered under a prepaid program that can be used before the customer's identity can be captured (including name, address, date of birth and identification number) and verified; or • That person sells prepaid access (including closed-loop prepaid access) to funds that exceed $10,000 to any person or entity (there is a limited exception for bulk sales) on any one day and has not implemented policies and procedures to reasonably prevent such sales. For further guidance, please refer to the sections: Prepaid Access, Stored-Value, and E-Cash and Providers and Sellers of Prepaid Access.

Glossary of Select Key Terms	
Private banking account	A private banking account is defined in the USA PATRIOT Act as an account (or combination of accounts) maintained at a financial institution that meets the following criteria: • Requires a minimum aggregate deposit of funds or other assets of not less than $1 million • Is established on behalf of or for the benefit of one or more non-U.S. persons who are direct or beneficial owners of the account • Is assigned to, or is administered or managed by, in whole or in part, an officer, employee or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account For further guidance, please refer to the sections: Private Banking, Due Diligence for Private Banking Accounts and Enhanced Due Diligence for Private Banking Accounts.
Private investment company (PIC)	A PIC generally is a company formed by one or more individuals to own and manage his or her assets. Often established in offshore financial centers (OFCS) for tax reasons, PICs provide confidentiality and anonymity to the beneficial owners of the funds since the management of the PIC often rests with a third party not readily associated with the beneficial owner. For further guidance, please refer to the Business Entities: Shell Companies and Private Investment Companies section.
Professional service providers	A professional service provider, also referred to as a "gatekeeper," acts as an intermediary between its client and a third-party financial institution and may conduct or arrange for financial dealings and services on its client's behalf (e.g., management of client finances, settlement of real estate transactions, asset transfers, investment services, trust arrangements). Examples of professional service providers include lawyers, notaries and accountants. For further guidance, please refer to the Professional Service Providers section.
Reintegro	Reintegro refers to a trade-based, reverse-BMPE laundering scheme that hinges on trade document manipulation and often includes the corruption of a bank employee or customs official. Unlike traditional BMPE activities that operate with goods (not funds) crossing the border, in reintegro transactions, peso exchange brokers repatriate drug proceeds by disguising them as payments for nonexistent or overvalued goods using purchased export papers, similar to letters of credit, to make the payments appear legitimate. This is known as "reintegro" or "reintegrate papers." For further guidance, please refer to Reintegro section.
Remote deposit capture (RDC)	RDC is the process by which a customer deposits a check or other monetary instrument into an account at a financial institution from a remote location via transmission of digital information or a scanned image to the financial institution rather than delivery of the physical check. RDC is used for domestic transactions and is more frequently being used to replace international pouch activities. For further guidance, please refer to the Remote Deposit Capture section.
Residual risk	Residual risk is the risk remaining after all controls have been applied to reduce the likelihood or impact of the risk. For further guidance, please refer to the Risk Assessments section.
Risk assessment	A risk assessment identifies (a) the inherent risks in a business and/or processes; (b) current controls and any noted gaps in the compliance program; and (c) the residual risk of a business and/or processes. For further guidance, please refer to the Risk Assessments section.
Safe harbor	Safe harbor is protection from civil liability to any financial institution, director, officer or employee that makes a suspicious transaction report under any federal, state or local law. A "bank, and any director, officer, employee or agent of any bank, that makes a voluntary disclosure of any possible violation of law or regulation to a government agency with jurisdiction, including a disclosure made jointly with another institution involved in the same transaction, shall be protected" under the Safe Harbor provision. For further guidance on safe harbor, please see the Safe Harbor section.

