Powerful Insights. Proven Delivery.®

Guide to U.S. Anti-Money Laundering Requirements

Fourth Edition

protiviti®
Risk & Business Consulting.
Internal Audit.

PREFACE

Protiviti is pleased to publish this fourth version of its *Guide to U.S. Anti-Money Laundering Requirements*. As with the first three editions of the Guide, this 2010 edition contains questions that have surfaced in our discussions with clients, attorneys, regulators and others, both in the United States and other markets. The number of questions and answers has been expanded from the previous version. Among the new information included are questions and answers related to rules and regulatory requirements issued in the past two years, as well as expanded discussions on a number of topics, including risk assessments, anti-money laundering (AML) and sanction compliance technology, and international perspectives and initiatives.

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, Risk Assessments, (including expanded discussion of high-risk customers), Transaction Monitoring and Investigations, Third-Party Reliance, AML Technology, Nonbank Financial Institutions and Nonfinancial Businesses, Convergence of AML with Fraud and Other Regulatory Topics, and International Perspectives and Initiatives. Also included in the resource sections at the back of the Guide are website addresses for some of the sources used to develop the questions and answers, a glossary of useful acronyms, and a listing of key AML laws and regulations. Although the focus of the Guide is on U.S. requirements, we have included some highlights of multilateral requirements and believe the Guide is instructive to companies outside of the United States because of the convergence of AML requirements and industry best 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 that many of the responses included in this booklet will continue to evolve.

Protiviti Inc.
October 2010

Acknowledgements

This booklet was developed through the collaborative effort of Protiviti's AML team, particularly Daniel Haggerty and Kaitlin Lemmo, and our colleague and former associate Karen L. Wilkes. The Protiviti AML team extends special thanks to Deborah Thoren-Peden of Pillsbury Winthrop Shaw Pittman LLP, who served as a reviewer.

CONTENTS AT A GLANCE

TABLE OF CONTENTS

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, tax evasion, 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. Notwithstanding the attempts of many organizations and academics to estimate the volume of money laundering, one of the most cited measurements, though it is somewhat dated, was developed by the International Monetary Fund (IMF), which estimated the volume of money laundering to be between 2 and 5 percent of global gross domestic product (GDP), equivalent to approximately $590 billion to $1.5 trillion annually. While this range may still be the best estimate, there have been suggestions that certain regional and global trends, such as the increase in trade with the expansion of the European Union (EU), are contributing to an increase in the volume of money laundering.

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 also 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?

As a result of the terrorist activities of September 11, 2001, the U.S. strengthened its AML regulations significantly. The USA PATRIOT Act expanded the traditional definition of a financial institution. It was broadened to encompass numerous businesses that previously were not subject to AML regulations. For example, U.S. AML regulations apply to, among others, casinos and dealers in precious metals and jewelry, which were previously unregulated businesses. The USA PATRIOT Act also required sweeping measures to be taken with respect to shell banks and correspondent accounts.

While these measures may not have been incorporated previously into other countries' AML standards, the continued international focus on AML standards has encouraged many countries to introduce several new AML regulations, which, in large part, already have been implemented in the United States because of the USA PATRIOT Act.

Unlike Australia and the United Kingdom, the United States has not implemented regulations for select "professional service providers" (e.g., attorneys, accountants). In fact, the Financial Action Task Force (FATF), in its most recent assessment of the United States' anti-money laundering 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, and real estate agents). For additional guidance, please refer to the Financial Action Task Force and Mutual Evaluation Reports 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], U.S. Securities and Exchange Commission [SEC]). 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.
- **The Federal Deposit Insurance Corporation (FDIC)** regulates federally charted banks (e.g., state-chartered banks that do not belong to the Federal Reserve System).
- **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.
- **The National Credit Union Administration (NCUA)** regulates federally chartered credit unions.
- **The Office of Thrift Supervision (OTS)** oversees federal savings and loans and federal savings banks. (As a result of the Wall Street Reform and Consumer Protection Act, known as the Dodd-Frank Act, the OTS will be dissolved and its supervisory responsibilities will be transferred to the FRB, OCC and FDIC.)

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 five federal regulators: FRB, FDIC, OCC, NCUA, OTS 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.

- **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, 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 OTS 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, stored value, 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.

FinCEN also has created several communication systems to facilitate the sharing of information among both domestic and international entities. The PATRIOT Act Communication System (PACS) 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 questions that answer basic questions asked about BSA and USA PATRIOT 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.

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 are generally report findings (and accompanying fines that have been modest compared to those levied against banks) that detail the nature of the deficiency, but do not prescribe specific corrective action.

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, may result from legal actions.

30. 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. Examples would include:

- Banking Organizations:
    - **ABN Amro**: In December 2005, ABN Amro was assessed an $80 million CMP (civil money penalty) 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 effectively manage its money laundering and terrorist financing risk
    - **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

- 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:
    - **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

31. 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 testing, validation and documentation of automated monitoring systems (e.g., inadequate sample sizes, inexperienced testers, incomplete/inadequate scope, incomplete follow-up on prior exceptions, and review/challenging of management's response)
- 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

32. 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.

33. 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 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.

34. 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.

35. 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.

36. 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. Even foreign financial institutions without U.S. operations are impacted by the BSA if they maintain correspondent relationships in the United States or otherwise clear USD through the United States.

37. 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

38. 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.

39. 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.

40. 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.

41. 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.

42. 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 use 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.) 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.

43. How do financial institutions submit CTRs to FinCEN?

Financial institutions can submit CTRs manually or through the PATRIOT Act Communication System (PACS), an Internet-based e-filing system developed by FinCEN to enable financial institutions to file CTR and SAR forms electronically. While the use of PACS 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.

44. 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.

45. How long should a financial institution retain CTRs?

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

46. 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.

47. 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.

48. 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.

49. 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.

50. What guidance has been issued related to CTRs?

The following key guidance 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 by FinCEN
    - BSA Electronic Filing Requirements for the Currency Transaction Report (CTR) (FinCEN Form 104) and Designation of Exempt Person (DOEP) (FinCEN Form 110) by FinCEN
    - Notice to Customers: A CTR Reference Guide by FinCEN
    - Reporting of Certain Currency Transactions for Sole Proprietorships and Legal Entities Operating Under a "Doing Business As" (DBA) Name by FinCEN
- Exemptions
    - 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, 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 by the United States Government Accountability Office (GAO)
    - Guidance on Determining Eligibility for Exemption from Currency Transaction Reporting Requirements by FinCEN
    - Revision of the CTR Exemption Rule: Completion of FinCEN Form 110 by FinCEN
    - 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 by FinCEN
    - Frequently Asked Questions: Concerning Completion of Part II of FinCEN Form 104, Currency Transaction Report by FinCEN
    - CTR Exemption Regulation Amended to Include MMDAs by FinCEN
- Casinos
    - Frequently Asked Questions: Casino Recordkeeping, Reporting, and Compliance Program Requirements 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 by FinCEN

CTR Threshold and Aggregation

51. 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.

52. 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., < $10,000). GTOs

are used to collect information on individuals/entities suspected of conducting transactions under reportable thresholds.

53. 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.

54. 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.

55. 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.

56. 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

57. 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.

58. 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

59. 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

60. 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.

61. 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.

62. 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.

63. 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

64. 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.

65. 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.

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

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

67. 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.

68. 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.

69. 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.

70. 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

71. 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.

72. 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.

73. 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 regularly 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

74. Are all transactions conducted by an exempt person excluded from the reporting requirement?

Exemptions may not apply to all accounts maintained or transactions conducted by an exempted 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.

75. Can individuals be exempted from CTR filing requirements?

No. CTR exemptions cannot be granted to individuals.

76. 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 August 2009, a customer should be conducting at least five large currency transactions throughout the year to be considered for exemption.

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

Per the 2008 Final Rule – CTR Exemption Changes, which went into effect on January 5, 2009, depository institutions can 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.

78. 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.

79. 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.

80. 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.

81. How have the recent updates to the exemption process impacted the completion of the DOEP form?

To assist depository institutions in completing the DOEP, FinCEN provided the following guidance for items affected by this final rule:

- Depository institutions should disregard any references to biennial renewals that appear on the face of FinCEN Form 110 as well as in the instructions:
    - **DOEP Form**: Part I, Item 1b, "Biennial renewal"; Part II, Item 11; Part III, Item 19, second sentence; and Part V
    - **DOEP Instructions**: Second paragraph under the heading "When and where to file"; the second sentence under the heading "Specific Instructions" that begins, "Additionally, with regard to non-listed businesses. * * *"); and the instruction to Item 11 under the heading "Exempt Person Information"
- Depository institutions should disregard Part II, Item 10a, ''Bank'' and ''Government agency/Government authority''

82. 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.

83. 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.

84. 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.

85. 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.

86. 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.

87. 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.

88. 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.

89. 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.

90. 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

91. 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.

92. 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.

93. 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.

94. 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.

95. 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.

96. 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.

97. 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.

CTR Trends

98. What CTR statistics and trends are available?

Following are some notable statistics and trends quoted in the United States Government Accountability Office's (GAO) February 2008 Report to Congress, "Increased Use of Exemption Provisions Could Reduce Currency Transaction Reporting While Maintaining Usefulness to Law Enforcement Efforts":

- Over 15 million CTRs were filed in 2006 by more than 17,000 financial institutions, of which 65 percent (9.75 million) were filed by the top 100 largest financial institutions.
- Of the more than 42,000 CTR exemptions filed by banks in 2006, 21 percent (approximately 8,900) were Phase I and 79 percent (approximately 33,500) were Phase II. Of the 8,900 Phase I exemptions, 32 percent were banks, 40 percent were government entities, and 28 percent were listed companies or subsidiaries of listed companies. And of the 33,500 Phase II exemptions, less than 1 percent were payroll customers and greater than 99 percent were nonlisted businesses.
- Seventy-seven percent of financial institutions reported having customers eligible for Phase I exemptions; however, only 45 percent reported that they always or usually file Phase I exemptions. Eighty-three percent of financial institutions reported having customers eligible for Phase II exemptions; however, only 49 percent reported that they always or usually file Phase II exemptions.
- A leading reason given by financial institutions for not maximizing exemptions is the difficulty in determining the percentage of a customer's gross revenue derived from business activity that is not eligible for exemption.
- The top 10 cities for CTR filings from 2004 to 2007 were, in descending order: Los Angeles, New York, Chicago, Houston, Las Vegas, Miami, Brooklyn, Dallas, Philadelphia and San Francisco.
- Approximately 65 percent of all CTRs filed resulted from aggregated, rather than single, transactions.

FinCEN published the following key statistics in its 18-month study "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":

- DOEP filings fell 44 percent to the lowest levels ever
- DOEP filings for banks, government agencies and governmental authorities dropped nearly 75 percent
- Initial designations for eligible nonlisted businesses increased 53 percent, indicating that many depository institutions were taking advantage of the new streamlined exemption process

- The total number of CTRs filed in 2009 declined nearly 12 percent compared with the previous year, dropping from 15.5 million to 13.7 million, indicating that the adoption of the amended CTR exemption rules have helped reduce the overall volume of CTR filings

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

99. 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) conducted at or through a financial institution.

100. 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.

101. Who is required to file SARs?

As of the time of this publication's preparation, broker-dealers, futures commission merchants, introducing brokers (IBs) in commodities, money services businesses (MSBs), casinos, card clubs, mutual funds, insurance companies and depository institutions (including insured banks, savings associations, savings associations service corporations, credit unions, bank holding companies, nonbank subsidiaries of bank holding companies, Edge and agreement corporations, and U.S. branches and agencies of foreign banks) are all required to file SARs. As AML regulations continue to evolve, other types of financial institutions also may be required to file SARs.

102. There are several types of SARs (e.g., SAR-DI, SAR-SF, SAR-MSB). Which one should a financial institution file?

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.

FinCEN is currently revising a number of the SAR forms; financial institutions should take extra care to ensure they are filing the correct forms. For additional guidance on the SAR reporting requirements for NBFIs, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

103. 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.

104. 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.

105. 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.

106. 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.

107. 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.

108. Where are SARs filed?

SARs are filed with FinCEN at the IRS Enterprise Computing Center – Detroit (formerly the Detroit Computing Center). It is 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.

109. How can financial institutions submit SARs to FinCEN?

Financial institutions can submit SARs manually, via regular mail, or through the BSA Direct E-Filing System, an Internet-based e-filing system developed by FinCEN to enable financial institutions to file and batch CTR and SAR forms electronically. While the use of this system can be beneficial for all financial institutions, its use is generally more cost-effective for financial institutions with a large volume of SAR filings, since it enables the batching of forms. Further information can be found on the U.S. Treasury Department website: http://bsaefiling.fincen.treas.gov/main.html.

110. 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.

111. 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.

112. 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 senior management (other than AML compliance personnel) and the board of directors need only be notified of SAR filings and need not be involved in the decision to file or not file a SAR; however, boards of directors must be notified of SAR filings, and prudent risk management would dictate that senior management also be apprised.

113. 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
- SAR Narrative Guidance Package
    - Part I: Guidance on Preparing a Complete and Sufficient Suspicious Activity Report Narrative
    - Part II: The Suspicious Activity Report (SAR) Form
    - Part III: Keys to Writing a Complete and Sufficient SAR Narrative

- Suspicious Activity Report Supporting Documentation
- 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
- Unauthorized Disclosure of Suspicious Activity Reports
- Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies
- Guidance on Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities
- BSA E-Filing System: Frequently Asked Questions (FAQs)
- Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting
- Requirements for Correcting Errors in Electronically Batch-Filed Suspicious Activity Reports
- Reporting Suspicious Activity – A Quick Reference Guide for MSBs
- Suspicious Activity Reporting Guidance for Casinos
- Frequently Asked Questions Suspicious Activity Reporting Requirements for Mutual Funds
- Frequently Asked Questions Anti-Money Laundering Program and Suspicious Activity Reporting Requirements for Insurance Companies
- Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption
- Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering
- Mortgage Fraud Related Guidance
    - Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding Loan Modification/Foreclosure Rescue Scams
    - 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])
    - Mortgage Loan Fraud Connections with Other Financial Crime
    - Filing Trends in Mortgage Loan Fraud
    - Mortgage Loan Fraud: An Update of Trends Based Upon an Analysis of Suspicious Activity Reports
    - FinCEN Mortgage Loan Fraud Assessment

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

SAR Filing Time Frame and Date of Initial Detection

114. 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.

115. 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.

116. 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.

117. 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.

118. 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 the identity of the potential suspect(s).

119. 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.

120. 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 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 that is so egregious 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.

121. 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 Form

122. Who should be included in Part I, Subject Information, on the SAR form?

A person who or an entity that is a subject of the investigation should be included in Part I, Subject Information, on the SAR form. 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.

123. Should all signers of an account be included in Part I, Subject Information, on the SAR form?

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.

124. What dates should be entered in Part II, Suspicious Activity Information, Section 22, Date or Date Range of Suspicious Activity on the SAR form?

Part II, Section 22 of the SAR form 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, 2008, to June 30, 2008, as part of an internal investigation; however, the reportable activity only may have occurred from February 4, 2008, to February 28, 2008. It is this latter date range that should be entered in Part II, Section 22.

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

125. What steps should a financial institution take to calculate Part II, Suspicious Activity Information, Section 23, 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.

126. What steps should a financial institution take to calculate Part II, Suspicious Activity Information, Section 23, 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.

127. What accounts should be included in Part III, Reporting Financial Institution Information, Section 41, Account Number(s) Affected, on the SAR form?

All accounts at a financial institution in which the reportable activity was discovered should be included in Part III, Section 41 on the SAR form 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.

128. What level of detail should a financial institution include in Part V, Suspicious Activity Information Narrative, on the SAR form?

Part V on the SAR form requires a narrative to explain 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). Tables, charts or other objects should not be used – only free-form text. 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.

129. 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, tax evasion, identity theft, wire fraud). The investigation of the underlying crime is the responsibility of law enforcement.

When evaluating suspicious activity and completing the SAR form, financial institutions should, to the best of their ability, describe the suspicious activity by selecting all applicable characteristics as provided in Part II, Section 24 on the SAR form (e.g., bribery/gratuity, defalcation/embezzlement).

130. 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.

131. 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.

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

No. Supporting documentation should not be forwarded to FinCEN with the SAR; however, 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

133. 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. In other words, no financial institution, 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. In March 2009, FinCEN proposed to clarify existing guidance on confidentiality. The proposed rule expands confidentiality not just to the SAR, but also to any information that would reveal the existence of a SAR.

134. 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 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 usually can be sent by alerting the business unit to the underlying activity without detailing the filing of the SAR itself.

135. What is the interagency guidance on sharing SARs?

FinCEN and the federal banking agencies issued interagency guidance in January 2006 concerning the sharing of SARs with head offices and controlling companies. The guidance confirms that the U.S. branch or agency of a foreign bank may share a 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.

In March 2009, FinCEN proposed to clarify existing guidance on interagency sharing. The proposed rule permits a depository institution 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.

136. Can SARs be shared with subsidiaries and affiliates?

Currently, a financial institution may not share SARs with nonparent entities, such as subsidiaries or affiliates. However, financial institutions may disclose to affiliates the information that supports a SAR filing. In March 2009, FinCEN proposed to clarify guidance on sharing with subsidiaries and affiliates. The proposed rule permits depository institutions to share SARs and information related to SARs to U.S. affiliates as long as the affiliate is subject to SAR regulations.

137. 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 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.

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

No. Institutions are expected to conduct a thorough investigation of all potentially suspicious activity, which may include requesting an explanation from customers or witnesses. However, staff responsible for contacting customers should be continually reminded of the need to protect the confidentiality of the SAR filing itself. Breaching confidentiality could jeopardize investigations conducted by law enforcement agencies and result in sanctions.

139. 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.

140. Are internal investigations that do not result in the filing of a SAR considered SAR-related? If so, does the same confidentiality apply?

The information contained in internal investigations that do not lead to a SAR filing is not covered under the terms of the Safe Harbor. However, financial institutions should apply the same rules of confidentiality that they do for a SAR to internal investigations that do not lead to a SAR filing.

141. 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 and the financial institution deems the inquiry suspicious, 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 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 and the financial institution's regulator should be notified promptly of the request.

Joint Filings of SARs

142. 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 the financial institution. However, sharing of such information must be done in compliance with regulatory guidance and applicable privacy laws.

143. What is the purpose of joint SAR filings?

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

144. 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

145. 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 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, regardless of whether such reports are filed pursuant to the SAR instructions. The Safe Harbor may not apply to SARs filed maliciously.

146. 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.

147. 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.

148. 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 financial institution, as that term is defined in the USA PATRIOT Act, whether mandatory or voluntary.

149. 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 reporting are through methods considered to be in accordance with the regulations of the applicable agency and applicable law.

150. 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 is protected by the Safe Harbor provisions applicable to both voluntary and mandatory suspicious activity reporting by financial institutions.

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

No. However, FinCEN's proposed rules 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 by financial institutions.

Monitoring and Terminating Relationships with SAR Subjects

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

Although the AML compliance officer may make a recommendation, the decision to exit a relationship with a SAR subject is really a business decision. 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.

153. 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.

154. 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, is 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.

155. 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.

156. 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.

157. 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.

158. 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).

159. 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

160. 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 voluntarily to law enforcement suspicious transactions that may relate to recent terrorist activity against the United States.

161. 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.

162. 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, 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; 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.

163. 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 in the United States.

164. 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 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.

165. 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. However, 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.