Glossary of Select Key Terms	
Shell company	A shell company generally refers to an entity without a physical presence in any country. For further guidance, please refer to the Business Entities: Shell Companies and Private Investment Companies section.
Signature authority	Signature authority is defined as "the authority of an individual (alone or in conjunction with another individual) to control the disposition of assets held in a foreign financial account by direct communication (whether in writing or otherwise) to the bank or other financial institution that maintains the financial account." For further guidance, please refer to the Report of Foreign Bank and Financial Accounts section.
Skimming	Skimming is a method of fraudulently obtaining and storing credit/debit card information through the use of computers or specialized card readers in order to re-encode the account information onto the magnetic strips of blank credit/debit cards, which then can be used to make purchases. For further guidance, please refer to the CIP vs. Identity Theft Prevention Program section.
Smurfing	Smurfing is the attempt to evade CTR filing requirements and/or detection by conducting numerous transactions at different locations of either the same institution or different institutions. For further guidance on smurfing, please see the CTR Evasion section.
Special Purpose Vehicle	A special purpose vehicle (SPV), also known as a special purpose entity (SPE), bankruptcy-remote entity, and orphan company, is a corporation, trust, partnership, or limited liability company that is created for a limited purpose, generally to isolate financial risk. An SPE may be owned by one or more other entities. For further guidance, please refer to the Business Entities: Shell Companies and Private Investment Companies section.
Specially Designated Nationals and Blocked Persons (SDN) List	The SDN List, administered by OFAC, identifies individuals, groups and entities, such as terrorists and narcotics traffickers, designated under programs that are not country-specific whose assets are blocked. U.S. persons generally are prohibited from dealing with them. For further guidance, please refer to the Specially Designated Nationals and Blocked Persons List.
Stored-Value Cards	Stored-value cards, now known as prepaid cards, are funds or monetary value represented in digital electronic format and stored or capable of storage on electronic media in such a way as to be retrievable and transferable electronically. For further guidance, please refer to the sections: Prepaid Access, Stored-Value and E-Cash and Providers and Sellers of Prepaid Access.
Structuring	Structuring is the attempt to evade CTR filing requirements by breaking transactions into smaller amounts, typically just below the reportable threshold (e.g., $10,000). For further guidance on structuring, please see the CTR Evasion section.
Terrorism	Terrorism is often defined as an activity that involves a violent act or an act dangerous to human life, property or infrastructure that appears to be intended to: intimidate or coerce a civilian population; influence the policy of a government by intimidation or coercion; affect the conduct of a government by mass destruction, assassination, kidnapping or hostage taking. For further guidance, please refer to the Anti-Money Laundering Fundamentals section.
Terrorist financing	Terrorist financing is a financial crime that uses funds to support the agenda, activities or cause of a terrorist organization. The funds raised may be from legitimate sources, such as charitable organizations or donations from supporters, as well as criminal sources such as drug trade, weapons smuggling, fraud, kidnapping and extortion for illegal activities. For further guidance, please refer to the Anti-Money Laundering Fundamentals section.

Glossary of Select Key Terms	
Trade-Based Money Laundering	The term trade-based money laundering (TBML) refers to the process of disguising the proceeds of illegal activity and moving value through the use of trade transactions so that they appear to come from legitimate sources or activities. Examples of TBML include the Black Market Peso Exchange (BMPE) and Reintegro schemes. For further guidance, please refer to the sections: Trade Finance Activities and Informal Value Transfer Systems.
Trade Finance	The term "trade finance" generally refers to the financial component of trade transactions executed between exporters from one country and importers from another country, which typically involves short-term financing to facilitate the import and export of goods. For further guidance, please refer to the Trade Finance Activities section.

KEY U.S. AML LAWS AND REGULATIONS AND USEFUL WEBSITES

In addition to our direct experience working with companies on AML projects, both in the United States and other markets, we have compiled the following key resources used to develop this booklet. Specific guidances are further detailed within various sections of this guide.

Key U.S. AML and Sanction Laws and Regulations	
31 USC 5311-5314, 5316-5326, 5328-5332; 12 USC 1829b; 12 USC 1951-1959	Bank Secrecy Act (BSA)
31 USC 5311	Declaration of purpose
31 USC 5312	Definitions and application
31 USC 5313	Reports on domestic coins and currency transactions (CTR)
31 USC 5314	Records and reports on foreign financial agency transactions
31 USC 5316	Reports on exporting and importing monetary instruments (CMIR)
31 USC 5317	Search and forfeiture of monetary instruments
31 USC 5318	Compliance, exemptions and summons authority
31 USC 5319	Availability of reports
31 USC 5320	Injunctions
31 USC 5321	Civil penalties
31 USC 5322	Criminal penalties
31 USC 5323	Rewards for informants
31 USC 5324	Structuring transactions to evade reporting requirement prohibited
31 USC 5325	Identification required to purchase certain monetary instruments
31 USC 5326	Records of certain domestic coin and currency transactions
31 USC 5328	Whistleblower protections (Safe Harbor)
31 USC 5329	Staff commentaries
31 USC 5330	Registration of money transmitting businesses
31 USC 5331	Reports relating to coins and currency received in nonfinancial trade or business (Form 8300)
31 USC 5332	Bulk cash smuggling into or out of the United States
12 USC 1829b	Retention of records by insured depository institutions
12 USC 1951	Congressional findings and declaration of purpose
12 USC 1952	Reports on ownership and control

Key U.S. AML and Sanction Laws and Regulations	
12 USC 1953	Recordkeeping and procedures
12 USC 1954	Injunctions
12 USC 1955	Civil penalties
12 USC 1956	Criminal penalty
12 USC 1957	Additional criminal penalty in certain cases
12 USC 1958	Compliance
12 USC 1959	Administrative procedure
H.R. 3162: Title III	Title III: International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act): • Subtitle A: International Counter Money Laundering and Related Measures • Subtitle B: Bank Secrecy Act Amendments and Related Improvements • Subtitle C: Currency Crimes and Protection
Title III: Subtitle A: Section 302	Findings and purposes
Title III: Subtitle A: Section 303	4-year congressional review; expedited consideration
Title III: Subtitle A: Section 311	Special measures for jurisdictions, financial institutions, or international transactions of primary money laundering concern
Title III: Subtitle A: Section 312	Special due diligence for correspondent accounts and private banking accounts
Title III: Subtitle A: Section 313	Prohibition on United States correspondent accounts with foreign shell banks
Title III: Subtitle A: Section 314	Cooperative efforts to deter money laundering
Title III: Subtitle A: Section 315	Inclusion of foreign corruption offenses as money laundering crimes
Title III: Subtitle A: Section 316	Anti-terrorist forfeiture protection
Title III: Subtitle A: Section 317	Long-arm jurisdiction over foreign money launderers
Title III: Subtitle A: Section 318	Laundering money through a foreign bank
Title III: Subtitle A: Section 319	Forfeiture of funds in United States interbank accounts
Title III: Subtitle A: Section 320	Proceeds of foreign crimes
Title III: Subtitle A: Section 321	Financial institutions specified in Subchapter II of Chapter 53 of Title 31, United States Code
Title III: Subtitle A: Section 322	Corporation represented by fugitive
Title III: Subtitle A: Section 323	Enforcement of foreign judgments
Title III: Subtitle A: Section 324	Report and recommendation
Title III: Subtitle A: Section 325	Concentration accounts at financial institutions
Title III: Subtitle A: Section 326	Verification of identification (CIP)
Title III: Subtitle A: Section 327	Consideration of anti-money laundering record
Title III: Subtitle A: Section 328	International cooperation on identification of originators of wire transfers
Title III: Subtitle A: Section 329	Criminal penalties
Title III: Subtitle A: Section 330	International cooperation in investigations of money laundering, financial crimes and the finances of terrorist groups
Title III: Subtitle B: Section 351	Amendments relating to reporting of suspicious activities
Title III: Subtitle B: Section 352	Anti-money laundering programs (AML programs)

Key U.S. AML and Sanction Laws and Regulations	
Title III: Subtitle B: Section 353	Penalties for violations of geographic targeting orders and certain recordkeeping requirements and lengthening effective period of geographic targeting orders
Title III: Subtitle B: Section 354	Anti-money laundering strategy
Title III: Subtitle B: Section 355	Authorization to include suspicions of illegal activity in written employment references
Title III: Subtitle B: Section 356	Reporting of suspicious activities by securities brokers and dealers; investment company study
Title III: Subtitle B: Section 357	Special report on administration of bank secrecy provisions
Title III: Subtitle B: Section 358	Bank secrecy provisions and activities of United States intelligence agencies to fight international terrorism
Title III: Subtitle B: Section 359	Reporting of suspicious activities by underground banking systems
Title III: Subtitle B: Section 360	Use of authority of United States executive directors
Title III: Subtitle B: Section 361	Financial Crimes Enforcement Network
Title III: Subtitle B: Section 362	Establishment of highly secure network
Title III: Subtitle B: Section 363	Increase in civil and criminal penalties for money laundering
Title III: Subtitle B: Section 364	Uniform protection authority for Federal Reserve facilities
Title III: Subtitle B: Section 365	Reports relating to coins and currency received in nonfinancial trade or business
Title III: Subtitle B: Section 366	Efficient use of currency transaction report system
Title III: Subtitle C: Section 371	Bulk cash smuggling into or out of the United States
Title III: Subtitle C: Section 372	Forfeiture in currency reporting cases
Title III: Subtitle C: Section 373	Illegal money transmitting businesses
Title III: Subtitle C: Section 374	Counterfeiting domestic currency and obligations
Title III: Subtitle C: Section 375	Counterfeiting foreign currency and obligations
Title III: Subtitle C: Section 376	Laundering the proceeds of terrorism
Title III: Subtitle C: Section 377	Extraterritorial jurisdiction
Title V: Section 505	Miscellaneous National Security Authorities
18 USC 1956, 1957	Money Laundering Control Act of 1986 (MLCA)
P.L. 100-690	Anti-Drug Abuse Act of 1988
12 USC 1811	Annunzio-Wylie Anti-Money Laundering Act of 1992
31 USC 5301	Money Laundering Suppression Act of 1994 (MLSA)
H.R. 1756	Money Laundering and Financial Crimes Strategy Act of 1998
S. 2845	Intelligence Reform and Terrorism Prevention Act of 2004
31 CFR Chapter X	Financial recordkeeping and reporting of currency and foreign transactions
31 CFR Chapter X 1010.205(a)-(d)	Exempted anti-money laundering programs for certain financial institutions
31 CFR Chapter X 1010.314(a)-(c)	Structured transactions
31 CFR Chapter X1010.306(a)(1)-(e)	Filing of reports (CTR, CMIR, FBAR)
31 CFR Chapter X 1010.306(a)(2)&(3); 1010.306(d)-(e)	CTR exemption recordkeeping requirements
31 CFR Chapter X1010.311(a)-!c)	Filing obligations of financial institutions and casinos
31 CFR Chapter X1010.312	Identification requirements
31 CFR Chapter X 1010.313(a)-(b)	Aggregation multiple branches; multiple transactions - general