166. 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) 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.

167. 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.

168. 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

169. 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.

170. 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.

171. 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.

172. 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

173. What are some of the trends in SAR filings related to depository institutions?

According to FinCEN, some of the trends of SAR filings related to depository institutions include, but are not limited to, the following:

- The number of SAR filings increased from 62,388 in 1996 to 720,309 in 2009
- Calendar year 2009 marked the first year since 1996 there was a decline in total SARs submitted by depository institution and MSBs, dropping from approximately 1.29 million SARs in 2008 to 1.28 million in 2009. Filings by the remaining types of financial institutions saw a slight increase in 2009
- Depository institution SARs and MSB SARs accounted for almost 98 percent of all SARs filed in 2009
- In 2000 through 2008, total SAR filings by depository institutions grew from approximately 163,000 to 732,000 per year, an increase of nearly 350 percent. Experts attribute the increase to the implementation and more effective use of automated monitoring systems, heightened awareness and scrutiny due to public enforcement actions, greater awareness of and training on AML requirements after September 11, 2001 and more regulator guidance for examinations
- Twenty-seven percent of the suspicious activity reported by depository institutions in 2009 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, and wire transfer fraud); mortgage loan fraud and check fraud remain the only summary characterizations that have experienced an increase every year since 1996
- Reports indicating terrorist financing increased 8 percent in 2009, making it the first such increase since 2004
- Filings for 2009 further revealed a 9 percent decrease in reports indicating identity theft from those filed the prior year; Delaware and California consistently ranked among the top three states associated with this specific characterization for the last two years
- The top 10 SAR filing cities from 2004 to 2007 were, in descending order: New York, New York; Los Angeles, California; Phoenix, Arizona; Houston, Texas; Brooklyn, New York; Flushing, New York; Chicago, Illinois; Wilmington, Delaware; San Jose, California; and San Diego, California

For additional trends in SAR filings for other types of financial institutions, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

Form 8300

Form 8300 Basics

174. 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.

175. What is the value of Form 8300?

Form 8300 is useful to 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.

176. 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.

177. 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

178. 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

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

Designated reporting transactions include retail sales of a consumer durable, 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.

180. 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.

181. Can Form 8300 be submitted 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 Internal Revenue Service (IRS) for any suspicious transaction(s), even if the total does not exceed $10,000.

182. 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.

183. Should additional Forms 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).

184. 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 or Puerto Rico (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

185. Are wholesalers subject to Form 8300 reporting requirements?

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

186. 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.

187. 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.

Notification

188. 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.

189. 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 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

190. 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

191. 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.

192. 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.

193. 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.

194. 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.

195. 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.

196. 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)
- Form 8300 – Report of Cash Payments Over $10,000 Received in a Trade or Business (Online Video)
- When Businesses Should File Form 8300 for Cash Transactions (Webinar)
- Workbook on Reporting Cash Payments of Over $10,000
- FAQs Regarding Reporting Cash Payments of Over $10,000 (Form 8300)

Reporting Suspicious Activity on Form 8300

197. 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.

198. 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.

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

Yes. The Safe Harbor provision applies to all SAR filings by financial institutions, whether mandatory or voluntary, including suspicious activity reported on Form 8300.

200. 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.

Report of Foreign Bank and Financial Accounts

FBAR Basics

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

The Report of Foreign Bank and Financial Accounts (FBAR), TD Form 90-22, requires a U.S. person who, at any time during the calendar year, has a financial interest in or signature or other authority over any foreign financial account, including bank, securities or other financial account in a foreign country if the aggregate value of these financial accounts exceeds $10,000 (alone or in aggregate) to file the FBAR with the U.S. Department of the Treasury on or before June 30 for account(s) maintained during the previous calendar year..

202. What does the term “U.S. person” mean for FBAR filing purposes?

A “U.S. person” includes a citizen or resident of the United States, a domestic partnership, a domestic corporation or a domestic estate or trust. A person is 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.

203. Do FBAR filing requirement apply to non-U.S. persons “in and doing business in the United States”?

In October 2008, the FBAR instructions were revised such that non-U.S. persons “in and doing business in the United States” would be required to file FBARs. This created uncertainty and confusion among taxpayers and practitioners, leading the IRS in June 2009 to suspend FBAR reporting requirements temporarily for those who are not U.S. citizens, U.S. residents or domestic entities.

204. What is the benefit of the FBAR to law enforcement?

Similar to other reporting mandated under the Bank Secrecy Act (BSA), the FBAR is intended to aid in the detection of schemes by U.S. persons to hide the proceeds of money laundering and terrorist financing, tax evasion, or other criminal activities.

205. Are financial institutions required to file FBARs?

Yes. Financial institutions that have a financial interest in a bank, securities or other financial account in a foreign country in excess of $10,000 are required to file an FBAR. Financial institutions also may be required to file FBARs if they maintain customer accounts in which the bank has financial interest in, or which it has signature or other authority. An officer or employee of a bank which is currently examined by Federal bank supervisory agencies for safety and soundness need not report that he has signature or other authority over a foreign bank, securities or other financial account maintained by the bank, if the officer or employee has no personal financial interest in the account.

206. What does the term “foreign country” mean for FBAR filing purposes?

The term “foreign country” includes all geographical areas outside of the United States, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and the territories and possessions of the United States, including Guam, American Samoa and the U.S. Virgin Islands.

207. Does the nationality of the financial institution in which the account is held determine whether the account is foreign and therefore subject to FBAR requirement?

The geographical location of the account, not the nationality of the financial institution in which the account is held, determines whether it is an account in a foreign country.

With the exception of an 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. Accounts maintained with a branch, agency or other office of a foreign bank or other institution that is located in the United States do not need to be reported.

208. 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, whether the account is maintained for his or her own benefit or for the benefit of others, including non-U.S. persons.
- A U.S. person has 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
    - A corporation in which the U.S. person owns directly or indirectly more than 50 percent of the total value of 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)
    - 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
    - Account owners who hold an equity interest in a fund, including hedge and private equity funds
    - Account holders of debit and pre-paid credit cards meeting the FBAR reporting threshold

209. What does the term "financial account" mean for FBAR filing purposes?

The term "financial account" includes any bank, securities, 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). The term also includes 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.

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.

210. What constitutes "signature" or "other authority" over an account?

A person who has signature authority or other authority over an account has the ability to control the assets in an account. This authority can be exercised by, depending upon the type of authority, providing documents to or communicating with (e.g., orally) the financial institution.

211. 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.

212. Are there exceptions to the FBAR requirement?

FBARs are not required to be filed by the following:

- An officer or employee of a bank that is subject to supervision by the Office of the Comptroller of the Currency (OCC), Federal Reserve Bank (FRB), Federal Deposit Insurance Corporation (FDIC), or Office of Thrift Supervision (OTS), if the officer or employee has no personal financial interest in the account

- An officer or employee of a domestic corporation that has equity securities listed upon national securities exchanges or assets exceeding $10 million and 500 or more shareholders of record, if the officer or employee has no personal financial interest in the account and has been advised in writing by the chief financial officer of the corporation that the corporation has filed a current report, which includes that account
- Reports are not required for accounts held in military banking facilities, defined as U.S. military 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

FBAR Filing

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

The FBAR must be filed on or before June 30 of each calendar year.

214. What does the term "maximum value of account" mean for FBAR filing purposes?

The term "maximum value of account" means the largest amount of currency or nonmonetary assets that appears on any quarterly or more frequent account statements issued for the applicable 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. Convert foreign currency by using the official exchange rate at the end of the year.

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.

215. Should the maximum value of the account be reported in U.S. currency or the currency of the country in which the foreign accounts are held?

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

216. 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.

217. Can a corporation file one FBAR for all 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 them is made part of the consolidated report. An authorized official of the parent corporation should sign such consolidated reports.

218. How long should FBARs be retained?

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

219. 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 violation.

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 the individual or institution discovers he/she or it has failed to file appropriately, a delinquent FBAR should be submitted, and a statement attached explaining why the reports are filed late. It is possible for cumulative FBAR penalties to exceed the balance in the foreign financial account.

220. Can an extension for FBAR filing be obtained?

In addition to the fallback option of filing a delinquent FBAR report, on August 31, 2009, the IRS provided amnesty to those filers who met the following criteria:

- Persons with no financial interest in a foreign financial account, but with signature or other authority over the foreign financial account and/or;
- Persons with a financial interest in, or signature authority over, a foreign financial account in which the assets are held in a commingled fund.

The IRS granted a onetime extension for any individual who or entity that met these terms, and had not filed FBARs for either 2009 or any of the prior years (up to six years previous).

Persons with signature authority over, but no financial interest in, a foreign financial account for which an FBAR would otherwise have been due on June 30, 2010, have until June 30, 2011 to report those financial transactions. The deadline of June 30, 2011 applies to FBARs reporting foreign financial accounts over which the person has signature authority, but no financial interest for the 2010 and prior calendar years.

Persons with a financial interest in, or signature authority over, a foreign commingled fund that is a mutual fund are required to file an FBAR unless another filing exception applies. The IRS announced in Notice 2010-23 that it will not interpret the term "commingled fund" as applying to funds other than mutual funds with respect to FBARs for calendar year 2009 and prior years.

Recent Tax Scandals

221. Why have FBARs been in the news so often in the last few years?

Some recent high-profile tax scandals have highlighted the use of non-reported foreign accounts by U.S. taxpayers. Testimony to Congress reported widespread use of foreign financial facilities located in secrecy jurisdictions for the purpose of violating U.S. laws. Secret foreign bank accounts and secret foreign financial institutions allegedly permitted proliferation of white collar crimes; were used by Americans to evade income taxes, illegally conceal assets, and purchase gold; allowed Americans and others to avoid security laws and regulations; facilitated fraud schemes; served as a source of questionable financials for certain stock and merger activity; and allegedly covered conspiracies to steal from the U.S. defense and foreign aid funds, as well as engage in money laundering.

222. Given the likelihood that there are many 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.

FBAR Proposals

223. What actions are being taken in the United States to address the problem of unreported foreign bank accounts and otherwise deal with some of the current confusion over FBAR rules?

The Obama Administration has offered a number of proposals to increase tax reporting on compliance with the FBAR reporting requirements. In addition, in February 2010, FinCEN issued a notice of proposed rulemaking related to FBARs.

224. What is proposed in FinCEN's February 2010 notice of proposed rulemaking?

The proposed rule:

- Includes provisions intended to prevent persons from avoiding reporting requirements.
- Defines a "United States person" required to file the FBAR and defines the types of reportable accounts such as bank, securities, and other financial accounts.

- Exempts certain persons with signature or other authority over, but no financial interest in, foreign financial accounts from filing FBARs.
- Exempts certain low-risk accounts (e.g., the accounts of a government entity or instrumentality for which reporting will not be required).
- Exempts participants/beneficiaries in certain types of retirement plans and includes a similar exemption for certain trust beneficiaries.
- Clarifies what it means for a person to have a "financial interest" in a foreign account.
- Permits summary filing by persons who have a financial interest in 25 or more foreign financial accounts, or signature or other authority over 25 or more foreign financial accounts. Also permits an entity to file a consolidated FBAR on behalf of itself and the subsidiaries of which it owns more than a 50 percent interest.

The comment period for the notice of proposed rulemaking closed in April 2010; however, as of the time of publication, no further action had been taken.

Report of International Transportation of Currency or Monetary Instruments

CMIR Basics

225. 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

226. 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.

227. 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.

228. 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.

229. 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

230. Are persons transporting or shipping stored-value 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)?

Not currently. Stored-value products do not meet the regulatory definition of currency or monetary instruments; therefore, a CMIR is not required. However, FinCEN is considering whether to expand the obligations for reporting of prepaid access products that are taken across the border. FinCEN has also proposed new cross-border recordkeeping requirements for many types of electronic funds transfers. For additional guidance on stored value products, please refer to the Prepaid Access, Stored-Value and E-Cash section.

231. 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.

232. 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.

CMIR Filing

233. 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.

234. 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.

235. How long should CMIRs be retained?

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

Recordkeeping Requirements

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

The BSA requires the retention of all BSA reports (e.g., SAR-DIs, 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

237. 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).

238. 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.

239. 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.

240. 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.

241. 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 (e.g., check cashers, currency dealers or exchangers, issuers, sellers and redeemers of traveler's checks, money orders or stored value)
- 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

242. 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.

243. 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.

244. 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

245. 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).

246. 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.

247. 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.

Addresses and Abbreviations

248. 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.

249. 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.

250. 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.

251. 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

252. 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.

253. 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).

254. 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

255. 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.

256. 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.

257. 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.

258. 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

259. 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.

260. 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.

261. 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

262. 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.

263. 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."

264. 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 transmittor's financial institution
- Name and address of the transmittor
- The account number of the transmittor (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 transmittor or recipient (as applicable) or, if none, the alien identification number or passport number and country of issuance

265. 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 accountholder.

266. 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 transmittor is a bank and the recipient is a foreign bank, or the transmittor 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.

267. 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

268. 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

269. 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

270. 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.

271. 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.

272. 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.

273. 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.

274. 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.

275. 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.

276. 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).

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

277. 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.

278. 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, redeemer or cashier of traveler's checks, 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 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.

279. 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.

280. 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.

281. 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.

282. 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. 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 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 and Informal Value Transfer Systems sections.
- 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

283. 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

284. 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.

285. 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.

286. 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.

287. 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.

288. 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.

289. 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.

290. 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

291. 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

292. 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.

293. 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.

294. 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.

295. 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.

296. 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.

297. 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

298. 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.

299. 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.

300. 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.

301. 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

302. 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.

303. 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.

304. 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.

305. 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.

306. 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)
- Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking by The New York Clearing House Payments Co., LLC
- Wolfsberg AML Principles for Correspondent Banking by the Wolfsberg Group
- Wolfsberg Frequently Asked Questions on Correspondent Banking by the Wolfsberg Group
- The Wolfsberg Group and the Clearing House Association: Cover Payments: Some Practical Questions Regarding the Implementation of the New Payments by the Wolfsberg Group
- Correspondent Account KYC Toolkit: A Guide to Common Documentation Requirements 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 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 by FinCEN
- Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries by FinCEN
- Application of the Regulations Regarding Special Due Diligence Programs for Certain Foreign Accounts to NSCC Fund/SERV Accounts by FinCEN
- Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-border Wire Transfers 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

Due Diligence for Correspondent Accounts

307. 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 currency dealer or exchanger

308. 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

309. 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.

310. 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.

311. 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

312. Are there any particular challenges to monitoring correspondent clearing activity?

One of the challenges to effective monitoring of correspondent clearing activity is the quality of information received. While generally less of an issue today than in the past, wire transfer instructions from outside the United States do not always include complete details about the originator of and beneficiary to a transaction. For example, the originator may not be identified by name, but described only as "Our Valued Customer" or by a number.

313. 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.

314. Since more information is available with the MT202 COV "cover payment," do institutions have additional due diligence responsibilities?

Ordering institutions may consider screening payments against the sanction lists of their jurisdiction, and possibly against sanctions lists relevant to the entire chain of the payment instruction.

Intermediary institutions do not have additional responsibilities; however, they may experience an increased volume of potential hits from suspicious activity monitoring and sanctions screening due to the increase in available information on the underlying parties.

315. 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.

Enhanced Due Diligence for Correspondent Accounts

316. 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)

317. 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.

318. 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.

319. 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.

320. 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

321. 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

322. 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

323. 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)

324. 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.

325. 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.

326. 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 stance 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.

327. 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. For further guidance, please refer to the Beneficial Owners section.

328. 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.

329. 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

330. 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

331. 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.

332. 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.

Senior Foreign Political Figure

333. 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.

334. 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.

335. 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.

336. 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.

337. 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.

338. What is the heightened money laundering risk of PEPs?

Access to government funds may increase the potential for corruption and bribery.

339. 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.

340. 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).

In June 2004, the U.S. bank regulators and FinCEN issued an advisory related to accepting accounts from foreign governments, foreign embassies and foreign political figures, collectively referred to as "embassy banking." This release highlighted some of the considerations that should be addressed by financial institutions that offer embassy banking, including ensuring that embassy banking customers are aware of applicable U.S. AML laws and regulations.

Additional guidance includes the following:

- **Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption** by the FinCEN
- **Wolfsberg FAQs on Politically Exposed Persons** by the Wolfsberg Group
- **Guidance on Enhanced Scrutiny for Transactions That May Involve the Proceeds of Foreign Official Corruption** 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
- **Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption** by the Financial Crimes and Enforcement Network (FinCEN)
- **Stolen Asset Recovery: Politically Exposed Persons, A Policy Paper on Strengthening Preventive Measures** by the World Bank
- **Stolen Asset Recovery: Guide on Non-Conviction Based (NCB) Asset Forfeiture** by the World Bank

For further guidance on PEPs, please refer to the Politically Exposed Persons section.

Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks

341. 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

342. 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.

343. 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

344. 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.

345. 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.

346. 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.

347. 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.

348. 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.

349. 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.

350. 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

351. 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.

352. 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.

353. 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.

354. 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.

355. 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.

356. 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.

357. 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.

358. 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.

359. 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.

360. 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

361. 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.

362. 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).

363. 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.

364. 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)

365. 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.

366. 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.

367. 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.

368. 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.

369. 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.

370. 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.

371. 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.

372. Has FinCEN issued statistics relating to the usefulness of 314(a) requests?

Yes. FinCEN issued a 314(a) Fact Sheet in August 2010 that outlined a number of statistics relating to 314(a) requests. To date, FinCEN has processed 1,230 requests for information, including:

- 343 requests (28 percent) pertaining to terrorism-related cases
- 887 cases (72 percent) related to money laundering
- 11,939 subjects of interest, with approximately 79,181 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 resulted in arrests and 54 percent of the confirmations resulted in indictments.

373. 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.

Section 314(b) – Cooperation among Financial Institutions

Section 314(b) enables 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.

374. 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.

375. 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).

376. 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.

377. 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.

378. 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.

379. 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.

380. 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.

381. 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.

382. 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

383. 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.

384. 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.

385. 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.

386. 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")

387. 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.

388. 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

389. 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.

390. 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.

391. 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

392. 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.

393. 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.

394. 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).

395. 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.

396. 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.

397. 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.

398. 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.

399. How often must a foreign respondent update its foreign bank certification?

Foreign bank certifications are required to be renewed every three years.

400. 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)

401. 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.

402. 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.

403. 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.

404. 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.

405. 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.

406. 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.

407. 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.

408. 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.

409. 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

410. 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.

411. 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.

412. 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

413. 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

414. 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.

415. 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

416. 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

417. 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.

418. 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

419. 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.

420. 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."

421. 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.

422. 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.

423. 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.

424. 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.

425. 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.

426. 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.

427. 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.

428. 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.

Account Defined

429. 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.

430. 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

431. 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.

432. 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.

433. 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.

434. 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).

435. 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.

436. 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.

437. 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.

438. 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.

439. 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.

440. 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.

441. 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.

442. 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.

443. 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.

444. 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.

445. 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.

446. 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

447. 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.

448. 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

449. 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.

450. 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).

451. 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.

452. 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.

453. 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

454. 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.

455. 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

456. 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.

457. 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.

458. 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

459. 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

460. 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.

Section 352 – AML Program

Overview

461. 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

462. 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.

463. 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.

464. 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

465. 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 testing, validation and documentation of automated monitoring systems (e.g., inadequate sample sizes, inexperienced testers, incomplete/inadequate scope, incomplete follow-up on prior exceptions and review/challenging of managements responses)
- 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

466. 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)
- 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

467. 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.