Key U.S. AML and Sanction Laws and Regulations	
31 CFR Chapter X1010.330	Reports relating to currency in excess of $10,000 received in a trade or business (Form 8300)
31 CFR Chapter X1010.340	Reports of transportation of currency or monetary instruments (CMIR)
31 CFR Chapter X 1010.350	Reports of foreign bank and financial accounts (FBAR)
31 CFR Chapter X 1010.360	Reports of transactions with foreign financial agencies
31 CFR Chapter X 1010.370	Reports of certain domestic coin and currency transactions
31 CFR Chapter X 1010.410	Records to be made and retained by financial institutions (funds transfer recordkeeping and transmittal requirements)
31 CFR Chapter X 1010.415	Purchases of bank checks and drafts, cashier's checks, money orders and traveler's checks
31 CFR Chapter X 1010.430 (a)(d)	Nature of records and retention period
31 CFR Chapter X 1010.440	Person outside the United States
31 CFR Chapter X 1010.520	Information sharing between federal law enforcement agencies and financial institutions (314(a))
31 CFR Chapter X 1010.540	Voluntary information sharing among financial institutions (314(b))
31 CFR Chapter X 1010.610	Due diligence programs for correspondent accounts for foreign financial institutions
31 CFR Chapter X 1010.620(a)-(e)	Due diligence programs for private banking accounts
31 CFR Chapter X 1010.630(a)-(f)	Prohibition on correspondent accounts for foreign shell banks; records concerning owners of foreign banks and agents for service of legal process
31 CFR Chapter X 1010.651	Special measures against Burma
31 CFR Chapter X 1010.652 (a)-(b)	Special measures against Myanmar Mayflower Bank and Asia Wealth Bank
31 CFR Chapter X 1010.653	Special measures against Commercial Bank of Syria
31 CFR Chapter X 1010.654	Special measures against VEF Bank
31 CFR Chapter X 1010.655	Special measures against Banco Delta Asia
31 CFR 1 Chapter X 1010.670(a)-(f)	Summons or subpoena of foreign bank records; termination of correspondent relationship
31 CFR Chapter X 1010.710	Administrative rulings scope
31 CFR Chapter X 1010.711(a)-(e)	Submitting requests
31 CFR Chapter X 1010.712	Nonconforming requests
31 CFR Chapter X 1010.713(a)(b)	Oral communications
31 CFR Chapter X 1010.714	Withdrawing requests
31 CFR Chapter X 1010.715	Issuing rulings
31 CFR Chapter X 1010.716(a)-(d)	Modifying or rescinding rulings
31 CFR Chapter X 1010.717(a)(b)	Disclosing information
31 CFR Chapter X 1010.810(a)-(g)	Enforcement
31 CFR Chapter X1010.820(a)-(h)	Civil penalty
31CFR Chapter X 1010.830	Forfeiture of currency or monetary instruments
31 CFR Chapter X 1010.840 (a)-(d)	Criminal penalty
31 CFR Chapter X 1010.850 (a)-(c)	Enforcement authority with respect to transportation of currency or monetary instruments
31 CFR Chapter X 1010.911	Summons-General
31 CFR Chapter X 1010.912(a)-(c)	Persons who may issue summons
31 CFR Chapter X 1010.913(a)&(b)	Contents of summons
31 CFR Chapter X 1010.914(a)-(c)	Service of summons