468. 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.

469. 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.

470. 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

471. 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.

472. 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.

473. 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.

474. 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.

475. 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.

476. 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).

477. 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 decision to offer a new product or service, however, rests with the business.

478. 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.

479. 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, the decision to exit a customer relationship usually rests with the business.

AML Training

480. 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.

481. 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

482. 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.

483. 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.

484. 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).

485. 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.

486. 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.

487. 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.

488. 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.

489. 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.

490. 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

491. 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.

492. 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.

493. 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.

494. 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

495. 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.

496. 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.

497. 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.

498. 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.

499. 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.

500. 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.

501. 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.

502. 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.

503. 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 and qualifications 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.

504. 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.

505. 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.

506. 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?
- **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?
- **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?

For further guidance on technology solutions, please refer to the AML Technology section.

507. 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.

508. 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.

509. 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.

510. 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.

511. 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 and a strong grasp of how AML software works.

512. 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.

513. 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

514. 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) 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.

515. 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

516. 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.

517. 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.

518. 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.

519. 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."

520. 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.

521. 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.

522. Is there a dollar threshold applicable to prohibited transactions?

No. There is no defined minimum or maximum amount subject to OFAC regulations.

523. 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:

- Designating an individual to be responsible for OFAC compliance
- Conducting an OFAC risk assessment
- Conducting comprehensive and ongoing training
- Developing and implementing written OFAC policies and procedures
- Developing internal controls for OFAC compliance, including screenings of customers and transactions, as appropriate, against the OFAC Specially Designated Nationals (SDN) and Blocked Persons List, Country and List-Based Sanctions and Non-SDN Palestinian Council (NS-PLC) list, collectively referred to as "Sanctions listings"; blocking/rejecting transactions; and reporting blocked or rejected transactions
- 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)

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

524. 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.

525. 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.

526. 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.

527. 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.

528. 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.

529. 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)
        - Diamond Trading Sanctions (NONE)
        - Iran Sanctions ([IRAN], [IRGC], [IFSR], [IRAN-HR])
        - Iraq-related Sanctions (IRAQ)
        - Former Liberian Regime of Charles Taylor Sanctions (LIBERIA)
        - Lebanon-related Sanctions (LEBANON)
        - Nonproliferation Sanctions (NPWMD)
        - North Korea Sanctions ([NORTH KOREA], [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.
- **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, North Korea, 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 SDN list, licensing, technology from multiple industries (e.g., financial institutions, insurance, importers/exporters)
- **OFAC Risk Matrix** – A matrix that assists institutions with rating (low, medium, high) areas of its own OFAC program 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, OCC and OTS** – 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

530. 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).

531. 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.

532. Are all SDN designees foreign?

No. SDN designees consist of many nationalities, including U.S. individuals and entities, although most are foreign.

533. 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 to the Sanctions listings with greater frequency, sometimes as often as three times per week. As soon as a name is added to the Sanctions listings, OFAC expects compliance.

534. 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.

535. How can companies ensure the most recent vessels are included in their sanctions filter?

Vessels are included in the SDN list; however, the most recent updates may not be included in the latest SDN List issued by OFAC. To ensure the most recent vessels are included, companies should monitor OFAC's website for updates and update their sanctions filters accordingly.

536. Can an individual/entity be listed on multiple sanctions programs?

Yes. An individual/entity can appear on multiple sanctions programs.

537. 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.

538. 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.

539. What does a positive “hit” mean?

A positive “hit” is defined as a confirmed true match to the OFAC Sanctions listings.

540. 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

541. 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

542. 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.

543. 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.

544. 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.

545. 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

546. 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 has 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.

547. 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.

548. Are U-Turn payments allowed?

No. As of November 10, 2008, U-Turn payments are no longer allowed.

Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA)

549. 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?

The CISADA imposes new economic penalties that are designed to force Iran to change its conduct and end its nuclear weapons program. The law includes:

- Expanded scope of persons who may be sanctioned
- 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
- 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"
- 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 to 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

550. Since most commerce between the United States and Iran is already prohibited under existing sanction programs, what more is really gained by CISADA?

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 seeks to bring pressure on these foreign firms to cease their business operations with Iran.

551. Is CISADA a unilateral action on the part of the United States?

No. There is a multilateral effort underway to toughen Iranian sanctions. The enactment of CISADA followed the passage in June 2010 of a comprehensive Iran sanctions resolution by the UN Security Council. A few weeks after CISADA was signed into law by President Barack Obama, the European Union (EU) adopted its own package of Iranian sanctions. Other countries, such as Australia and Canada, also have followed suit.

552. How will CISADA 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) for Iran's production of refined petroleum industry; or
- Sell, lease or provide to Iran goods, services or technology, or provide at least $1 million (or, during a 12-month period, have an aggregate value of $5 million or more) for exportation of Iran's refined petroleum products.

Insuring, reinsuring, financing or brokering such transactions, or providing the ships for delivery, are also subject to new prohibitions. These prohibitions are collectively referred to as the "petroleum-related sanctions."

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.

553. 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.

554. CISADA requires the imposition of sanctions when a person "knowingly" invests. What does "knowingly" mean in this context?

"Knowingly" in this context means actual knowledge or constructive knowledge (i.e., the person should have known).

555. What sanctions will be imposed on foreign companies that violate CISADA's petroleum-related sanctions?

Nine possible sanctions may be imposed for violation of the petroleum-related 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

CISADA requires that at least three of the above sanctions be imposed when there is a finding that a person has violated the petroleum-related sanctions provision set forth in CISADA. The U.S. president, however, does have the authority to waive the imposition of sanctions.

556. 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.

557. 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.

558. Has the U.S. Treasury Department issued implementing regulations related to the prohibitions on U.S. financial institutions?

On August 16, 2010, the Treasury Department issued regulations 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. Other CISADA requirements are expected to be subject to additional rulemaking.

559. What are the major provisions of the Treasury Department's August 16, 2010, implementing regulations?

The Treasury Department's August 16, 2010, regulations 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.

560. 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.

561. 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.

562. 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.

563. 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)

564. How does CISADA treat pre-existing financial contracts?

At the time of our publication, regulations were silent on the treatment of pre-existing financial contracts. The industry has requested additional guidance from the U.S. Treasury Department.

565. How does CISADA define "financial services"?

CISADA's definition of "financial services" includes loans, transfers, accounts, insurance, investments, securities, guarantees, foreign exchange, letters of credit, and commodity futures or options.

566. 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. Additionally, on September 29, 2010, several individuals were added to the SDN list pursuant to CISADA. U.S. financial institutions are encouraged to monitor the Treasury Department's website for information on additions to Appendix A.

567. 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.

568. What steps do U.S. financial institutions need to take to ensure compliance with the requirements of CISADA?

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.

Screening Customers and Transactions

569. 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.

570. 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).

571. 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.

572. 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.

573. 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.

574. 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."

575. How does OFAC define the term "interest"?

"Interest" is broadly defined by OFAC as "any interest whatsoever, direct or indirect."

576. 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.

577. 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.

578. 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.

579. 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).

580. 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.

581. 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.

582. 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.

583. 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.

584. 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 you would not be able 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.

585. 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.

586. 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.

587. Since more information is available with the MT202 COV "cover payment," do institutions have additional due diligence responsibilities?

Ordering institutions may consider screening payment against the sanctions lists of their jurisdiction, and possibly, against sanctions lists relevant to the entire payment chain of the payment instruction.

Intermediary institutions do not have additional responsibilities; however, they may experience an increased volume of potential hits from suspicious activity monitoring and sanctions screening due to the increase in available information on the underlying parties.

588. 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.

589. 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

590. 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.

591. 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.

592. 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.

593. 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

594. 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

595. 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.

596. 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.

597. 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.

598. 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.

599. 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.

600. 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

601. 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

602. 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

603. 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.

604. 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.

605. 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.

606. 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.

607. 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.

608. 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.

609. 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.

610. How much has been blocked/rejected?

Based on the 2006 Terrorist Assets Report issued by OFAC, the United States has blocked $309.5 million in terrorist-related assets within the United States and $600,000 in foreign branches of U.S. institutions. An additional $102 million in unblocked funds also has been identified by OFAC as related to terrorism.

611. 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.

612. 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

613. 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.

614. 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.

615. 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.

616. 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.

617. 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.

618. 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

619. 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.

620. 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.

621. What does the term "date of detection" mean for OFAC purposes?

The term "date of detection" is the date of the blocked/rejected transaction.

622. 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.

623. 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.

624. 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.

625. 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).

626. 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

627. 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.

628. 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.

629. 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."

630. 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.

631. 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.

632. 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.

633. 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.

634. Are specific licenses transferable?

In general, specific licenses are not transferable.

635. 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.

636. 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.

637. 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.

638. 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).

639. 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.

640. Does BIS issue any lists similar to OFAC's SDN list?

Yes. BIS publishes the Denied Persons List (DPL), which includes individuals who/entities that have been denied export privileges.

641. Who is required to screen against the BIS DPL?

Exporters are required to screen against the BIS DPL. 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.

642. Are financial institutions required to screen against the BIS DPL?

No. It is the responsibility of the exporter to ensure that it is not transacting with an individual or entity listed on the DPL; 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.

643. What action must institutions take if a positive "hit" is identified on the BIS DPL?

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).

644. 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.

645. 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

646. 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.

647. 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.

648. 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.

649. 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

650. 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.

651. 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.

652. 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.

653. 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

654. 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

655. 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.

656. 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

657. 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])

658. 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.

659. 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.

660. 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 procedures 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

661. What are some examples of OFAC violations in nonfinancial service 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

662. What have been some of the more noteworthy recent OFAC settlements?

The more recent (2009-2010) 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.

Additional settlements are expected for other foreign banking organizations as a result of continuing OFAC investigations.

663. 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

664. 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 and the State Department, have independent prohibitions on transactions with certain individuals or entities beyond those included in OFAC Sanctions listings. 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.

665. 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.

666. 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

667. 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)

668. 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.

669. 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

670. 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

671. 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. For additional information on EDD for specific types of customers, please refer to the High Risk Customers section.

672. 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, may be lower risk than others.

673. 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.

674. 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. 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.

Updating Customer Due Diligence and Enhanced Due Diligence

675. 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.

Beneficial Owners

676. 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.

677. 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 Guidance on Obtaining and Retaining Beneficial Ownership Information, issued March 5, 2010, does not contain specific percentages, but instead looks to the level of control over or entitlement to the account.

678. 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.

679. 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 and purpose of funds.

680. What are a financial institution's obligations with respect to identifying beneficial ownership?

Leading industry practice, the Financial Action Task Force's (FATF) Recommendation 5 – Customer Due Diligence and other regulatory guidance dictate that financial institutions develop and maintain Customer Due Diligence (CDD) procedures reasonably designed to identify and verify the identity of beneficial owners.

For some financial institutions in the United States, the expectation that they have an obligation to identify and verify the identity of beneficial owners only became clear in March 2010, when the U.S. bank regulators, the Securities and Exchange Commission (SEC) and the Commodities Futures Trading Commission (CFTC) joined FinCEN in the Joint Release titled "Guidance on Obtaining and Retaining Beneficial Ownership Information." The Guidance states the following:

- Heightened risks can arise with respect to beneficial owners of an account because nominal account holders can enable individuals and business entities to conceal the identity of the real owner of assets or property derived from or associated with criminal activity.
- Identifying the beneficial owner(s) of some legal entities may be challenging, but such identification may be important in detecting suspicious activity and providing useful information to law enforcement.
- Financial institution should establish and maintain customer due diligence procedures reasonably designed to identify and verify the identity of beneficial owners of an account, as appropriate, based on the institution's evaluation of risk pertaining to an account. Accounts with heightened risk should have enhanced due diligence, which may include steps, in accordance with the risk level, to identify and verify beneficial owners (e.g., trusts, corporate entities, shell entities and private investment companies).
- The establishment of due diligence requirements for beneficial owners in the areas of private banking and foreign correspondent accounts is required.

681. 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).

682. 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.

683. 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 enterprisewide 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.

684. 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?
- In what jurisdiction is it established and why?
- 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?

685. 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:

- **Joint Guidance on Obtaining and Retaining Beneficial Ownership Information** by the Financial Crimes Enforcement Network (FinCEN)
- **Advisory – Potential Money Laundering Risks Related to Shell Companies** by FinCEN
- **FAQs on Beneficial Ownership** by the Wolfsberg Group
- **FAQs on Intermediaries** by the Wolfsberg Group
- **The Misuse of Corporate Vehicles, Including Trust and Company Service Providers** by the Financial Action Task Force (FATF)
- **Behind the Corporate Veil – Using Corporate Entities for Illicit Purposes** by the Organisation for Economic Co-operation and Development (OECD)
- **Identification of Ultimate Beneficiary Ownership and Control of a Cross-Border Investor** by the Organisation for Economic Co-operation and Development (OECD)
- **Principles on Client Identification and Beneficial Ownership for the Securities Industry** by the International Organization of Securities Commissions (IOSCO)

Know Your Employee

686. 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 system for potentially suspicious activity will help mitigate the risk of a financial institution being used for money laundering or terrorist financing.

687. 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.

688. What additional risks do employees of the financial institution pose?

CDD and EDD standards should be applied to all employees of a financial institution, regardless of status or position within the financial institution.

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).

Know Your Third Parties

689. 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 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 card program managers.
- **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) may not identify and manage AML risks appropriately.
- **Agents** of money services businesses (MSBs) may not appropriately manage AML risk and may expose a MSB to reputational risk even where it may not be legally responsible.
- **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.

690. 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
- 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)
- 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 and Agents.

691. 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.

692. 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.

693. 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.

694. Should third-party service providers be included in the independent testing requirement of an AML program?

Third-party service providers that qualify under the CIP rule do not 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.

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:

- Business line risk assessments
- Customer risk assessments
- Office of Foreign Assets Control (OFAC) risk assessments

695. 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.

696. 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.

697. 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.

698. 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.

699. 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

700. 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.

701. 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.

702. 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.

703. 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.

704. 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).

705. 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** 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** by the Financial Crimes Enforcement Network (FinCEN)
- **Guidance on a Risk-Based Approach for Managing Money Laundering Risks** by the Wolfsberg Group
- **Money Laundering and Terrorist Financing Risk Assessment Strategies** by FATF
- **Risk-Based Approach for Casinos** by FATF
- **Risk-Based Approach Guidance for Legal Professionals** by FATF
- **Risk-Based Approach for the Life Insurance Sector** by FATF
- **RBA Guidance for Trust and Companies Service Providers (TCSPs)** by FATF
- **RBA Guidance for Real Estate Agents** by FATF
- **RBA Guidance for Accountants** by FATF
- **High-Level Principles and Procedures for Dealers in Precious Metals and Dealers in Precious Stones** by FATF
- **Guidance for Money Services Businesses – Risk-Based Approach** by FATF
- **Risk Matrix for Financial Institutions** by the Office of Foreign Assets Control (OFAC)
- **Risk Matrix for the Securities Sector** by OFAC
- **Risk Matrix for the Charitable Sector** by OFAC

Business Line Risk Assessment

706. 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.

707. 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).

708. 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.

709. 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.

710. 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.

711. 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).

712. 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.

713. 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.

714. 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

715. 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.

716. 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.

717. 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.

718. 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.

719. 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.

720. 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.

721. 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).

722. 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.

723. 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.

724. 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.

725. 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.

726. 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.

727. 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

728. 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

729. 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 noncooperative by the Financial Action Task Force (FATF)

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.

730. 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)

731. 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)

732. 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.

733. 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.

734. 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.

735. 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.

736. 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.

737. 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.

738. 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.

739. 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

740. 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.

741. 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.

742. 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.

743. 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.

744. 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

745. 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.

746. 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.

747. 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.

748. 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

749. 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.

750. 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.

751. 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.

752. 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.

753. 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."

754. 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)

755. 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

756. 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.

757. 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.

758. 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.

759. 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.

760. 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).

761. 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.

762. What guidance has been issued on professional service providers?

The following key guidance has been issued on professional service providers:

- **Professional Service Providers – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Guardians at the Gate: The Gatekeeper Initiative and the Risk-Based Approach for Transactional Lawyers** by the American Bar Association (ABA)
- **Forty Recommendations and Nine Special Recommendations on "Designated Nonfinancial Businesses and Professions (DNFBP)"** by the Financial Action Task Force (FATF)
- **RBA Guidance for Trust and Companies Service Providers (TCSPs)** by FATF
- **RBA Guidance for Real Estate Agents** by FATF
- **RBA Guidance for Accountants** by FATF
- **Risk-Based Approach Guidance for Legal Professionals** by FATF

- **Wolfsberg FAQs on Intermediaries** by the Wolfsberg Group
- **OFAC Regulations for the Corporate Registration Industry** by the Office of Foreign Assets Control (OFAC)

Trust and Asset Management Services

763. 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)

764. 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) and the Office of Thrift Supervision (OTS) use the broader term "fiduciary capacity" instead of "trust."

765. 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."

766. 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

767. 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."

768. 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.

769. 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])

770. Is there a legitimate purpose for utilizing trust and asset management services?

The legitimate reasons for utilizing these services are often the same features exploited by criminals:

- Asset protection
- Estate planning
- Privacy and confidentiality
- Reduction of tax liability

771. 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

772. 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.

773. Should other parties to the trust beyond the accountholder be subject to the CIP rule?

Although not 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. For further guidance on identifying ultimate beneficial owners, please refer to the Beneficial Owners section.

774. Since beneficiaries of trusts are not 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.

775. 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 section. For further guidance on professional service providers, please refer to the Professional Service Providers section.

776. 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** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Forty Recommendations and Nine Special Recommendations on "Designated Nonfinancial Businesses and Professions (DNFBP)"** by the Financial Action Task Force (FATF)
- **RBA Guidance for Trust and Companies Service Providers (TCSPs)** by FATF

Deposit Broker

777. 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.

778. 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.

779. 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

780. 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 "subaccountholder" does not require verification.

781. 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

782. 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.

783. 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

784. 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

785. 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

786. 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).

787. 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 who have private banking customers.

788. What guidance has been issued on private banking?

The following are examples of key guidance that has been issued on private banking:

- **Private Banking - Overview** 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** by the Wolfsberg Group
- **Wolfsberg FAQs on Beneficial Ownership** by the Wolfsberg Group
- **Private Banking and Money Laundering: A Case Study of Opportunities and Vulnerabilities** 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

789. 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.

790. 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.

791. 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.

792. 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.

793. 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.

794. 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.

795. 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.

796. 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.

797. 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.

798. 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).

799. 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.

800. 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.

801. How can a multinational financial institution manage its multicountry 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.

802. 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.

803. 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 who have PEPs as customers.

804. 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** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Guidance to Financial Institutions on Filing Suspicious Activity Reports Regarding the Proceeds of Foreign Corruption** by the FinCEN
- **Wolfsberg FAQs on Politically Exposed Persons** by the Wolfsberg Group
- **Guidance on Enhanced Scrutiny for Transactions That May Involve the Proceeds of Foreign Official Corruption** 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
- **Guidance to Financial Institutions on Filing Suspicious Activity Reports Regarding the Proceeds of Foreign Corruption** by the Financial Crimes and Enforcement Network (FinCEN)
- **Stolen Asset Recovery: Politically Exposed Persons, A Policy Paper on Strengthening Preventive Measures** by the World Bank
- **Stolen Asset Recovery: Guide on Non-Conviction Based (NCB) Asset Forfeiture** by the World Bank

For additional guidance on PEPs and required due diligence, please refer to the Politically Exposed Persons section.