Key U.S. AML and Sanction Laws and Regulations	
31 CFR Chapter X 1010.915(a)-(c)	Examination of witnesses and records
31 CFR Chapter X 1010.916	Enforcement of summons
31 CFR Chapter X 1010.917	Payment of expenses
31 CFR Chapter X 1010.920	Access to records
31 CFR Chapter X 1010.930(a)-(c)	Rewards for informants
31 CFR Chapter X 1010.940(a)&(b)	Photographic or other reproductions of Government obligations
31 CFR Chapter X 1010.950(a)-(f)	Availability of information
31 CFR Chapter X 1010.960	Disclosure
31 CFR Chapter X 1010.970(a)-(c)	Exceptions, exemptions, and reports
31 CFR Chapter X 1010.980	Dollars as including foreign currency
31 CFR Chapter X 1020.100(d)(1); 1023.100(e) (1); 1010.100; 1020.210; 1023.210(a)(b); 1026.210(b)(1)&(2)	Anti-money laundering program requirements for financial institutions regulated by a federal functional regulator or a self-regulatory organization, and casinos (AML program)
31 CFR Chapter X 1020.100; 1020.220	Customer identification programs for banks, savings associations, credit unions, and certain nonfederally regulated banks (CIP)
31 CFR Chapter X 1020.315(a)-(i)	Transactions of exempt persons
31 CFR Chapter X 1020.320(a)-(f)	Reports by banks of suspicious transactions (SAR)
31 CFR Chapter X 1020.410 (b)(c)	Additional records to be made and retained by banks
31 CFR Chapter X 1021.100	Special terms for casinos
31 CFR Chapter X 1021.210(b)	Special rules for casinos
31 CFR Chapter X1021.313	Multiple transactions - casinos
31 CFR Chapter X1021.320(a)-(g)	Reports by casinos of suspicious transactions (SAR)
31 CFR Chapter X 1021.410 (a)-(c)	Additional records to be made and retained by casinos
31 CFR Chapter X 1022.210(a)-(e)	Anti-money laundering programs for money services businesses (MSB) (AML program)
31 CFR Chapter X1022.320(a)-(f)	Reports by money services businesses (MSB) of suspicious transactions (SAR)
31 CFR Chapter X 1022.380(a)-(f)	Registration of money services businesses (MSB)
31 CFR Chapter X 1022.410 (a)-(c)	Additional records to be made and retained by currency dealers or exchangers
31 CFR Chapter X 1023.100; 1023.220	Customer identification programs for broker-dealers (CIP)
31 CFR Chapter X 1023.320(a)-(h)	Reports by brokers or dealers in securities of suspicious transactions (SAR)
31 CFR Chapter X 1023.410 (a)(b)	Additional records to be made and retained by brokers or dealers in securities
31 CFR Chapter X 1024.100; 1010.100; 1010.605	Customer identification programs for mutual funds (CIP)
31 CFR Chapter X 1024.210(a)(b);	Anti-money laundering programs for mutual funds (AML program)
31 CFR Chapter X 1024.320(a)-(g)	Reports by mutual funds of suspicious transactions (SAR)
31 CFR Chapter X 1025.100; 1025.210(a)-(d):	Anti-money laundering programs for insurance companies (AML program)
31 CFR Chapter X 1025.320(a)-(h)	Reports by insurance companies of suspicious transactions (SAR)
31 CFR Chapter X 1026.100; 1026.220	Customer identification programs for futures commission merchants and introducing brokers (CIP)
31 CFR Chapter X 1026.320(a)-(h)	Reports by futures commission merchants and introducing brokers in commodities of suspicious transactions (SAR)