Foreign Embassy and Consulates

805. 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).

806. 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.

807. 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

808. 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)

809. 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).

810. What guidance has been issued on foreign embassies and consulates?

In June 2004, the U.S. bank regulators and FinCEN issued an advisory related to accepting accounts from foreign governments, foreign embassies and foreign political figures, collectively referred to as “embassy banking.” This release highlighted some of the considerations that should be addressed by financial institutions that offer embassy banking, including ensuring embassy banking customers are aware of applicable U.S. AML laws and regulations.

In addition, the **Embassy and Foreign Consulate Accounts – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC) addresses this topic.

Business Entities: Shell Companies, Private Investment Companies

811. 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.

812. 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.

813. Is there a legitimate purpose for establishing these types of business entities?

The legitimate reasons for establishing these business types are often the same features exploited by criminals:

- 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

814. 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.

815. 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.

816. 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.

817. How is the term “bearer share ownership” defined?

Bearer share ownership is based on physical possession of the stock certificates.

818. 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).

819. 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.

820. 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** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Potential Money Laundering Risks Related to Shell Companies** by the Financial Crimes Enforcement Network (FinCEN)
- **Company Formations – Minimal Ownership Information Is Collected and Available** by the U.S. Government Accountability Office (GAO)
- **The Misuse of Corporate Vehicles, Including Trust and Company Service Providers** by the Financial Action Task Force (FATF)
- **Wolfsberg FAQs on Beneficial Ownership** by the Wolfsberg Group
- **Wolfsberg FAQs on Intermediaries** by the Wolfsberg Group
- U.S. Senate Hearing: **“Refer to Failure to Identify Company Owners Impedes Law Enforcement”**
- U.S. Senate Hearing: **“Tax Haven Abuses: The Enablers, the Tools and Secrecy”**
- U.S. Senate Hearing: **“Failure to Identify Company Owners Impedes Law Enforcement”**
- **OFAC Regulations for the Corporate Registration Industry** by the Office of Foreign Assets Control (OFAC)

Correspondent Banking

821. 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.

822. 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.

823. 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).

824. 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 who 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) 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 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

For additional guidance on CISADA, please refer to the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA) section.

825. 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)** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking** by The New York Clearing House Payments Co., LLC
- **Wolfsberg AML Principles for Correspondent Banking** by the Wolfsberg Group
- **Wolfsberg Frequently Asked Questions on Correspondent Banking** by the Wolfsberg Group
- **The Wolfsberg Group and the Clearing House Association: Cover Payments: Some Practical Questions Regarding the Implementation of the New Payments** by the Wolfsberg Group
- **Correspondent Account KYC Toolkit: A Guide to Common Documentation Requirements** 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** 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** by FinCEN
- **Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries** by FinCEN
- **Application of the Regulations regarding Special Due Diligence Programs for Certain Foreign Accounts to NSCC Fund/SERV Accounts** by FinCEN
- **Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-border Wire Transfers** 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**

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

826. 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
- 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.

827. 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

828. 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.

Charitable Organizations and Nongovernmental Organizations

829. 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).

830. 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.

831. 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).

832. 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.

833. 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.

834. 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** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities** by the U.S. Department of the Treasury
- **Office of Foreign Assets Control Regulations for Non-Governmental Organizations** by the Office of Foreign Assets Control (OFAC)
- **Risk Matrix for the Charitable Sector** by OFAC
- **Frequently Asked Questions on NGO Registration Numbers** by OFAC
- **FATF Interpretive Note to Special Recommendation Eight: Non-Profit Organizations** by FATF
- **FATF International Best Practices for Combating the Abuse of Non-Profit Organizations** by FATF

Third-Party Payment Processors

835. 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 clearinghouse (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.

836. 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.

837. 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.

838. 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.

839. 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.

840. 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.

841. 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 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.

842. What is an independent sales organization?

The FDIC defines an independent sales organization (ISO) as an "outside company contracted to procure new merchant relationships."

843. 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

844. 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 accountholder 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.

845. 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 (UIGE) and Prohibition on Funding of Unlawful Internet Gambling (PFUIG) Regulation. For further guidance, please refer to the Unlawful Internet Gambling Enforcement Act and Prohibition on Funding of Unlawful Internet Gambling Regulation section.

846. 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, seller or redeemer of money orders
- Issuer, seller or redeemer of traveler's checks
- Check casher
- Currency dealer or exchanger
- Issuer, seller or redeemer of stored-value cards
- 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 whom 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.

847. 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.

848. 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 comply with the Unlawful Internet Gambling Enforcement Act (UIGEA) and Prohibition on Funding of Unlawful Internet Gambling (PFUIG) Regulation. For further guidance, please refer to the Unlawful Internet Gambling Enforcement Act and Prohibition on Funding of Unlawful Internet Gambling Regulation section.

849. What guidance has been issued on third-party payment processors?

The following are examples of guidance that has been issued on third-party payment processors:

- **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)
- **Retail Payment Systems** and **Wholesale Payment Systems Booklet** within the FFIEC Information Technology Examination Handbook by the FFIEC
- **Third-Party Senders and the ACH Network: An Implementation Guide** by The Electronic Payments Association (NACHA) (formerly National Automated Clearing House Association)
- **Bank Use of Foreign-Based Third-Party Service Providers** by the Office of the Comptroller of the Currency (OCC)
- **Third-Party Relationships: Risk Management Principles** by the OCC
- **Guidance on Payment Processor Relationships** by the Federal Deposit Insurance Corporation (FDIC)
- **Guidance on Managing Third-Party Risk** by the FDIC

Privately Owned Automated Teller Machines (ATMs)

850. 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.

851. 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.

852. 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.

853. 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.

854. 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.

855. 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.

856. 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

857. 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, stored value, 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.

858. 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 who 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

859. What does the term "currency" mean?

"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.

860. 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.

861. 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.

862. 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

863. 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.

864. 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.

865. 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.

866. 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.

867. 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

868. 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

869. 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.

870. 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.

871. 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.

872. 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.

873. 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.

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

No, they are not, as 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.

875. 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.

876. 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.

877. 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.

878. 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.** by the Financial Crimes Enforcement Network (FinCEN)
- **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

879. 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.

880. 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.

881. 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.

882. 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.

Automated Clearing House Transactions

883. 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

884. Are ACH transactions limited to domestic payments?

No. ACH transactions can be processed for both domestic and international (cross-border) payments.

885. 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.

886. 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.

887. 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/.

888. 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.

889. 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.

890. 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."

891. 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 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 Prohibition on Funding of Unlawful Internet Gambling (PFUIG) Regulation. For further guidance, please refer to the Unlawful Internet Gambling Enforcement Act and Prohibition on Funding of Unlawful Internet Gambling Regulation 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.

892. 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.

893. 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.

894. 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** within the FFIEC BSA/AML Examination Manual by the FFIEC
- **Automated Clearinghouse Activities - Risk Management Guidance** by the Office of the Comptroller of the Currency (OCC)
- **International ACH Transaction (IAT) Frequently Asked Questions** by the Federal Reserve Financial Services
- **FedGlobal® Frequently Asked Questions** by the Federal Reserve Financial Services
- **Guidance to National Automated Clearing House Association (NACHA) on Domestic and Cross-border ACH Transactions** by OFAC
- **Update on OFAC Requirements for Gateway Operators' Processing of Inbound IAT Debits** by NACHA
- **National Automated Clearinghouse Operating Rules** by NACHA
- **Comptroller's Handbook: Merchant Processing** by the OCC
- **FFIEC IT Examination Handbook on Retail Payment Systems** by the FFIEC

Monetary Instruments

895. 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.

896. 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).

897. 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.

  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.

898. 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.

U.S. Dollar Drafts

899. 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.

900. 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.

901. 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.

902. 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

903. 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.

904. 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.

905. 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.

906. 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.

907. 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.

908. 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

909. 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.

910. 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.

911. 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.

912. 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.

913. 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.

914. 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.

- **Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA)**: Recently, the United States imposed sanctions on Iran under the Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA) that may restrict or prohibit the opening or maintenance of payable through accounts (PTAs) 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

  For additional guidance on CISADA, please refer to the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA) section.

Concentration Accounts

915. 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.

916. 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.

917. 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

918. 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

919. 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.

920. 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.

921. 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 (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

922. 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

923. 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.

924. 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.

925. 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.

926. 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

927. 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.

928. 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.

929. 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

930. 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.

931. 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.

932. Can cash be deposited through RDC?

Yes. RDC also may include the electronic capture of deposit information comprised of cash through remote safekeeping arrangements at customer locations or through other intermediaries.

933. 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.

934. 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

935. 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.

936. How should RDC activities be monitored for potentially suspicious activity?

Financial institutions should examine RDC transactions 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 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

For additional guidance on red flags, please refer to the sections: Suspicious Activity Red Flags and Pouch Activity and Remote Deposit Capture.

937. 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.

938. 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** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Risk Management of Remote Deposit Capture** by the FFIEC
- **Interagency Guidance on Authentication in an Internet Banking Environment** by the FFIEC
- **"Remote Deposit Capture"** within **Retail Payment System Overview** within the FFIEC IT Examination Handbook by the FFIEC
- **E-Banking Booklet** by the FFIEC
- **Risk Management for Electronic Banking and Electronic Money Activities** by the Bank for International Settlements (BIS)
- **Security of Electronic Money** by the BIS
- **ML and TF Vulnerabilities of Commercial Websites and Internet Banking Systems** by the Financial Action Task Force (FATF)
- **Report on New Payment Methods** by FATF
- **Money Laundering in Cyberspace** by the World Bank (WB)
- **Mobile Phone Financial Services** Paper by the WB

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**
    - **Cross-Border Outsourcing and Risk Management for Banks, Published in Capco Institute Journal of Financial Transformation, 8th edition**
    - **Internet Banking: Developments and Prospects**
    - **Report to the Congress on Review of Regulations Affecting Online Delivery of Financial Products and Services**
    - **Internet Banking in the U.S., Published in Capco Journal of Financial Transformation, 2nd edition**
    - **Internet Banking: Developments and Prospects, Economics Working Paper**
    - **Who Offers Internet Banking?, Quarterly Journal Vol. 19, No. 2**
    - **Banking Over the Internet, Quarterly Journal Vol. 17, No. 4**
    - **Technological Innovation in Banking and Payments, Quarterly Journal Vol. 7, No. 3**
    - **The Report of the Consumer Electronic Payments Task Force**
    - **Toward Electronic Money and Banking: The Role of Government Conference Paper – "An Introduction to Electronic Money Issues"**

Prepaid Access, Stored-Value and E-Cash

939. What do the terms "prepaid access," "stored value" and "e-cash" mean?

"Prepaid access" includes an electronic device or vehicle, such as a card, plate, code, number, electronic serial number, mobile identification number, personal identification number, or other instrument that provides a portal to funds or the value of funds that have been paid in advance and can be retrievable and transferable at some point in the future.

Prepaid access products encompass most of the emerging growth products, such as open-loop general purpose prepaid cards, certain closed-loop cards, mobile phone access, fob or barcode access. Prepaid products also include prepaid payroll as well as government benefit products.

The term "stored value" is a type of prepaid access.

"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.

FinCEN's recent proposal, "Amendment to the Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Prepaid Access" (issued in June 2010 and further explained below), uses the term "prepaid access" to include a broader range of products, and proposes to use "prepaid access" in lieu of "stored value" for purposes of the regulations.

940. What is the difference between electronic banking and e-cash?

Electronic banking generally refers to the use of the Internet to conduct traditional banking transactions; prepaid access and e-cash refer to products and services that can be accessed through multiple methods, including but not limited to electronic banking.

941. How is the term “stored-value card” defined?

Stored-value cards, also 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. However, as noted above, FinCEN has proposed to change and broaden the definition of “prepaid access.”

942. What are the heightened money laundering and terrorist financing risks of prepaid access and e-wallet products?

Transactions may involve funds that have been transferred to or from an unknown party. Customers may be able to avoid certain border disclosure requirements currently in effect. Where the accounts are not personally identifiable, specific cardholder activity may be difficult to identify. However, as most prepaid access products are issued by either a bank or a licensed money transmitter, both of which are subject to extensive Bank Secrecy Act and USA PATRIOT Act recordkeeping and reporting requirements, issuers and others, such as program managers, are subject to most of the requirements applicable to a bank checking account. Moreover, 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 stored-value 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

943. Do all types of stored-value products pose the same degree of risk?

No. FinCEN has issued guidance to the effect that closed-universe cards (cards that may be used only at a single merchant) and certain mall cards do not pose as high a risk as open-loop cards, although it is considering whether to change that guidance and impose standard BSA recordkeeping and reporting requirements on closed-loop cards that allow funds or value to be transmitted internationally, or allow transfers between or among users of prepaid access within a prepaid program such as person to person transfers.

944. What is the difference between a closed-loop and open-loop system?

Closed-loop 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 products may be used at multiple merchants, such as a prepaid card that contains a Visa product and can be used at any merchant that accepts Visa debit cards. Open-loop cards may also come in fixed or reloadable amounts.

945. Can a closed-loop stored-value product be used to launder illicit funds?

As with any type of payment product or service, it is possible for a closed-loop product to be misused. Law enforcement has identified instances where drug dealers used illicit funds to purchase closed-loop gift cards with illicit funds, and the cards were then used to purchase retail items. However, there have been very few incidents of reported 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.

946. 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.
- Obtain identifying information from the purchaser or recipient for higher-risk products.

947. What type of due diligence can an issuer of prepaid access products collect on third-party agents that sell or redeem such products?

Following are examples of the types of due diligence that may be collected on third-party agents, depending on the risks posed by both the products offered and the agent 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 SDN and Sanctions lists
- Periodic audits of their compliance, which may include an on-site visit
- AML training review
- AML Compliance Program review
    - CIP of purchasers
    - BSA/AML policy and procedures
    - Independent assessments of program
- Acquisition of AML audits/reviews of company-prepared self-assessments

948. Is an entity that is engaged in the sale of prepaid access/stored-value products considered a MSB?

Yes. If an entity sells more than $1,000 in stored-value products to any person in any one day, then it is considered a MSB. However, if the prepaid access product enables money transmittals, then it is a MSB, and there is no dollar threshold.

949. With which key AML requirements are MSBs that only issue, sell or redeem covered prepaid access/stored-value products required to comply?

Regulations require an issuer, seller or redeemer of stored-value products to file CTRs and to establish a written AML program, including policies, procedures and internal controls. However, the current regulations exempt a stored-value MSB (where that is the only money services business activity the entity conducts) from filing SARs or registering as a MSB with FinCEN.

It is important to recognize, however, that the issuer of the prepaid access/stored-value product (unless exempt as closed loop) will be either a bank or licensed MSB, which is subject to SAR filing and MSB registration requirements (banks are exempted from the MSB filing requirements).

FinCEN has proposed to impose both SAR filing and MSB registration requirements on many parties involved with prepaid access, although at the time of the printing of this document it is unknown whether such proposal will become final rules.

For additional guidance on the AML requirements of MSBs, please refer to the Money Services Businesses section.

950. Do stored-value products meet the definition of monetary instruments for reporting requirement purposes?

No. Stored-value products do not currently meet the definition of monetary instruments, so sellers are not required to record the information of the purchaser. FinCEN is considering whether to include prepaid access products as monetary instruments, at least for the purpose of cross-border transactions. However, most issuers of general purpose reloadable prepaid access cards require the capture and retention of the name and address of the purchaser, to help them identify potentially suspicious activity.

Expanding the Definition of "Stored Value"

951. Are there any plans to modify and expand the regulatory definition of "stored value"?

Yes. In June 2010, FinCEN issued a notice of proposed rulemaking addressing definitions and regulations relating to prepaid access that would cover prepaid devices such as stored-value cards, electronic serial numbers, key fobs and other mechanisms that provide a portal to funds that have been prepaid and are retrievable and transferable.

Key features of the proposal include:

- Renaming "stored value" as "prepaid access"
- Replacing the terms "issuer" and "redeemer" of stored value with the terms "provider" and "seller"
- Expanding AML requirements to include providers and sellers of prepaid access (e.g., registration requirements, suspicious activity reporting, customer information recordkeeping and new transactional recordkeeping)
- Exemptions for lower-risk prepaid access products

952. To what types of companies does the notice of proposed rulemaking apply?

The notice for proposed rulemaking applies only to nonbanks, although bank-issued card programs will be impacted as the proposal would significantly increase the recordkeeping and reporting requirements on other parties involved in their product offerings. The proposed rule does not apply to entities regulated by the SEC or CFTC.

953. Why does the proposed rule rename "stored value" as "prepaid access"?

The proposed rule seeks to rename "stored value" as "prepaid access" because the technology used in the stored-value industry has changed. FinCEN wants the proposed rule to encompass all emerging payment methods rather than just payment methods in which "value" is stored directly on the card. Advancements in the industry allow for other payment methods such as cards with magnetic strips, key fobs, mobile phones, etc.

954. What is the purpose of the proposed rule?

The purpose of the proposed rule is to bring the regulatory requirements for nonbank entities involved in stored-value products in line with other financial institutions. In addition, the proposed rule would centralize the primary BSA reporting obligations with the prepaid provider since it may be the party with the greatest access and/or the ability to gain access to relevant information to comply with BSA reporting requirements. Sellers of prepaid access products would continue to have BSA reporting obligations; and the proposed regulations would greatly increase their obligations to capture and retain information.

955. How does the proposed rule define a "provider" of prepaid access products?

The proposed rule defines a provider as the person with principal oversight and control over one or more prepaid programs. Which person exercises "principal oversight and control" is a matter of facts and circumstances. FinCEN believes the "provider of prepaid access" 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.

956. How does the proposed rule define a "seller" of prepaid access?

The proposed rule defines a "seller" of prepaid access to mean any person who receives funds or the value of funds in exchange for providing prepaid access as part of a prepaid program directly to the person who provided the funds or value, or to a third party as directed by that person.

957. How is the term "provider" of prepaid access products defined in the proposed rule?

The proposed rule identifies the following activities as strong indicators that an entity is acting as a "provider":

- The party in whose name the prepaid program is marketed to the purchasing public
- The party whom a "reasonable person" would identify as the principal entity in a transaction chain – the principal decision-maker
- The party to whom the issuing bank views as its principal representative in protecting its network relationship and its brand integrity

- The party who determines distribution methods and sales strategies
- The party whose expertise in the prepaid environment is recognized by the others, particularly by the issuing bank, as instrumental in bringing together the most appropriate parties for the delivery of a successful program

In addition, the proposed rule lists the following as factors used in determining who the "provider" of prepaid access is:

- Organizing the prepaid program
- Setting the terms and conditions and determining that the terms have not been exceeded
- Determining the other businesses that will participate in the transaction chain, which may include the issuing bank, the payment processor or the distributor
- Controlling or directing the appropriate party to initiate, freeze or terminate prepaid access
- Engaging in activity that demonstrates control and oversight of transactions

958. Are there exemptions to "provider" of prepaid access products?

Yes. Banks and financial institutions regulated by the SEC and the CFTC are exempted from the definition of "provider" by the proposed rule.

959. With which AML requirements will a provider of prepaid access be required to comply?

The proposed rule expands the AML requirements of "provider" of prepaid access products to include the following:

- Registration as a MSB with FinCEN
- Development of an AML program that should include:
    - Internal policies and procedures for identifying unusual activity and submitting SARs
    - Internal policies and procedures for identifying transactions that meet CTR and other recordkeeping and reporting requirements
- Retention of transaction records that may include:
    - 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
- Development of training programs for third parties used to support prepaid products so the third-party provider can refer potentially unusual activity to the provider of prepaid access products

960. With which AML requirements will a seller of prepaid access be required to comply?

The proposed rule expands the AML requirements of "seller" of prepaid access products to include the following:

- The maintenance of an effective AML program
- SAR reporting
- Recordkeeping of customer identifying information and transactional data
- Customer identification and verification, which may include:
    - Name
    - Date of birth
    - Address
    - Identification number

961. Which prepaid products are exempted from the proposed rule since they are lower risk?

The following products are exempted from AML requirements required by the proposed rule because they are considered lower risk:

- The payment of benefits, incentives, wages or salaries through payroll cards or other such electronic devices for similar purposes
- Payment of government benefits such as unemployment, child support and disaster assistance through electronic devices
- Disbursement of reimbursement funds from pre-tax flexible spending accounts for healthcare and dependent care expenses
- Closed-loop products that do not permit funds or value to be transmitted internationally or allow transfers between or among users of prepaid access within a prepaid program such as person-to-person transfers
- Provision of prepaid access to funds subject to limits that include a maximum value as indicated below, where such maximum value is clearly visible on the prepaid access product:
    - At the point of initial load, the load limit cannot exceed $1,000.
    - At any point in the lifecycle of the prepaid access, no more than $1,000 in total maximum value may be accessed.
    - On any given day, no more than $1,000 can be withdrawn with the use of the prepaid access.
    - However, it is important to note that the exemption for these cards does not apply if the cards permit funds or value to be transmitted internationally, or allow transfers between or among users of prepaid access within a prepaid program such as person-to-person transfers, or (unless it qualifies as closed-loop prepaid access) allow the ability to load monetary value from other nondepository sources onto prepaid access.

962. Are persons transporting or shipping stored-value 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)?

Not currently. Stored-value products do not meet the regulatory definition of currency or monetary instruments; therefore, a CMIR is not required. However, FinCEN is considering whether to expand the obligations for reporting of prepaid access products that are taken across borders. FinCEN has also proposed new cross-border recordkeeping requirements for many types of electronic funds transfers. For additional guidance on CMIRs, please refer to the Report of International Transportation of Currency or Monetary Instrument section.

963. What guidance has been issued on prepaid or stored-value products?

The following are examples of information and guidance that have been issued on stored value:

- **"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
- **Community Affairs Department – Analysis Paper, "Payroll Cards: An Innovative Product for Reaching the Unbanked and Underbanked"** 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** by the Financial Action Task Force (FATF)
- **Consumer Payment Choice: A Central Bank Perspective** by the Federal Reserve Bank of Boston
- **Prepaid Cards: Vulnerable to Money Laundering?** by the Federal Reserve Bank of Philadelphia
- **The Laws, Regulations, Guidelines, and Industry Practices That Protect Consumers Who Use Gift Cards** by the Federal Reserve Bank of Philadelphia

- **Emerging Risk Forum "Cash, Check, or Cell Phone?" Protecting Consumers in a Mobile Finance World** by the Federal Reserve Bank of Boston
- **New Technologies, New Risks? Innovation and Countering the Financing of Terrorism** by the World Bank (WB)
- **Survey of Developments in Electronic Money and Internet and Mobile Payments** by the Bank of International Settlements (BIS)
- **Recommended Practices for Anti-Money Laundering Compliance for U.S.-Based Prepaid Card Programs** by the Network Branded Prepaid Card Association (NBPCA)
- **Person-to-Person Electronic Funds Transfers: Recent Developments and Policy Issues** by the Federal Reserve of Boston
- **Risk Management of Remote Deposit Capture** by the Federal Deposit Insurance Corporation (FDIC**)**
- **Notice of Proposed Rulemaking: Amendment to the Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Prepaid Access** by the Financial Crimes Enforcement Network (FinCEN)
- **Report on New Payment Methods** by FATF
- **Understanding Risk Management in Emerging Retail Payments** 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)

Trade Finance Activities

964. 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).

965. 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.

966. 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.

967. 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.

968. 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."

969. 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.

970. 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.

971. 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.

972. What is the role of correspondent banking in trade finance transactions?

Financial institutions should ensure that collection and penalty procedures stipulated in contracts are enforceable in foreign countries in which business is conducted. Many financial institutions rely on the local expertise 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.

973. What are "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 more than 130 countries. Financial institutions may consider conducting enhanced due diligence on parties and transactions associated with free trade zones. The Financial Action Task Force (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.

974. 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 Defense Department 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.

975. 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)).

976. 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.

977. 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.

978. 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** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Trade-Based Money Laundering** by the Financial Action Task Force (FATF)
- **Money Laundering Vulnerabilities of Free Trade Zones** by FATF
- **Best Practices Paper on Trade-Based Money Laundering** by FATF
- **The Wolfsberg Trade Finance Principles** by the Wolfsberg Group
- **Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering** by the Financial Crime Enforcement Network (FinCEN)
- **Application of a Section 311 Special Measure to Payments under a Stand-By Letter of Credit** by FinCEN
- **Black Market Peso Exchange Update** by FinCEN
- **Guidance to Financial Institutions on the Repatriation of Currency Smuggled into Mexico from the United States** by FinCEN
- **Comptroller's Handbook: Trade Finance** by the Office of the Comptroller of Currency (OCC)
- **Comptroller's Handbook: Banker's Acceptances** by the OCC

The following key OFAC guidance has been issued for importers and exporters:

- **Foreign Assets Control Regulations for Exporters & Importers** by OFAC
- **Frequently Asked Questions from Importers and Exporters** by OFAC
- **Frequently Asked Questions on Licensing** by OFAC
- **Ask the TIC: Guide to Export Controls** by the Trade Information Center (TIC)
- **Letter of Credit Update: OFAC Regulations: The Countries Aren't Enough!** by OFAC
- **Notice to Mariners** by the National Geospatial-Intelligence Agency (NGA)
- **Part 1 and Part 2 - Export Controls Compliance: Don't Neglect OFAC** 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

979. 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

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.

980. 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

981. 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)
- 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.

982. 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

983. 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 and Professional Service Providers.

984. What AML guidance has been issued on lending activities?

The following key guidance has been issued on lending activities:

- **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** by the Office of Foreign Assets Control (OFAC)
- **RBA Guidance for Real Estate Agents** by the Financial Action Task Force (FATF)
- **Money Laundering and Terrorist Financing Through the Real Estate Sector** by FATF
- **Money Laundering in the Commercial Real Estate Industry: An Assessment Based Upon Suspicious Activity Report Filing Analysis** by the Financial Crimes Enforcement Network (FinCEN)

Nondeposit Investment Products

985. 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.

986. 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

987. 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).

988. 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.

989. 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.

990. 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.

991. 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

992. 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

993. 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.

994. 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.

995. 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.

996. 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** by the FFIEC
- **Insurance Industry Suspicious Activity Reporting: An Assessment of Suspicious Activity Report Filings** by the Financial Crimes Enforcement Network (FinCEN)
- **Frequently Asked Questions from the Insurance Industry** by the Office of Foreign Assets Control (OFAC)
- **Risk-Based Approach for the Life Insurance Sector** by the Financial Action Task Force (FATF)
- **Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism** by the International Association of Insurance Supervisors (IAIS)
- **Anti-Money Laundering Guidance Notes** by the IAIS

Administration of Customer Risk Assessment

997. 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).

998. 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

999. 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 personnel. Changes to the score should be clearly documented. Some financial institutions limit downgrading of risk scores to customers who have maintained relationships with the financial institution for a minimum of one year.

1000. How can a financial institution validate 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.

1001. 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

1002. 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

1003. 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.

1004. 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.

1005. How often should an OFAC risk assessment be conducted?

At a minimum, the OFAC risk assessment should be conducted annually.

1006. 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).

1007. 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.

1008. 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

1009. 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)

1010. 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.

1011. 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

1012. 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.

1013. 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 is 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).

1014. On what level should transactions be monitored (e.g., account, customer)?

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.

1015. 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.

1016. 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. As mentioned earlier, the financial institution should review the profile created using historical data with the institution's expectations for the customer.

1017. 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 when 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.

1018. How is transaction monitoring conducted in institutions that do not have AML monitoring software?

Many institutions generate reports from various internal systems for other purposes. The review of these reports often can be combined with an institution's suspicious activity monitoring efforts. 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.

Roles and Responsibilities

1019. 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.

1020. 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.

1021. 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.

1022. When selecting personnel to staff the investigative unit, what skills should be required by the financial institution?

Investigations of unusual or potentially suspicious activity require a variety of skills, including the ability to identify patterns, spot anomalies, draw and support conclusions, and summarize findings in a logically organized report. As more financial institutions utilize automated transaction monitoring, many require computer skills, including advanced spreadsheet analysis.

Investigation Process

1023. 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).

1024. 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.

1025. 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.

1026. 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.

1027. How can a financial institution evaluate the effectiveness of its monitoring?

In line with the financial institution's board reporting requirements, the investigative unit should conduct analyses to determine, for each method the institution uses to generate alerts (e.g., transaction monitoring software, business unit referrals), the result of its investigations and SAR filings. This will help the institution (a) determine which rules/ parameters used by the automated transaction monitoring system should be modified to better identify unusual or potentially suspicious activities, (b) determine if additional training should be given to business unit personnel to identify unusual or potentially suspicious activity, and (c) determine trends in customer activity.

1028. 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

1029. 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 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 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
- Transactions that involve higher-risk businesses
- 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)
- 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)
- Customer conducts multiple transactions several times in one day or over a short period of time (possibly using different tellers), indicating structuring
- Customer attempts to bribe or threaten an employee in order to circumvent reporting requirements
- Transactions involving senior political figures, both foreign and domestic
- 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
- Sudden high volume of unexplained activity
- 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

Currency Red Flags

- 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
- High volume of currency deposits and/or withdrawals inconsistent with the profile of the customer
- 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 Mexican 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
- Deposits by *casas de cambio* to their accounts at U.S. financial institutions that include third-party items (including sequentially numbered monetary instruments)
- 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

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
- 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
- Use of one or more monetary instruments to purchase another monetary instrument(s)
- 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
- Customer purchases multiple money orders with no apparent purpose

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

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
- Intentional circumvention of approval authorities or reporting limits by splitting transactions
- A large deposit followed by numerous, smaller wire transactions
- 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
- Large number of wire transfers to/from unrelated third parties
- 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
- 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
- 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

Trade Finance Red Flags

- Goods/services involved in transaction do not match the customer’s stated line of business
- Irregular or inflated pricing of goods
- Transactions involving high-risk goods (e.g., weapons, nuclear equipment, chemicals)
- Goods are transshipped through one or more jurisdictions for no apparent economic reason

- Missing information on trade documentation (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
- Documentary fraud
- Changes in payment instructions
- Numerous inquiries by the beneficiary regarding the credit's issuance; a sense of urgency and/or angry complaints displayed by the beneficiary
- Excessively amended letters of credit
- Presentations of letters of credit or documents where the financial institution has no record of the credit's existence
- Letters of credit opened by telex when the telex has not been tested with the receiving bank
- Letters of credit involving high-risk jurisdictions or obscure ports and/or locations that cannot be contacted by telephone or telex
- 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

- Large single-payment premiums for life and annuity policies
- Unusual methods of payment, particularly cash or cash equivalents
- Beneficiaries are unidentified or located in countries known for illegal activities
- Policy repayments inconsistent with the customer's source of funds and/or income
- Premium payments 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)

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 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 stored value/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

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

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)

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

AML TECHNOLOGY

Overview

1030. How can technology be used to support a financial institution's AML program?

Much has been written about the use of AML technology in a financial institution's transaction monitoring process. 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, 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

1031. Can one system support multiple aspects of an AML program?

A number of vendors have alliances with other vendors to offer an institution a wider range of services. For example, some vendors only offer AML transaction monitoring software; others may offer a combination of AML transaction monitoring and interdiction software when creating an alliance with a list provider (e.g., PEP, OFAC). Some vendors offer standard packages with the ability to add on additional features.

Since customer bases and levels of transaction activity vary across institutions, each institution needs to consider the standard software package that best meets its requirements, requiring minimal add-on services.

1032. What are the benefits of implementing AML software on an enterprisewide basis rather than on a local basis?

An increasing number of large financial institutions are selecting and implementing AML software on a global basis, as this can be cost-effective and can enhance efficiency and consistency throughout an organization.

1033. 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 enterprisewide 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?

1034. 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.

1035. 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).

1036. What are some challenges in selecting and implementing 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
- 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
- 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

Suspicious Transaction Monitoring and Suspicious Activity Report Filing Software

1037. 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 increasingly are encouraging financial institutions to adopt such software, and in some cases, have required the implementation of software under the terms of enforcement actions.

1038. 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.

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.

1039. 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)?

1040. 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.

1041. 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.

The reasons for changes made to the system parameters following the initial implementation should be well documented.

1042. 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

1043. 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. Management also should periodically review the filtering criteria and thresholds established to ensure that they are still effective.

1044. 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. Those charged with monitoring must be experienced and knowledgeable enough to interpret alerts. Additionally, 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 should be trained to identify unusual or potentially suspicious 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. Additionally, current events that may impact a financial institution's customer base need to be considered when monitoring transactions.

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.

1045. 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.

1046. 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.

Case Management Software

1047. 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.

1048. 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?

Large Currency Transaction Monitoring and Currency Transaction Report Filing Software

1049. 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.

1050. 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?

Customer Information Database and Customer Risk Assessment Software

1051. 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.

1052. 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)?
- 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?

1053. 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.

1054. 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?

Customer Verification Software

1055. 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.

1056. 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?

1057. 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

1058. 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.

1059. 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.

1060. 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.

1061. 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 this decision, 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)?

Interdiction Software

1062. 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).

1063. 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.

1064. 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.

1065. 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

1066. 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?

Training Software

1067. What types of training software are currently available?

Some of the most commonly used training solutions include Internet-, intranet- and computer-based training modules.

1068. 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?

NONBANK FINANCIAL INSTITUTIONS AND NONFINANCIAL BUSINESSES

Nonbank Financial Institutions

1069. 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
- Businesses engaged in vehicle sales, including automobile, airplane and boat sales
- Travel agencies
- Pawnbrokers
- Telegraph companies

For additional guidance on the above, please refer to the respective questions below.

1070. 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, other types of companies included under the definition of “financial institution” 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).

1071. 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. 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.

1072. 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 whose subsidiaries may be subject to AML regulations issued by multiple agencies have chosen to implement high-level, enterprisewide 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 industry.

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. Although this guidance has not been extended formally to AML programs generally, regulators expect banks to ensure adequate AML programs are implemented throughout their subsidiary organizations (whether or not those organizations are formally subject to AML requirements).

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).

1073. Are NBFIs required to comply with OFAC regulations?

Yes, assuming they are U.S. businesses. 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.

1074. What are the heightened money laundering and terrorist financing risks of NBFIs?

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 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 store and 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 to foreigners to funds held in domestic financial institutions
- Subjectivity 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

Money Services Businesses

Definition

1075. What is a money services business (MSB)?

Any organization offering one or more of the following services is classified as a MSB:

- Issuer, seller or redeemer of money orders
- Issuer, seller or redeemer of traveler's checks
- Check casher
- Currency dealer or exchanger
- Issuer, seller or redeemer of stored-value cards
- Money transmission (domestic or international)

Issuers and Redeemers of Monetary Instruments

1076. How is the term "issuer" defined for MSBs?

An issuer is the business that issues the money order, traveler's check or stored value. Usually, it is ultimately responsible for payment of money orders, traveler's checks or stored value as the drawer of such instruments.

1077. 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

1078. 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 requirements.

Currency Dealers or Exchangers

1079. What is a currency dealer or exchanger?

A currency dealer or exchanger is a "person who deals in or exchanges currency as a business," excluding a person who does not exchange currency in an amount greater than $1,000 in currency or monetary or other instruments for any person on any day in one or more transactions.

1080. 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.

Stored Value

1081. How is the term "stored value" defined?

Stored-value cards, also 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. However, as noted above, FinCEN has proposed to change and broaden the definition of "Prepaid Access."

For additional guidance on the proposed rule, please refer to the Prepaid Access, Stored-Value and E-Cash section.

Money Transmitters

1082. What is a money transmitter?

A money transmitter is any person who accepts currency or funds denominated in currency and transmits the currency or funds, or the value of the currency or funds, through a formal funds transfer system (e.g., by any means through 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; or an electronic funds transfer network or any person that is engaged as a business in the transfer of funds) or through an informal funds transfer system (e.g., hawala).

A business that engages in the above activity is a money transmitter whether or not it is licensed or required to be licensed. Money transmitters that provide money transmission services in any amount are subject to applicable AML requirements.

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.

1083. 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.

1084. 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.

1085. 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.

1086. 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 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.

1087. 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.

1088. Is a "foreign exchange dealer" included in the definition of a currency dealer or exchanger or money transmitter?

Yes. According to FinCEN's Ruling FIN-2008-R002, a foreign exchange dealer is included in the definition of a currency dealer or exchanger 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.

1089. Is a "foreign exchange broker or consultant" included in the definition of a currency dealer or exchanger 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.

1090. Is a "person who is engaged in the business of foreign exchange risk management" included in the definition of a currency dealer or exchanger 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 currency dealer or exchanger and a money transmitter, 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 Requirements

1091. Which types of MSBs are required to comply with AML requirements?

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 requirements. 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 requirements for a 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.

1092. Are there plans to simplify or modify the regulatory definition of MSBs?

Yes. FinCEN has proposed the following amendments to make it easier for businesses to understand whether they meet the regulatory definition of a MSB and what their subsequent AML responsibilities are:

- Raising or lowering the definitional threshold of $1,000 of MSB activity with the same person (in an aggregate amount in one type of MSB activity) on the same day
- Addressing regulatory changes concerning stored-value providers
- Including foreign-located entities engaging in MSB activities within the United States as MSBs that are subject to regulation (e.g., foreign entities with U.S. customers, foreign entities transmitting funds to or from U.S. recipients)

1093. With which key AML requirements are MSBs required to comply?

MSBs 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 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., 314(a), in most cases, mandatory; 314(b), optional)
- Registration with FinCEN (issuers, sellers or redeemers of stored value are exempt, as are agents of other MSBs that are MSBs solely because they offer products or services of the other MSBs)

For additional guidance on the various AML requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections.

1094. 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 a 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.

1095. There are several types of CTR forms (e.g., CTR, CTR-C). Which one should a MSB file?

All financial institutions that are required to file currency transaction reports, except casinos, should file the general CTR form. For additional guidance on CTRs, please refer to the Currency Transaction Reports section.

1096. 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.

1097. Should a 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, a 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.

1098. There are several types of SAR forms (e.g., SAR-DI, SAR-SF, SAR-MSB). Which one should a MSB file?

MSBs are required to file the Suspicious Activity Report by Money Services Business (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.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

1099. 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** – A 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.

1100. Are there exemptions to the suspicious activity reporting requirement of MSBs?

The SAR requirement currently does not apply to MSBs engaged in the following activities:

- Check casher
- Stored value – issuer, seller and redeemer

Therefore, if a 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 and stored-value activity.

1101. Should MSBs file SARs on behalf of their agents?

Yes. A 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.