Key U.S. AML and Sanction Laws and Regulations	
31 CFR Chapter X 1027.100; 1027.210(a)-(c);	Anti-money laundering programs for dealers in precious metals, precious stones or jewels (AML program)
31 CFR Chapter X 1028.100; 1028.210 (a)(b)	Anti-money laundering programs for operators of credit card systems (AML program)
31 CFR 103, Appendix A to Subpart I of Part 103	Certification regarding correspondent accounts for foreign banks (foreign bank certification)
31 CFR 103, Appendix B to Subpart I of Part 103	Recertification regarding correspondent accounts for foreign banks
31 CFR 103, Appendix B to Part 103	Certification for purposes of Section 314(b) of the USA PATRIOT Act and 31 CFR 103.110
H.R. 2194	Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA)
50 USC 1701-1707	International Emergency Economic Powers Act (IEEPA)
50 USC 1701	Iran Sanctions Act of 1996 (ISA)
H.R. 1905	Iran Threat Reduction and Syria Human Rights Act of 2012 (ITRSHRA)
H.R. 1540	National Defense Authorization Act for Fiscal Year 2012 (NDAA)
12 USC 95a	Trading with the Enemy Act of 1917 (TWEA)
31 CFR 500	Foreign Assets Control Regulations (OFAC)
31 CFR 501	Reporting, Procedures and Penalties Regulations
31 CFR 505	Regulations Prohibiting Transactions Involving the Shipment of Certain Merchandise Between Foreign Countries
31 CFR 510	North Korea Sanctions Regulations
31 CFR 515	Cuban Assets Control Regulations
31 CFR 535	Iranian Assets Control Regulations
31 CFR 536	Narcotics Trafficking Sanctions Regulations
31 CFR 537	Burmese Sanctions Regulations
31 CFR 538	Sudanese Sanctions Regulations
31 CFR 539	Weapons of Mass Destruction Trade Control Regulations
31 CFR 540	Highly Enriched Uranium (HEU) Agreement Assets Control Regulations
31 CFR 541	Zimbabwe Sanctions Regulations
31 CFR 542	Syrian Sanctions Regulations
31 CFR 543	Côte d'Ivoire Sanctions Regulations
31 CFR 544	Weapons of Mass Destruction Proliferators Sanctions Regulations
31 CFR 545	Taliban (Afghanistan) Sanctions Regulations
31 CFR 546	Darfur Sanctions Regulations
31 CFR 547	Democratic Republic of the Congo Sanctions Regulations
31 CFR 548	Belarus Sanctions Regulations
31 CFR 549	Lebanon Sanctions Regulations
31 CFR 551	Somalia Sanctions Regulations
31 CFR 560	Iranian Transactions Regulations (ITR)
31 CFR 561	Iranian Financial Sanctions Regulations (IFSR)
31 CFR 562	Iranian Human Rights Abuses Sanctions Regulations

Key U.S. AML and Sanction Laws and Regulations	
31 CFR 575	Iraqi Sanctions Regulations
31 CFR 576	Iraq Stabilization and Insurgency Sanctions Regulations
31 CFR 585	Federal Republic of Yugoslavia (Serbia and Montenegro) and Bosnian Serb-controlled Areas of the Republic of Bosnia and Herzegovina Sanctions Regulations
31 CFR 586	Federal Republic of Yugoslavia (Serbia and Montenegro) Kosovo Sanctions Regulations
31 CFR 587	Federal Republic of Yugoslavia (Serbia and Montenegro) Milosevic Sanctions Regulations
31 CFR 588	Western Balkans Stabilization Regulations
31 CFR 592	Rough Diamonds Control Regulations
31 CFR 593	Former Liberian Regime of Charles Taylor Sanctions Regulations
31 CFR 594	Global Terrorism Sanctions Regulations
31 CFR 595	Terrorism Sanctions Regulations
31 CFR 596	Terrorism List Governments Sanctions Regulations
31 CFR 597	Foreign Terrorist Organizations Sanctions Regulations
31 CFR 598	Foreign Narcotics Kingpin Sanctions Regulations
H.R.4954	Security and Accountability For Every Port Act of 2006, Title VII: Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA)
31 CFR 132	Prohibition on funding of unlawful Internet gambling
H.R. 2847	Hiring Incentives to Restore Employment Act (HIRE): Title V: Subtitle A: Foreign Account Tax Compliance Act (FATCA)

For additional information on the United States Code (USC), refer to www.gpoaccess.gov/uscode/; on the Code of Federal Regulations (CFR), refer to www.gpoaccess.gov/cfr/.

Useful Websites	
Protiviti	www.protiviti.com
KnowledgeLeader	www.knowledgeleader.com
Pillsbury Winthrop Shaw Pittman LLP	www.pillsburylaw.com
American Bankers Association (ABA)	www.aba.com
American Gaming Association (AGA)	www.americangaming.org
American Stock Exchange (AMEX/ASE)	www.amex.com
Bank for International Settlements/Basel Committee on Banking Supervision (BIS)/(BCBS)	www.bis.org
Bureau of Industry and Security (BIS)	www.bis.doc.gov
Central Intelligence Agency (CIA)	www.cia.gov
Code of Federal Regulations (CFR)	www.gpoaccess.gov/cfr/
Commodity Futures Trading Commission (CFTC)	www.cftc.gov
Consumer Financial Protection Bureau (CFPB)	www.consumerfinance.gov
Customs and Border Protection (CBP)	www.cbp.gov

Useful Websites	
Department of Defense (DoD)	www.defense.gov
Department of Homeland Security (DHS)	www.dhs.gov
Department of Health and Human Services (HHS)	www.hhs.gov
Department of Justice (DOJ)	www.usdoj.gov
Department of State (DOS)	www.state.gov
Department of the Treasury (DOT)	www.treas.gov
Egmont Group	www.egmontgroup.org
Electronic Payments Association (NACHA)	www.nacha.org
European Union	www.eurunion.org/eu
Federal Bureau of Investigation (FBI)	www.fbi.gov
Federal Deposit Insurance Corporation (FDIC)	www.fdic.gov
Federal Financial Institutions Examination Council (FFIEC)	www.ffiec.gov
Federal Reserve Bank of Boston Consumer Payments Research Center (CPRC)	www.bos.frb.org/economic/cprc
Federal Reserve Board (FRB)	www.federalreserve.gov
Financial Action Task Force (FATF)	www.fatf-gafi.org
Financial Crimes Enforcement Network (FinCEN)	www.fincen.gov
Financial Industry Regulatory Authority (FINRA)	www.finra.org
Government Accountability Office (GAO)	www.gao.gov
Global Trade Finance Program	www.ifc.org/
Homeland Security & Government Affairs: Permanent Subcommittee on Investigations	http://www.hsgac.senate.gov/subcommittees/investigations
Immigration and Customs Enforcement (ICE)	www.ice.gov/
Internal Revenue Service – Criminal Investigations (IRS-CI)	www.irs.gov/compliance/enforcement/
Internal Revenue Service (IRS)	www.irs.gov
International Association of Insurance Supervisors (IAIS)	www.iaisweb.org
International Chamber of Commerce	www.iccwbo.org
International Labour Organization	www.ilo.org
International Monetary Fund (IMF)	www.imf.org
International Trade Administration (ITA)	www.ita.doc.gov
International Organization of Securities Commissions	www.iosco.org
Managed Funds Association (MFA)	www.mfainfo.org
Money Services Businesses (MSB)	www.fincen.gov/financial_institutions/msb
Money Transmitter Regulators Association (MTRA)	www.mtraweb.org

Useful Websites	
National Association of Insurance Commissioners (NAIC)	www.naic.org
National Credit Union Administration (NCUA)	www.ncua.gov
National Futures Association (NFA)	www.nfa.futures.org
National Geospatial Intelligence Agency	www1.nga.mil
Network Branded Prepaid Card Association	www.nbpca.org
New York Clearing House Association (NYCH)	www.theclearinghouse.org
New York Stock Exchange (NYSE)	www.nyse.com
Office of Foreign Assets Control (OFAC)	www.treas.gov/ofac
Office of National Drug Control Policy	www.whitehousedrugpolicy.gov
Office of Terrorism and Financial Intelligence (OTFI)	www.treas.gov/offices/enforcement/
Office of the Comptroller of the Currency (OCC)	www.occ.treas.gov
Organisation for Economic Co-operation and Development (OECD)	www.oecd.org
Polaris Project	www.polarisproject.org
U.S. Securities and Exchange Commission (SEC)	www.sec.gov
Security Industry Association (SIA)	www.siaonline.org/
Society for International Affairs	www.siaed.org
Society for Worldwide Interbank Financial Telecommunications (SWIFT)	www.swift.com
Treasury Executive Office for Asset Forfeiture and Treasury Forfeiture Fund (TEOAF)	www.treas.gov/offices/enforcement/teoaf/
Trade Compliance Center (TCC)	http://tcc.export.gov/
Trade Information Center	www.export.gov
Transparency International (TI)	www.transparency.org
United Nations (UN)	www.un.org
United States Code (USC)	www.gpoaccess.gov/uscode
Wolfsberg AML Principles	www.wolfsberg-principles.com
World Bank (WB)	www.worldbank.org
World Trade Organization	www.wto.org

ABOUT PROTIVITI

Protiviti (**www.protiviti.com**) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE® 1000 and Global 500 companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

Our Anti-Money Laundering Practice

Protiviti has a dedicated AML team within its Regulatory Risk Consulting practice. Composed of former regulators, fraud and forensic specialists, and technology experts, Protiviti's AML team members have considerable experience advising institutions of all types on the design and implementation of their AML programs, conducting independent tests of AML program effectiveness and conducting money laundering investigations.