1102. What are some trends of SAR filings related to MSBs?

According to FinCEN, some characteristics of SAR filings related to MSBs include, but are not limited to, the following:

- In 2009, the number of MSB-related SARs filed (12,093) showed little change, decreasing less than 1 percent when compared to the number of MSB-related SARs filed in 2008 (11,162).
- Money transfers and money orders, respectively, remain the most frequent types of financial service related to suspicious activity, accounting for 93 percent of services reported during the last year.
- Since 2008, only one category of suspicious activity reported by SAR-MSB filers has shown an increase: money transfers.
- Money orders saw a second straight year of decline since reaching their height in 2007; in fact, 2009 represented a record low for that category since reporting began. Also in decline since 2008 is the number of instances where MSB filers listed either traveler's checks or currency exchanges as the type of financial services related to suspected suspicious activity.
- In 2009, there were increases in the following types of suspicious activity noted by SAR-MSB filers:
    - Same individual(s) using multiple locations over a short time period
    - Changes in spelling or arrangement of name
- SAR-MSB filings characterizing a suspicious activity as "two or more individuals using the similar/same identification" have decreased every year since 2007; during the 12-month period from 2008 to 2009, the decrease was 19 percent.

1103. 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.

1104. Must a MSB maintain its AML program in English?

There is no prohibition against a 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.

1105. 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 this 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.

1106. What type of information should a 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 a MSB either at account opening or at a later date.

1107. What are the key recordkeeping requirements of the BSA for MSBs?

The BSA requires the retention of all BSA reports (e.g., SAR-MSBs, CTRs, FBARs, CMIRs). Additionally, other required documentation must be retained by currency dealers or exchangers, 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 currency dealer or exchanger 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 currency dealer or exchanger 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.

1108. 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.

1109. 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 same reasoning applies to conducting OFAC risk assessments. For additional guidance on AML and OFAC risk assessments, please refer to the Risk Assessments section.

1110. Are MSBs required to conduct customer risk assessments?

In instances in which MSBs have “customers” as defined in the Customer Identification Program (CIP), financial institutions are cautioned not to “define or treat all members of a specific category of customers as posing the same level of risk.” Further guidance states that MSBs should consider other customer-specific risk factors to assess risk. Leading practice dictates all financial institutions, including MSBs with “customers,” should have a customer risk assessment methodology in place. For additional guidance on customer risk assessments, please refer to the Risk Assessments section.

1111. 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 provided to the MSB). Evaluating the risks of MSBs in this manner will result in different risk ratings (e.g., low, moderate, high).

1112. 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.

1113. 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.

1114. What AML guidance has been issued related to MSBs?

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

- **Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses** by Internal Revenue Service (IRS), state agencies responsible for MSB regulation, the Money Transmitter Regulators Association (MTRA), the Conference of State Bank Supervisors (CSBS), and the Financial Crimes Enforcement Network (FinCEN).
- **Nonbank Financial Institutions – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Money Laundering Prevention: A Money Services Business Guide** by FinCEN
- **Guidance for Money Services Businesses – Risk-Based Approach** by the Financial Action Task Force (FATF)
- **Bank Secrecy Act Requirements: A Quick Reference Guide for Money Services Businesses** by FinCEN
- **Reporting Suspicious Activity: A Quick Reference Guide for Money Services Businesses** by FinCEN
- **Financial Institutions Outreach Initiative: Report on Outreach to Money Services Businesses** by FinCEN
- **Currency Transaction Reporting: Transactions between Money Transmitters and their Agents** by FinCEN
- **Determination of Money Services Business Status and Obligations Under the Funds Transfer Recordkeeping Rule, and Request for Regulatory Relief** by FinCEN
- **Frequently Asked Questions: Conducting Independent Reviews of Money Services Business Anti-Money Laundering Program** by FinCEN
- **Guidance - (Interpretive Release 2004-1) Anti-Money Laundering Program - Requirements for Money Services Businesses With Respect to Foreign Agents or Foreign Counterparties** by FinCEN
- **Preparation Guidelines for Use of Special Response "XX" in FinCEN Form 109, Suspicious Activity Report by Money Services Business** by FinCEN
- **Whether a Money Services Business Must Establish and Maintain Separate Deposit Accounts for its Separate Check Cashing and Money Transmission Lines of Business** by FinCEN
- **Guidance on Registration of MSBs** by FinCEN
    - Registration and De-Registration of Money Services Businesses
    - Completion of TIN on FinCEN Form 107 for Inclusion on FinCEN's Posted MSB Registration List
- **Guidance on the Provision of Banking Services to MSBs**
    - **"Providing Banking Services to Money Services Businesses"** within **Nonbank Financial Institutions – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
    - **Advisory - Guidance to Money Services Businesses on Obtaining and Maintaining Banking Services** by FinCEN
    - **Guidance - Interagency Interpretative Guidance on Providing Banking Services to Money Services Businesses Operating in the United States** by FinCEN

- **Joint Statement on providing banking services to money services businesses** by FinCEN
- **Difficulties Encountered by Money Services Businesses in Obtaining Banking Services** by FinCEN

- **Applicability of the Definition of MSB**
  - Definition of Money Services Business ("Doing Business" as a Money Services Business)
  - Definition of Money Services Business (Ceasing to be a Money Services Business)
  - Money Transmitter
    - Definition of Money Transmitter (Merchant Payment Processor)
    - Definition of Money Transmitter (Armored Car Companies)
    - Definition of Money Services Business (Money Transmitter/Currency Dealer or Exchanger)
    - Definition of Money Services Business (Money Transmitter/Currency Dealer or Exchanger) Whether an Authorized Agent for the Receipt of Utility Payments is a Money Transmitter
    - Whether a Company that Engages in Microfinance is a Money Services Business
    - Whether a Company that Engages in Certain Operations as an Authorized Agent for Collection of Social Security and Veteran Benefits is a Money Services Business
    - Whether a Company that Offers a Loan Acceleration Product for Consumer Financing is a Money Services Business
    - Whether a Certain Operation Protecting On-line Personal Financial Information is a Money Transmitter
    - Definition of Money Services Business (Debt Management Company)
  - Check Casher
    - Definition of Check Casher
    - Definition of Check Casher (Payday Lenders)
    - Whether a Business that Cashes Checks Payable to Customers to Apply Proceeds to the Repayment of Customers' Obligations is a Money Services Business
    - Frequently Asked Questions: Businesses Cashing Their Own Checks
    - Guidance - Definition of Check Casher and BSA Requirements
    - Whether a Publicly Traded Company that Cashes its own Checks Issued to Loan Customers is a Money Services Business
    - Whether a Business that Cashes Checks Payable to Customers to Apply Proceeds to the Repayment of Customers' Obligations is a Money Services Business
    - Whether a Publicly Traded Company that Cashes its own Checks Issued to Loan Customers is a Money Services Business
  - Currency Dealer or Exchanger
    - Application of the Definition of Money Transmitter to Brokers and Dealers in Currency and other Commodities
    - Whether a Foreign Exchange Consultant is a Currency Dealer or Exchanger or Money Transmitter
    - Whether a Person Who is Engaged in the Business of Foreign Exchange Risk Management is a Currency Dealer or Exchanger or Money Transmitter
    - Whether a Foreign Exchange Dealer is a Currency Dealer or Exchanger or Money Transmitter
    - Whether a Person Who is Engaged in the Business of Foreign Exchange Risk Management is a Currency Dealer or Exchanger or Money Transmitter
    - Whether a Foreign Exchange Consultant is a Currency Dealer or Exchanger or Money Transmitter

        - Definition of Money Services Business (Foreign-Located Currency Exchanger With U.S. Bank Account)
        - Whether a Foreign Exchange Dealer is a Currency Dealer or Exchanger or Money Transmitter
    - Stored Value
        - Whether Certain Reloadable Card Operations are Money Services Businesses
        - Application of the Definition of Money Services Business to Certain Owner-Operators of Automated Teller Machines Offering Limited Services
        - Whether Certain Operations of a Service Provider to Prepaid Stored-Value Program Participants is a Money Services Business
        - Definition of Money Transmitter/Stored Value (Gift Certificates/Gift Cards)

Additional guidance on how MSBs, including *casas de cambio* and informal value transfer systems (IVTS), can be abused by criminals include, but are not limited to, the following:

- **Guidance to Financial Institutions on the Repatriation of Currency Smuggled into Mexico from the United States** by FinCEN
- **FinCEN Advisory: Informal Value Transfer Systems** by FinCEN
- **General Principles for International Remittance Services** by the BIS
- **Bilateral Remittance Corridor Analysis (BRCA)** by the World Bank
- **Regulatory Frameworks for Hawalas and Other Remittance Systems** by the International Monetary Fund (IMF)
- **Combating the Abuse of Alternative Remittance Systems: International Best Practices Paper** by the Financial Action Task Force (FATF)

Additional organizations providing guidance on MSBs and the vulnerabilities of MSBs include, but are not limited to, the following:

- **Money Transmitter Regulators Association (MTRA)** is a national nonprofit organization that works toward the unifying regulatory practices amongst state-level regulators of money transmitters and check sellers.
- **Money Services Business Working Group (MSB-WG)** is an interagency working group composed of various law enforcement agencies that focuses on eliminating vulnerabilities posed by unlicensed MSBs.

Registration

1115. What is the registration requirement for MSBs?

MSBs are required to register by filing the Registration of Money Services Business form with FinCEN. (Stored-value issuers, redeemers or sellers are exempt if they do not provide other MSB services.)

1116. 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 requirements.

1117. Are all MSBs required to register with FinCEN?

All MSBs must register with FinCEN, except the following:

- A MSB that solely serves as an agent of another MSB
- A MSB that is solely an issuer, seller or redeemer of stored-value cards
- U.S. Postal Service
- Government agencies

1118. Should each branch of a MSB register separately with FinCEN?

No. A MSB should not register each branch separately with FinCEN.

1119. What should a MSB do if an error was found on a submitted registration form?

A 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

1120. What information does a MSB have to include with respect to its agents on its registration form?

A 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

1121. What supporting information is a MSB required to maintain?

A 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

1122. Should a MSB send this supporting information to FinCEN along with its registration form?

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.

1123. Are MSBs required to reregister after the initial registration with FinCEN?

Registrations must be renewed every two years. 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.

1124. 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.

1125. 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.

1126. Is inclusion on the monthly MSB Registration List a recommendation or endorsement from FinCEN?

No. Inclusion on the monthly MSB Registration List is not a recommendation or endorsement of the MSB from FinCEN or any other government agency. The MSB Registration List is intended only as general reference for the public.

1127. Can inclusion on the monthly MSB Registration List serve as evidence of a MSB's registration with FinCEN?

No. Only the registration acknowledgement letter issued from the IRS Enterprise Computing Center – Detroit (ECC-D) that a MSB receives after filing its registration can serve as evidence of registration with FinCEN.

1128. 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

1129. 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.

1130. Is an employee of a MSB considered an agent?

No. A person who is solely an employee of the MSB is not an agent of that MSB.

1131. 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.

1132. What information is a 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. A MSB's regulators and auditors also may request such information.

1133. 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

1134. What is a foreign agent or foreign counterpart of a MSB, and what are the heightened money laundering and terrorist financing risks of foreign agents?

A foreign agent or counterpart of a 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.

1135. Has any guidance been issued relating to a MSB's obligations with respect to foreign agents and foreign counterparts?

FinCEN issued interpretive guidance requiring that a 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

1136. 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).

1137. 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

1138. 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.

1139. Are IVTSs used only to transfer money?

No. Commodities can be transferred through this system as well.

1140. 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.

1141. 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.

1142. 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).

1143. 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

1144. 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.

1145. 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

1146. 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.”

1147. 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.

1148. 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.

Broker-Dealers

Definition

1149. 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.

1150. Who is responsible for examining broker-dealers for compliance with AML requirements?

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]).

1151. 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.

1152. Have the SEC, FINRA, or SROs issued new 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 new rule governing AML requirements.

1153. Does the New 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.

1154. 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).

1155. 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.

1156. 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.

1157. 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.

1158. 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 requirements

1159. With which key AML 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 (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 broker-dealers is provided below.

1160. 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

1161. 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.

1162. 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.

1163. There are several types of CTR forms (e.g., CTR, CTR-C). Which one should a broker-dealer file?

All financial institutions that are required to file currency transaction reports, except casinos, should file the general CTR form. For additional guidance on CTRs, please refer to the Currency Transaction Reports section.

1164. Can broker-dealers grant CTR exemptions?

No. Only depository institutions (banks, savings associations, thrift institutions or credit unions) can grant exemptions.

1165. There are several types of SAR forms (e.g., SAR-DI, SAR-SF, SAR-MSB). Which one should a broker-dealer file?

Broker-dealers are 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.

FinCEN is currently revising a number of the SAR forms. Broker-dealers should take extra care to ensure they are filing the correct forms. For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

1166. 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.

1167. 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-SF

1168. 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 instruments. The obligation to file a SAR-SF rests with each broker-dealer involved in the transaction, but only one SAR-SF filing is required per transaction.

For additional guidance on third-party reliance, please refer to the Third-Party Reliance section.

1169. What are some trends in SAR filings related to the securities and futures industry?

According to FinCEN, some trends in SAR filings related to the securities and futures industry include, but are not limited to, the following:

- Number of SAR filings have increased by more than 40 percent, from 4,267 in 2003 to 5,984 in 2007
- Increase in suspicious activity characterizations, including market manipulation, securities fraud and computer intrusion
- Increase in the use of mutual funds and stocks as the instrument types used

1170. Are there any exceptions to the independent testing requirement of the AML program for broker-dealers?

Yes. Under FINRA Rule 3310 (formerly the NASD rule 3011), broker-dealers that do 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) are only obligated to independently test their AML program every two years.

1171. 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.

1172. What are the key recordkeeping requirements of the BSA for broker-dealers?

The BSA requires the retention of all BSA reports (e.g., SAR-SFs, 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.

1173. 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** by the Securities and Exchange Commission (SEC)
- **Template for Small Firms** by Financial Industry Regulatory Authority (FINRA)
- **AML E-Learning Courses** by FINRA

- **AML Compliance Program Reporting Template** by the Chicago Board Options Exchange (CBOE)
- **Money Laundering and Terrorist Financing in the Securities Sector** by Financial Action Task Force (FATF)
- **Wolfsberg Frequently Asked Questions on Selected Anti-Money Laundering Issues in the Context of Investment and Commercial Banking** by the Wolfsberg Group
- **Principles on Client Identification and Beneficial Ownership for the Securities Industry** by International Organization of Securities Commissions (IOSCO)
- **Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities** by FinCEN
- **Frequently Asked Questions - Question and Answer Regarding the Broker-Dealer Customer Identification Program Rule** by FinCEN
- **Frequently Asked Questions – Customer Identification Program Responsibilities under the Agency Lending Disclosure Initiative** by FinCEN
- **Customer Identification Program Rule No-Action Position Respecting Broker-Dealers Operating Under Fully Disclosed Clearing Agreements According to Certain Functional Allocations** by FinCEN
- **Bank Secrecy Act Obligations of a U.S. Clearing Broker-Dealer Establishing a Fully Disclosed Clearing Relationship with a Foreign Financial Institution** by FinCEN
- **Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries** by FinCEN

Futures Commission Merchants and Introducing Brokers

Definition

1174. What is a futures commission merchant (FCM)?

An FCM is a person or entity registered, or required to register, as an FCM with the Commodities 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.

1175. 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 Requirements

1176. With which key AML 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 (314(a) (mandatory), 314(b) (optional))
- Complying with Special Measures
- Obtaining Foreign Bank Certifications
- Establishing an enhanced due diligence (EDD) program for 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 FCMs and IBs is provided below.

1177. 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

1178. There are several types of CTR forms (e.g., CTR, CTR-C). Which one should FCMs and IBs file?

All financial institutions that are required to file Currency Transaction Reports (CTRs), except casinos, should file the general CTR form. For additional guidance on CTRs, please refer to the Currency Transaction Reports section.

1179. There are several types of SAR forms (e.g., SAR-DI, SAR-SF, SAR-MSB). Which one should FCMs and IBs file?

FCMs and IBs should file the SAR-SF for suspicious transactions of $5,000 (or that aggregate to $5,000) or more.

FinCEN is currently revising a number of the SAR forms. FCMs and IBs should take extra care to ensure they are filing the correct form. For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

1180. Who is responsible for examining FCMs and IBs for compliance with AML requirements?

The Commodity Futures Trade Commission (CFTC) is responsible for examining FCMs and IBs for compliance with AML requirements. 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 and Commodity Pool Operators

Definition

1181. 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.

1182. Which types of CTAs are required to comply with AML requirements?

All CTAs, except the following, are required to comply with AML requirements:

- CTAs that publish newsletters, maintain noncustomized Internet websites, or create noncustomized computer software
- CTAs that do not direct client accounts

1183. What is a commodity pool operator (CPO)?

A CPO is an investment trust, a syndicate or a similar form of enterprise operated for the purpose of trading commodity interests.

A CPO includes an investment trust, a syndicate or a similar type of business that solicits, accepts or receives from others funds, securities or property for trading in any commodity for future delivery on, or subject to the rules of, any contract market or derivatives transaction execution facility.

Key AML Requirements

1184. With which key AML requirements are CTAs and CPOs required to comply?

CTAs and CPOs 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)

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 and CPOs is provided below.

1185. Are CTAs and CPOs required to establish an AML program?

No. At present, the AML program requirement of the USA PATRIOT Act does not apply to CTAs and CPOs.

1186. Are CTAs and CPOs subject to the CIP requirement?

No. Currently, CTAs and CPOs 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.

1187. Are CTAs and CPOs required to file CTRs?

No. Currently, CTAs and CPOs are not required to file Currency Transaction Reports (CTRs). CTAs and CPOs 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.

1188. Are CTAs and CPOs required to file SARs?

While CTAs and CPOs 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.

1189. Are CTAs and CPOs 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)).

Mutual Funds

Definition

1190. 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.

1191. Which types of mutual funds are required to comply with AML requirements?

All types of mutual funds are required to comply with AML requirements.

Key AML Requirements

1192. With which key AML requirements are mutual funds required to comply?

Mutual funds 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 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 (314(a) (mandatory), 314(b) (optional))
- Screening for Special Measures
- Requiring Foreign Bank Certifications
- Establishment of an enhanced due diligence (EDD) program for 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 mutual funds is provided below.

1193. Are mutual funds required to file CTRs?

No. Currently, mutual funds are not required to file CTRs. Mutual funds 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.

1194. There are several types of CTR forms (e.g., CTR, CTR-C). Which one should a mutual fund file?

All financial institutions that are required to file CTRs, except casinos, should file the general CTR form. For additional guidance on CTRs, please refer to the Currency Transaction Reports section.

1195. 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.

1196. There are several types of SAR forms (e.g., SAR-DI, SAR-SF, SAR-MSB). Which one should a mutual fund file?

Mutual funds are 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.

FinCEN is currently revising a number of the SAR forms. Mutual funds should take extra care to ensure they are filing the correct forms. For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

1197. 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-SF 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-SF was filed on the suspicious activity, regardless of which firm actually filed the report.

1198. 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.

1199. 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.

1200. Who is responsible for examining mutual funds for compliance with AML requirements?

The SEC is responsible for examining mutual funds for compliance with AML requirements.

Insurance Companies

Definition

1201. Which types of insurance companies are required to comply with AML requirements?

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 requirements.

1202. 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

1203. Are there any exemptions from the definition of insurance companies that are not subject to AML requirements?

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.