Anti-Money Laundering Solutions

Increasingly, companies are realizing the importance of implementing a risk-based AML Compliance Program that can be applied across diverse business lines; however, evaluating the money laundering risks in an organization and the tools and techniques available for mitigating these risks can present a significant challenge. Protiviti provides a wide variety of consultative services designed to assist organizations in all aspects of AML compliance, including the following:

Risk Assessment

An effective and complete AML program considers the business and customer profile of an institution. We can review the institution's business, customers and transactions to identify areas with high potential for exposure to money laundering and/or OFAC violations.

Program Development and Implementation

AML risk management requires companies to identify, measure, control and monitor money laundering risk effectively. Our professionals have assisted and continue to assist a variety of clients with developing and implementing comprehensive AML programs that address the latest regulatory and industry expectations and the company's own unique money laundering risk. This includes documentation of the AML program in the form of customized policies and procedures.

Gap Analysis

A gap is often defined as the “space between the firm’s current state and where the firm feels its state should be” (due to regulatory expectations and/or leading practices). We work with the firm to identify those gaps and help them develop an action plan to move the compliance function forward.

OFAC Program Reviews

We work with a variety of organizations to review existing OFAC programs and make recommendations for enhancements. We also assist in the development, implementation and documentation of an effective OFAC program.

Money Laundering Investigations

Money laundering schemes are becoming increasingly sophisticated and complex. Our professionals identify the flow of funds from originator to ultimate beneficiary and identify the parties and the financial institutions involved. We identify the types of instruments used in the scheme(s), determine the amount of funds involved, and identify relationships between related parties. We trace assets through the financial system and assist with their ultimate recovery.

Independent Testing

We perform testing of existing AML programs, including a review of written AML policies and procedures, the AML training program, and AML-related technology reviews. We also perform selected transaction testing and provide recommendations for enhancements. Testing is performed independently of the AML compliance function to meet USA PATRIOT Act requirements.

Regulatory Remediation

Should your organization become the subject of an enforcement action, we can assist you with identifying the root cause and magnitude of the issue, and the improvements necessary to prevent recurrence; negotiating regulatory agreements; developing and implementing corrective action plans; and liaising with regulatory agencies and/or outside counsel.

AML Training

Customized and relevant AML training provides the basis for a successful AML program. We assist organizations with the development, implementation and delivery of AML training that is customized to reflect your company’s primary business activities, customer profile, current AML knowledge base and internal procedures.

Software Vendor Selection and Utilization

We can assist in the selection of appropriate technology tools to support ongoing AML and OFAC monitoring. This includes current and future requirements, vendor review and assessment scorecarding, project planning and management, implementation support, system tuning and system validation.

For additional information about Protiviti’s AML services, please contact:

Carol M. Beaumier
Managing Director/Global AML Practice Leader
Phone: 212.603.8337
Fax: 212.399.8794
carol.beaumier@protiviti.com

THE AMERICAS

United States

Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Woodbridge

Argentina
Buenos Aires*

Brazil
Rio de Janeiro*
São Paulo*

Canada
Kitchener-Waterloo
Toronto

Mexico
Mexico City*
Monterrey*

Peru
Lima*

Venezuela
Caracas*

EUROPE

France
Paris

Germany
Frankfurt
Munich

Italy
Milan
Rome
Turin

The Netherlands
Amsterdam

United Kingdom
London

MIDDLE EAST

Bahrain
Manama*

Kuwait
Kuwait City*

Oman
Muscat*

United Arab Emirates
Abu Dhabi*
Dubai*

ASIA-PACIFIC

Australia
Brisbane
Canberra
Melbourne
Perth
Sydney

China
Beijing
Hong Kong
Shanghai
Shenzhen

India
Bangalore
Mumbai
New Delhi

Indonesia
Jakarta**

Japan
Osaka
Tokyo

Singapore
Singapore

South Korea
Seoul

* Protiviti Member Firm
** Protiviti Alliance Member

protiviti®
Risk & Business Consulting.
Internal Audit.

©2012 Protiviti Inc. An Equal Opportunity Employer. PRO-1112-101045
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.