Key AML Requirements

1204. With which key AML 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 (314(a) (mandatory), 314(b) (optional))

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.

1205. Are insurance agents and brokers subject to AML requirements?

While insurance agents and brokers are not subject to separate AML requirements, 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.

1206. 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.

1207. 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.

1208. There are several types of SAR forms (e.g., SAR-DI, SAR-SF, SAR-MSB). Which one should an insurance company file?

Insurance companies are 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.

Although FinCEN has proposed a new SAR form for insurance companies, it has not yet been adopted. Until it is, insurance companies should continue to use the SAR-SF form with the words "Insurance SAR" in the first line of the narrative. Insurance companies should take extra care to ensure they are filing the correct forms. For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

1209. 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.

1210. What are some trends of SAR filings related to insurance companies?

SAR filings related to insurance companies are somewhat difficult to unbundle from other industry segments. That is because FinCEN has not released a SAR form specifically for insurance companies and has instructed insurance companies, for the interim, to use FinCEN Form 101, Suspicious Activity Report by the Securities and Futures Industries.

FinCEN's most recent review of SAR activity for the second year of mandatory filing for insurance companies included, among others, the following observations:

- While SAR filings almost doubled in the second year of mandatory reporting, from 641 to 1,276 SARs, almost half of the filings came from the subsidiaries of just two companies, suggesting that some institutions may not have fully developed their monitoring, investigation and reporting capabilities.
- The top-reported states based on subject location were New York, California, New Jersey, Florida and Texas.
- Policy holders and annuity owners continue to be the most-reported subjects in the SAR filings for insurance products, and while most were individual subjects, business entities, trusts and retirement plans were also reported as subjects. Insiders, primary agents, brokers and gatekeepers (e.g., lawyers, accountants) also were cited as subjects in a meaningful number of SARs filed.
- Consistent with depository institutions, BSA/Money Laundering/Structuring was noted as the primary reason for the filings.
- Life insurance policies and annuities were the products most often mentioned in SARs.

1211. 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.

1212. Who is responsible for examining insurance companies for compliance with AML requirements?

The Internal Revenue Service (IRS) is responsible for examining insurance companies for compliance with AML requirements. 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 requirements.

1213. What AML 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:

- **Insurance - Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Frequently Asked Question: Customer Identification Programs and Banks Serving as Insurance Agents** by the FFIEC
- **Insurance Industry Suspicious Activity Reporting: An Assessment of Suspicious Activity Report Filings** by the Financial Crimes Enforcement Network (FinCEN)
- **Frequently Asked Questions from the Insurance Industry** by the Office of Foreign Assets Control (OFAC)
- **Risk-Based Approach for the Life Insurance Sector** by the Financial Action Task Force (FATF)
- **Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism** by International Association of Insurance Supervisors (IAIS)
- **Anti-money Laundering Guidance Notes** by the IAIS

Casinos or Card Clubs

Definition

1214. 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.

1215. 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.

1216. Which types of casinos or card clubs are required to comply with AML requirements?

Casinos or card clubs that have a gross annual gaming threshold in excess of $1 million are required to comply with AML requirements.

1217. 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).

1218. Which types of gaming activities may qualify an institution as a casino or card club subject to AML requirements?

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.

1219. 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.

1220. 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.

1221. 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.

1222. 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 Requirements

1223. With which key AML 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 (314(a) (mandatory), 314(b) (optional))

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.

1224. 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.

1225. 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. 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.

1226. There are several types of CTR forms (e.g., CTR, CTR-C). Which one should casinos and card clubs file?

Casinos and card clubs are required to file a 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).

1227. Are there exceptions to the CTR filing requirement for certain transactions in casinos and card clubs?

Yes. As of July 1, 2007, FinCEN ruled that casinos are exempt from the requirement to file CTRs on jackpots from slot machines and video lottery terminals.

1228. 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

1229. 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.

1230. What are the Form 8300 reporting requirements for casinos and card clubs?

Form 8300 relates specifically to 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).

1231. 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.

1232. There are several types of SAR forms (e.g., SAR-DI, SAR-SF, SAR-MSB). Which one should casinos and card clubs file?

Casinos and card clubs are 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.

FinCEN is currently revising a number of the SAR forms. Casinos and card clubs should take extra care to ensure they are filing the correct forms. For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

1233. 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.

1234. 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-C for a robbery or burglary committed or attempted that is reported to appropriate law enforcement authorities.

1235. 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.

1236. What are some trends of SAR filings related to casinos and card clubs?

According to FinCEN, some trends in SAR filings related to casinos and card clubs include, but are not limited to, the following:

- The largest number of Suspicious Activity Reports by Casinos and Card Clubs (SAR-C) filings by U.S. States and Territories between August 1, 1996 and December 31, 2009 were in New Jersey (16,833) and Nevada (11,553). The next highest numbers of filings, in descending order, were in Louisiana, Mississippi, California and Connecticut.

- The largest number of SAR-C filings by U.S. States and Territories in 2009 were, in descending order, Nevada, New Jersey, Louisiana, Oklahoma and California.
- Filings in the four-year period 1996-1999 were 1,123 as compared to 40,484 during the 4-year period 2006-2009, a 3,505 percent increase.
- Using queries of the Document Control Number (DCN), FinCEN identified 40,409 SAR-Cs filed by casinos and cards clubs from January 1, 2004 through December 31, 2008. These SAR-Cs reported an aggregate of more than $900 million of suspicious activity. Although the SAR-Cs examined were filed from 2004 through 2008, some of the suspicious activity began as early as August 2001.
- Ninety-five percent of SAR-Cs were filed within 30 days of detection, and 76 percent were filed electronically.
- SAR-C filers fully identified the subject(s) by listing the full name, address and a Social Security Number (SSN) on 59 percent of the SAR-Cs. Of the remaining SAR-Cs (41 percent), nearly half did not include a SSN but did list another type of identification such as a driver's license number, passport number, or alien registration number.
- The key suspicious activities of patrons that casinos observed or detected and reported included:
    - Reducing the number of chips or tokens to be cashed out at a cage when asked to provide identification or a SSN when the cash out was over $10,000, or when a subject had previously cashed out chips or tokens and the additional cash out would exceed $10,000 in a gaming day (the most reported structuring activity).
    - Reducing the amount of cash buy-ins in pits to avoid providing identification or a SSN.
    - Using agents to cash out chips: casino employees observed individuals handing over chips to agents to cash out. After cashing out the chips, agents were observed passing the cash to the true owners of the funds. Although many of the narratives identified at least the names of all the individuals involved, most listed only one individual in the SAR-C subject field (usually the true owner of the funds). A few filers opted to submit individual reports for each individual involved in the transaction.
    - Cashing out chips, tickets, and/or tokens multiple times a day at different times or at different windows/cages: Several SAR-Cs reported individuals cashing checks multiple times a day but in amounts just below $3,000 per location.
    - Requesting jackpot winnings exceeding $10,000 to be paid in two or three checks of lesser value.
    - Depositing and withdrawing structured amounts of cash held in a safekeeping account.
    - Wiring funds into front money accounts and depositing cash the next day followed by withdrawing half of the funds through structured drafts.
    - Repaying outstanding balances with structured cash, wired funds, and checks over several days: One individual sent an agent on three different days to repay a debt with eight checks, all under $10,000, drawn on the accounts of eight different companies at different depository institutions.
    - Purchasing $9,000 in chips with cash at the cage and purchasing another $1,000 in chips with cash in a pit.

1237. 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.

1238. 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., SAR-Cs, 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 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.

1239. Who is responsible for examining casinos and card clubs for compliance with AML requirements?

The Internal Revenue Service (IRS) is responsible for examining casinos and card clubs.

1240. 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.

1241. What AML guidance has been issued related to casinos?

The following key guidance has been issued related to casinos:

- **Nonbank Financial Institutions – Overview** 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** by the Financial Action Task Force (FATF)
- **Risk-Based Approach for Casinos** by the FATF
- **Guidance on Casino or Card Club Risk-Based Compliance Indicators** by FinCEN
- **Guidance (Frequently Asked Questions) – Casino Recordkeeping, Reporting and Compliance Program Requirements (2007 and 2009)** by FinCEN
- **Guidance on Casino or Card Club Compliance Program Assessment** by FinCEN
- **Definition of Money Services Business (Casinos as Money Services Businesses)** by FinCEN
- **Suspicious Activity Reporting Guidance for Casinos** by FinCEN
- **Guidance on Recognizing Suspicious Activity – Red Flags for Casinos and Card Clubs** by FinCEN
- **Currency Transaction Reporting: Aggregation by Casinos at Slot Machines** by FinCEN
- **Guidance on Determining Whether Tribally Owned and Operated Casinos are Eligible for Exemption from CTR Requirements** by FinCEN
- **A Cash Wager on Table Game Play Represents a "Bet of Currency"** by the Financial Crimes Enforcement Network (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

1242. 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).

1243. Which types of operators of credit card systems are required to comply with AML requirements?

All operators of credit card systems doing business in the United States are required to comply with AML requirements. There is no exemption from the definition.

1244. 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.

1245. 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.

1246. 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 Requirements

1247. With which key AML 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 (314(a) (mandatory), 314(b) (optional))

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.

1248. 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.

1249. 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.

1250. 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.

Dealers in Precious Metals, Stones or Jewels

Definition

1251. Which types of dealers in precious metals, stones or jewels are required to comply with AML requirements?

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 are required to comply with AML requirements.

1252. 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.

1253. 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.

1254. 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.

1255. 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.

1256. 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.

1257. 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 Requirements

1258. With which key AML requirements are dealers of precious metals, stones or jewels required to comply?

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
- 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 (314(a) (mandatory), 314(b) (optional))

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.

1259. 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.

1260. 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.

1261. 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.

1262. Who is responsible for examining dealers for compliance with AML requirements?

The IRS is responsible for examining dealers for compliance with AML requirements.

Persons Involved in Real Estate Settlements and Closings

Definition

1263. Which types of persons involved in real estate settlements and closings are required to comply with AML requirements?

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.

1264. Are all types of real estate transactions subject to AML requirements?

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 requirements.

1265. 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

1266. What factors are being considered by the U.S. Treasury Department to determine which involved persons will be subject to further AML requirements?

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).

1267. Are any persons involved in real estate settlements and closings exempt from AML requirements?

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 requirements.

1268. 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."

Key AML Requirements

1269. With which key AML 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)

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.

1270. 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.

1271. 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.

1272. 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.

1273. 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.

1274. 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.

1275. 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)).

1276. 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** by the Office of Foreign Assets Control (OFAC)
- **RBA Guidance for Real Estate Agents** by the Financial Action Task Force (FATF)
- **Money Laundering and Terrorist Financing Through the Real Estate Sector** by FATF
- **Money Laundering in the Commercial Real Estate Industry: An Assessment Based Upon Suspicious Activity Report Filing Analysis** by the Financial Crimes Enforcement Network (FinCEN)

Investment Advisers

Definition

1277. What is an investment adviser?

An investment adviser is any person whose business involves advising others as to the value of securities or the advisability of investing in, purchasing or selling securities, or who issues reports or analyses regarding such activities.

1278. Which types of investment advisers would be required to comply with AML requirements under the proposed rule?

The proposed rule defines two groups of investment advisers who would be subject to AML requirements. The first group includes investment advisers who are located at a principal office and/or place of business in the United States, are registered with the Securities and Exchange Commission (SEC), and report to the SEC that they have assets

under management, including advisers registered with the SEC who have either discretionary or nondiscretionary authority over their clients' assets.

The second group includes investment advisers who are not registered with the SEC, but who have $30 million or more of assets under management, and are relying on the registration exemption provided by Section 203(b)(3) of the Investment Adviser's Act of 1940, which states that advisers with fewer than 15 clients who do not hold themselves out generally to the public as investment advisers are exempted from SEC registration.

1279. Are any investment advisers exempt from AML requirements?

Investment advisers who are not registered with the SEC because they are state-registered firms that have less than $30 million in assets under management and advisers who are registered with the SEC but do not manage client assets are exempt.

In addition, unregistered advisers who are otherwise required to have an AML program because they are also registered as a financial institution in another capacity, and are therefore subject to examinations by a federal functional regulator for compliance with the AML program requirement under that capacity, are exempt from investment adviser-specific AML requirements.

1280. What is meant by the term "managed"?

When an account is managed, the client's assets are under the direction of the investment firm that is responsible for investing the fund's assets, implementing its investment strategy, and managing the day-to-day portfolio trading. The actual account is usually maintained with a broker-dealer, bank or other custodian.

In reality, many investment advisers manage portfolios for some clients, but have other clients for which the firm provides very different services (e.g., pension consulting, securities newsletters or research reports, or financial planning). Under such circumstances, an investment adviser may exclude from its AML procedures clients whose assets are not managed by the firm.

1281. Do partnerships or other pooled investment vehicles count as one client when determining the exemption criteria of advisories of less than 15 clients?

Yes. Rather than count each limited partner or other investor as a client, an SEC rule allows the adviser to count the partnership or other pooled investment vehicles as a single client. This rule can result in the advisers having only one or two pooled investment vehicle clients, but managing tens or hundreds of millions of dollars.

Some of these pooled investment vehicles may be subject to FinCEN's proposed rule, which requires unregistered investment companies to implement AML programs. These advisers may have other clients who are not subject to FinCEN's proposed rule.

1282. 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 the only one who can truly monitor customer transactions for suspicious activity.

Key AML Requirements

1283. With which key AML requirements are investment advisers required to comply?

Investment advisers 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)

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 advisers is provided below.

1284. How will unregistered investment advisers be identified by FinCEN?

FinCEN's proposed rule will require unregistered investment advisers to file a notice with FinCEN in order to provide FinCEN with identifying information about the firm to ensure that these entities are in compliance with AML requirements.

1285. Are investment advisers required to establish an AML program?

No. At present, the AML program requirement of the USA PATRIOT Act does not apply to investment advisers.

1286. Are investment advisers subject to the CIP requirement?

No. Currently, investment advisers 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.

1287. Are investment advisers required to file CTRs?

No. Currently, investment advisers 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.

1288. Are investment advisers required to file SARs?

While investment advisers 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.

1289. Are investment advisers 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)).

Unregistered Investment Companies

Definition

1290. What is an unregistered investment company?

According to the 1940 Act, an "investment company'' is defined as any issuer that:

Represents or carries out its primary purpose of investing, reinvesting or trading in securities; issuing face-amount certificates of the installment type or conducting such activities and has outstanding certificates; or investing, reinvesting, owning, holding or trading in securities and owning or planning to acquire investment securities exceeding 40 percent of the value of such issuer's total assets (exclusive of government securities and cash items) on an unconsolidated basis.

Under the 1940 Act, certain investment companies, such as hedge funds, are exempt from registration requirements.

1291. Which types of unregistered investment companies are required to comply with AML requirements?

Unregistered investment companies that meet any of the following criteria are required to comply with AML requirements:

- Permits an owner to redeem his or her interest within two years of purchasing that interest
- Has total assets as of the end of the most recent calendar quarter valued at $1 million or more
- Is organized under the law of a state or the United States, is organized, operated or sponsored by a U.S. person, or sells ownership interests to a U.S. person

1292. What are some examples of unregistered investment companies?

Some examples of unregistered investment companies include, but are not limited to, the following:

- Hedge funds
- Funds of hedge funds (a registered or unregistered investment company that invests in hedge funds attractive to investors who seek access to multiple hedge fund investments by investing in only one investment company)
- Private equity funds
- Venture capital funds
- Real estate investment trusts (REITs)

1293. Which types of unregistered investment companies are not subject to AML requirements?

The following types of unregistered investment companies are exempted from the definition and therefore are not subject to AML requirements:

- An investment company with nonredeemable or conditionally redeemable interests
- A family company
- An employees' securities company or investment companies established by employers for the benefit of employees
- An employee benefit plan that is not construed to be a pool
- An offshore unregistered investment company

1294. How is the term "family company" defined?

The term "family company" is defined as a company that has $5 million or more in investments that are owned directly or indirectly by two or more related natural persons.

Key AML Requirements

1295. With which key AML requirements are unregistered investment companies required to comply?

Unregistered investment companies must comply with the following key AML laws and regulations:

- 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)
- Filing Notice with FinCEN

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 unregistered investment companies is provided below.

1296. Are 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 unregistered investment companies; however, more and more unregistered investment companies are voluntarily developing AML programs.

1297. Are unregistered investment companies subject to the CIP requirement?

No. Unregistered investment companies are not subject to the Customer Identification Program (CIP) requirement. For a list of financial institutions that are subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

1298. Are unregistered investment companies required to file CTRs?

No. Currently, unregistered investment companies are not required to file Currency Transaction Reports (CTRs). Unregistered investment 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 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

1299. Are unregistered investment companies required to file SARs?

While 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 on Form 8300 for indicating that a transaction is potentially suspicious.

1300. Are 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)).

Notice

1301. How are unregistered investment companies identified by regulatory bodies?

The proposed rule requires unregistered investment companies to file a notice with FinCEN in order to provide FinCEN with identifying information about the firm to ensure these entities are in compliance with AML requirements.

1302. What information must be provided by unregistered investment companies on the notice to FinCEN?

The notice includes the following information:

- Name of the unregistered investment company, including all family or complex names, trade names and doing business as (DBA) names
- Complete street address, telephone number and, if applicable, the e-mail address of the unregistered investment company
- Name, complete street address, telephone number, and if applicable, the e-mail address and registration number of the investment adviser, commodity trader adviser (CTA), commodity pool operator (CPO), organizer and/or sponsor of the unregistered investment company
- Total assets under management held by the unregistered investment company as of the end of the unregistered investment company's most recent fiscal year
- Total number of participants, interest holders or security holders in the unregistered investment company

1303. When should an unregistered investment company file a notice?

An unregistered investment company should file a notice within 90 days after it first becomes subject to AML program requirements.

1304. What should an unregistered investment company do if the information filed on the original notice changes?

An unregistered investment company should file an amendment to its notice within 30 days after any change to the information in the notice other than the total amount of assets under management or the total number of participants, interest holders or security holders.

1305. What should an unregistered investment company do if it ceases to be subject to the provisions of this rule?

An unregistered investment company should withdraw its notice within 90 days after ceasing to be subject to the provisions of this rule.

Nonfinancial Businesses

Definition

1306. 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 Requirements

1307. With which key AML 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)

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.

1308. Are nonfinancial institutions required to comply with OFAC 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.

1309. 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.

1310. 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.

1311. 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.

1312. 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.

1313. 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)).

1314. 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

1315. 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.

1316. 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).

1317. 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.

1318. 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.

1319. 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.

1320. 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.

1321. 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.

1322. 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

1323. 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.

1324. 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.

1325. 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

1326. 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.

1327. 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

1328. 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)

1329. 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.

1330. 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.

1331. 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.

1332. 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

1333. Which institutions are required to implement an ITPP?

Financial institutions as defined in the Fair Credit and Reporting Act (FCRA) (i.e., 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) are required to implement an ITPP.

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.

However, for other types of institutions potentially subject to the “creditor” standard in the Federal Trade Commission’s (FTC’s) Rule, significant confusion and disagreement exists as to how broadly Congress intended this definition to be applied. In particular, certain types of healthcare providers, attorneys and other businesses not traditionally considered financial institutions, but who/that may allow consumers to defer payments of their debts, disagreed with the FTC’s opinion that they should be subject to the Rule. Thus, the FTC has delayed the effective date of the Rule several times, and it is possible Congress may amend the statute to clarify its applicability.

1334. 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).”

1335. 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

1336. 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).

1337. 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.

1338. 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

1339. 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).

1340. 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

1341. 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.

1342. 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

1343. 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

1344. 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.

1345. 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).

1346. 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.)

Mortgage Fraud

1347. 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.

1348. Which types of loan products typically have been used in mortgage fraud schemes?

Estimates suggest that more than 70 percent of mortgage fraud cases have used purchase loan types; refinances were used in 12 percent of mortgage fraud cases, of which more than 25 percent were cash-out refinances; and home equity, second trust and construction loan types accounted for less than 10 percent of mortgage fraud cases. All of the above loan products were used primarily for fraud for housing schemes, except for the home equity and construction loan types.

1349. 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.
- **Income Boosting** – 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.
- **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.
- **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.

When monitoring for suspicious activity, it is important for financial institutions to develop red flags to identify suspicious activity in which the borrower is not only the suspect but also the victim (i.e., abused by industry professionals). For a list of red flags, please refer to the Lending Red Flags and Mortgage and Real Estate Red Flags sections.

1350. 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)

1351. Are financial institutions required to report suspected mortgage fraud on SARs?

Yes. Financial institutions are required to report suspected mortgage fraud on Suspicious Activity Reports (SARs). According to FinCEN, SAR filings related to mortgage fraud have increased from approximately 1,700 filings in 1997 to more than 67,000 in 2009, an increase of nearly 4,000 percent. Hot spots for mortgage fraud included California, Florida, Georgia, Illinois, New York and Texas.

However, it is important to note that more than 75 percent of the mortgage fraud-related SARs filed in 2009 pertained to activity that occurred a year or more before the filing date. This may suggest that the increase in SAR filings stems, at least in part, to the efforts of secondary market investors, mortgage insurers, and other stakeholders to find evidence of underwriting deficiencies (including fraud) that would allow them to force originators to buy back non-performing loans, as it does to a bona fide increase in the incidence of mortgage fraud itself. In other words, it is possible that much of the apparent fraud now being reported would never have been detected had the loans in question not gone into default, regardless of whether the fraud and reasons for default were related.

1352. Various studies have shown a significant percentage of "stated income" loans include misrepresentation, such as boosted income. Is a financial institution required to file on this type of activity?

Yes. If misrepresentation is detected, a financial institution is required to file a SAR. However, there are varying views among industry participants as to exactly what constitutes sufficient evidence of boosting to file a SAR. Some organizations file only if they have affirmative evidence an intentional misstatement has occurred (e.g., a borrower admits that his/her income was inflated, or a loan servicer subsequently obtains income documents that disagree substantially with stated values previously provided). Other organizations have performed more proactive reviews, comparing borrowers' stated incomes to expected incomes based on salary surveys for borrowers' lines of work, and also have conducted investigations and potentially filed SARs when the percentage differences between stated and industry average income values exceed certain materiality thresholds.

Key drivers for the increase in SAR filings related to boosting and other misrepresentations have been the mortgage foreclosure crisis and widespread adoption of the U.S. Treasury Department's Home Affordable Modification Program (HAMP) and similar foreclosure-prevention alternatives. HAMP and nearly all such similar programs require that distressed borrowers, to be considered for a modification, submit paystubs, tax returns, and other verifiable income

documentation. This can often lead the servicer (particularly if the firm that services the loan also originated it) to realize the borrower significantly boosted his/her income in order to obtain the loan in the first place.

Interestingly, although not surprisingly, mortgage fraud SAR filings related to modification programs themselves have skyrocketed, with 150 percent more such SARs filed in 2009 than in the entire preceding five-year period.

1353. Which participants in the mortgage lending process are most commonly the subject of mortgage fraud-related SARs?

Few would disagree that blame for the financial crisis is shared among many parties, including borrowers. In fact, although perhaps not the most objective source, SAR filing trends suggest that borrowers own much of the blame. According to FinCEN, approximately 50 percent of mortgage SARs filed identified borrowers as subjects. In contrast, appraisers were listed as subjects approximately 5 percent of the time. Institutions' own employees were listed in 1 percent of cases or fewer.

1354. What are the most common types of suspicious activity reported in connection with mortgage loan fraud SAR filings?

According to FinCEN data, secondary activities include, in descending order of frequency:

- False statements
- Identity theft
- Consumer loan fraud
- Misuse of position or self-dealing
- BSA/structuring/money laundering
- Commercial loan fraud

1355. Are any AML requirements under consideration with regard to mortgage lenders and originators?

Yes. Due to the rise in abusive and fraudulent sales and financing practices in both the primary and secondary residential mortgage markets, in July 2009, FinCEN issued the proposed rule, "Anti-Money Laundering Program and Suspicious Activity Report Requirements for Non-Bank Residential Mortgage Lenders and Originators." The proposed rule would apply to a subset of loan and finance companies, nonbank residential mortgage lenders, and originators. (As is the case with the term "persons involved in real estate closings and settlements," the term '"loan or finance company" is not defined or discussed in any FinCEN regulation.) For further guidance, please refer to the Persons Involved in Real Estate Closing and Settlements section.

The proposed rule would require nonbank residential mortgage lenders and originators 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
- Independent testing of the AML Compliance Program

The rule may also require mortgage lenders and originators to file Suspicious Activity Reports (SARs). For further guidance, please refer to the following section: Section 352 – AML Program and Suspicious Activity Reports.

Unlawful Internet Gambling Enforcement Act and Prohibition on Funding of Unlawful Internet Gambling Regulation

1356. What is Internet gambling?

Simply put, Internet gambling is the online wagering of money or other value.

1357. How big is the global Internet gambling market?

Some estimates suggest that the global Internet gambling market is between $17.7 billion and $23.6 billion dollars.

1358. How big is the U.S. Internet gambling market?

For 2008, it has been estimated that the U.S. Internet gambling market was roughly one-fourth to one-third of the global market, or approximately $5.9 billion.

1359. Is Internet gambling widely prohibited?

Although some foreign countries permit and actually license various forms of online gaming, the United States has enacted federal legislation to prohibit "unlawful Internet gambling."

1360. What is "unlawful Internet gambling"?

Under the U.S. Unlawful Internet Gambling Enforcement Act of 2006 (UIGE Act), 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 lands in which the bet or wager is initiated, received or otherwise made. Certain law enforcement agencies also have taken the position that most online gambling is illegal under the federal Wire Act and certain state laws.

1361. Are there any exclusions to unlawful Internet gambling under the UIGE Act?

The UIGE Act 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 offer by the sponsor.

The UIGE Act also exempts participation in any fantasy or simulation sports game or educational game or contest in which the game or contest involves a team(s) whose members are not based on the 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

1362. 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

1363. How does the UIGE Act aim to prevent illegal Internet gambling?

The UIGE Act 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 UIGE Act was enacted in October 2006, and the U.S. Treasury Department and Federal Reserve 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 (PFUIG regulation).

1364. Why was the effective date for compliance with the UIGE Act deferred until June 1, 2010?

A number of parties subject to the rule indicated they would not be able to implement policies and procedures within the initial time frame, and also expressed concern over certain ambiguities in the UIGE Act.

1365. 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, the PFUIG regulation, the following payment systems are designated:

- **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 depositary 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 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 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**. However, 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.

1366. Are customers of designated participants also subject to the PFUIG regulation?

The UIGE Act 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 non-exempt participants in designated payment systems.

However, as noted above, it is important to understand that other federal and state laws prohibiting illegal Internet gambling can apply directly to customers, and other parties to the transaction.

1367. Are any participants exempt from the requirement to have policies and procedures?

The rule does exempt certain participants, but does not identify these participants. Rather, as detailed above, certain types of participants are exempt from establishing written policies and procedures.

1368. What types of policies and procedures does the PFUIG regulation require designated 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 must 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 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.

1369. 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
- Circumstances under which the access to the card system for the merchant, merchant acquirer or third party processor should be denied

1370. 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.

1371. What types of policies and procedures does the PFUIG regulation expect nonexempt participants to develop and implement?

The PFUIG regulation contemplates that nonexempt participants will develop and maintain policies and procedures addressing the following:

- Notices to new and existing commercial account holders that restricted transactions are prohibited
- 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 institutions must require:
        - A certification from the customer stating that it does not engage in Internet gambling or, if it does, a commercial license or legal opinion that such activity does not involve restricted transactions
        - A written commitment to report any change in its legal authority
        - 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

1372. What if a participant has actual knowledge that a commercial customer is engaging in Internet gambling?

If a participant has actual knowledge that a commercial customer is engaging in Internet gambling, then the participant should obtain the documentation outlined above.

1373. What if a participant has actual knowledge that a customer is conducting restricted transactions?

Participants are expected to have policies and procedures to address continued transaction processing, account review, suspicious activity report (SAR) filing, and account closure in circumstances where it has knowledge that the customer is conducting restricted transactions.

1374. Since most 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.

1375. Does the PFUIG regulation provide any safe harbor to nonexempt 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.

1376. If an operator-driven system, such as a card system, has policies and procedures in place to comply with the UIGE 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 policies and procedures of the system operator. The participant must obtain written 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.

1377. Which regulators are responsible for enforcing the UIGE Act?

Enforcement is the responsibility of designated federal functional regulators; if no such regulator exists, the Federal Trade Commission (FTC) is responsible for enforcement.

1378. What are the consequences for not complying with the UIGE Act?

A violation of the UIGE Act 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.

1379. 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 transmission of sports bets or wagers or information assisting in the placement of such bets or wagers. 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.

1380. Are there any expected changes to the U.S. ban on Internet gambling?

A bill has been proposed in Congress that could overturn the UIGE Act and permit online poker and other non-sports betting. Whether the bill becomes law remains to be seen.

1381. Does the UIGE Act have any applicability outside of the United States?

The UIGE Act encourages the cooperation of foreign governments and the Financial Action Task Force (FATF) in sharing information on Internet gambling and related abuses.

Certain foreign countries have challenged whether the United States can prevent Internet gambling.

1382. What is the relationship of the UIGE Act to the Bank Secrecy Act/Anti-Money Laundering compliance?

UIGE Act compliance is separate and distinct from BSA/AML compliance, though customer due diligence is a tenet of both. Compliance with the UIGE Act does not fulfill any other BSA/AML compliance requirement, such as the requirement to file SARs.

INTERNATIONAL PERSPECTIVES AND INITIATIVES

International Perspectives

1383. How do U.S. regulations compare to international AML regulations?

As a result of the terrorist activities of September 11, 2001, the U.S. AML regulations are among the most far-reaching in the world. The USA PATRIOT Act expanded the traditional definition of a financial institution. It is now much broader and encompasses numerous businesses that previously were not subject to AML regulations. For example, U.S. AML regulations now apply to, among others, casinos and dealers in precious metals and jewelry, which were previously unregulated businesses. The USA PATRIOT Act also requires sweeping measures to be taken with respect to shell banks and correspondent accounts.

While these measures may not have been incorporated previously into other countries' AML standards, the recent international focus on AML standards has encouraged many countries to introduce several new AML regulations, which, in large part, already have been implemented in the United States because of the USA PATRIOT Act.

Unlike Australia and the United Kingdom, the United States has not implemented regulations for select "professional service providers" (e.g., attorneys, accountants). In fact, the Financial Action Task Force (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 Evaluation Reports sections.

1384. 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 Forty Recommendations and Nine Special Recommendations (also referred to as "Forty plus Nine Recommendations" or "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 Forty plus Nine Recommendations, please refer to the Financial Action Task Force section.

1385. 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.

While the USA PATRIOT Act stipulates regulations for many different types of financial institutions, essentially, the underlying requirements for all financial institutions are similar. And with the revision of FATF's Recommendations, compliance requirements across the globe are continually converging. This builds the case for introducing an institutionwide AML framework, allowing for customization within the different businesses. A common framework also limits opportunities for money launderers or terrorists to take advantage of lax regimes.

Where possible, institutionwide 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.

1386. 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 customers 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

1387. 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 create 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) 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.
- **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 the FTAF'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.

1388. 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.

1389. 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** – 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 – March 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** – Guidance to assist mutual funds and other pooled investment vehicles with managing their money laundering risk.
- **Wolfsberg Statement on Monitoring Screening and Searching – September 2003** – (Note: This guidance was superseded by subsequent guidance issued on the same topic in November 2009) – As other guidelines, statements and principles made by the Wolfsberg Group have not addressed issues related to the development of a risk-based monitoring and screening process for an institution's customers and related transactions, this statement speaks to issues that should be addressed in order to develop such a process.
- **Wolfsberg Statement on AML Screening, Monitoring and Searching – November 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 – November 2002** – Guidance concerning the establishment and ongoing maintenance of correspondent banking relationships.
- **Wolfsberg Frequently Asked Questions on Correspondent Banking** – 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 – August 2009** – Guidance issued by 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 – January 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 – Revised Version May 2002** – Guidance tailored towards 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** – Guidance addressing specific money laundering concerns in the investment and commercial banking industries.
- **Wolfsberg FAQs on Beneficial Ownership** – A guide addressing questions concerning "Beneficial Ownership" that arose from the Wolfsberg AML Principles on Private Banking.
- **Wolfsberg FAQs on Politically Exposed Persons** – A guide addressing frequently asked questions about politically exposed persons (PEPs).
- **Wolfsberg FAQs on Intermediaries** – A guide addressing frequently asked questions about intermediaries.
- **Wolfsberg AML Guidance on Credit/Charge Card Issuing and Merchant Acquiring Activities – May 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 – January 2009** – A guide on the vulnerabilities of trade finance and recommendations on methods for managing these risks.

1390. 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 2010 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: Guide on Non-Conviction Based (NCB) Asset Forfeiture** – A publication 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

1391. 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:

- **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.

1392. 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)
- 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.
    - **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:

- Human Trafficking and Migrant Smuggling
- Criminal Justice, Prison Reform and Crime Prevention
- Organized Crime
- Piracy

For further information, please visit the United Nations Office on Drug and Crime's website at www.unodc.org.

1393. 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.

1394. 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 (CIBO) 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
        - Report on Special Purpose Entities, Joint Forum (IOSCO, BCBS and IAIS)
    - **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)

1395. 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?**
  - **Making Government Anti-Corruption Hotlines Effective**
  - **Corruption and Local Government**
  - **Corruption in the [Middle East and North Africa] MENA Region**
  - **Corruption and Sport: Building Integrity and Preventing Abuses**
  - **Recovering Stolen Assets: A Problem of Scope and Dimension**
  - **Corruption and (In)security**
  - **Accountability and Transparency in Political Finance**
- **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**
  - **Corruption in Judicial Systems**
  - **Political Corruption**
- **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**
  - **Building Corporate Integrity Systems to Address Corruption Risks**
  - **Making Anti-Corruption Regulation Effective for the Private Sector**
  - **Countering Cartels to End Corruption and Protect the Consumer**
  - **Strengthening Corporate Governance to Combat Corruption**
  - **Political Finance Regulations: Bridging the Enforcement Gap**
  - **Effectively Monitoring the United Nations Convention against Corruption (UNCAC)**
  - **Standards on Political Funding and Favours**
- 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.

1396. What guidance has the Egmont Group provided?

Egmont has provided the following guidance:

- **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.

- **FIU Definition "Countering of Terrorism Financing" Complementary Interpretive Note** – A document 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 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.

1397. 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.

1398. How many FIUs are members of the Egmont Group?

As of August 2010, 120 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)
- **China/Hong Kong** – Joint Financial Intelligence Unit (JFIU)
- **Colombia** – Unidad de Informacion y Analisis Financiero (UIAF)
- **Côte d'Ivoire** – National Unit for the Processing of Financial Information in Côte d'Ivoire
- **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
- **India** – Financial Intelligence Unit – India (FIU-IND)
- **Ireland** – An Garda Síochána/Bureau of Fraud Investigation (MLIU)
- **Israel** – Israel Money Laundering Prohibition Authority (IMPA)
- **Italy** – Ufficio Italiano dei Cambi/Servizio Antiriciclaggio – (Italian Foreign Exchange Office/Anti-Money Laundering Service) (UIC/SAR)
- **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

1399. 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 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. Additional information on FATF membership standards and current members is included below.

1400. How does FATF establish international standards for combating money laundering and terrorist financing?

FATF achieves this by creating awareness through its publications, such as *Financial Action Task Force Money Laundering,* various typology and methodology reports, and the *Annual Review of Non-Cooperative Countries and Territories,* and by issuing recommendations – in particular, the Forty Recommendations and the Nine Special Recommendations (also known as "Forty plus Nine Recommendations" or "Recommendations") – aimed at establishing best practices for jurisdictions, regulators and market participants. The Recommendations cover the following general areas of a country's AML infrastructure:

- Legal/criminal justice systems and law enforcement
- Institutional/regulatory system for combating money laundering and terrorist financing
- Preventive measures that should be taken by financial institutions and certain businesses and professionals
- International cooperation

Since their initial issuance, the Forty Recommendations and the Nine Special Recommendations have been revised to reflect changes in money laundering and terrorist financing methods, techniques and trends.

The Recommendations have been recognized by the IMF and the World Bank (WB) and other international organizations as setting international standards for combating money laundering and the financing of terrorism.

1401. How are FATF and the Recommendations relevant to U.S. financial institutions?

The United States is a founding member of FATF and, therefore, a number of U.S. AML statutes and regulations are influenced by the Recommendations.

1402. 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 Cooperation and Development (OECD). The FATF president serves one 12-month term.

1403. 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.

1404. 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 Accion 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)
    - Groupe Inter-gouvernemental d'Action Contre le Blanchiment en Afrique (GIABA)

FATF also has close partnerships with the Offshore Group of Banking Supervisors (OGBS), the IMF, the WB, the U.N., the Egmont Group and other international organizations.

1405. 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. However, many countries have made a political commitment to fight money laundering and terrorist financing by implementing the Recommendations. All potentially suspicious activity should be reported to local investigative authorities (e.g., FinCEN), not to FATF.

1406. 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.

1407. What is a Suspicious Transaction Report (STR)?

An STR is the equivalent of the U.S. Suspicious Activity Report (SAR). If a financial institution detects suspicious activity, it has an obligation to file the report to the respective nation's financial intelligence unit (FIU).

1408. What guidance has FATF provided?

Key publications issued by the FATF include, but are not limited to, the following:

- **Forty Recommendations and the Nine Special Recommendations** – Recommendations that are aimed at establishing AML best practices for jurisdictions, regulators and market participants. For additional guidance, please refer to the Analysis of Forty Recommendations and Nine Special 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. Mutual Evaluation Reports (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.
- **NCCT Annual Report** – A publication created annually that summarizes the progress made by countries previously listed as a non-cooperative country and territory (NCCT). For additional guidance, please refer to the Non-Cooperative Countries and Territories and High-Risk Jurisdictions section.
- **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**
    - **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 Companies 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 TCSP (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**
  - **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**
  - **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.
  - **ML and 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**
    - **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 [WMD]) 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.

Members and Observers

1409. 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 FATF-style regional body (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 an FIU

1410. 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 anti-money laundering 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.

1411. Who is currently a member of FATF?

As of August 2010, 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 Co-operation 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

1412. What is an observer of FATF?

Being an observer can be the first step on the path toward becoming a member of FATF. They include FATF-style regional bodies (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.

1413. 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 its three annual meetings.

1414. Which countries and regional organizations are currently observers of FATF?

As of August 2010, the following countries and regional organizations are observers of FATF:

- 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)
- Basel Committee on Banking Supervision (BCBS)
- Commonwealth Secretariat
- INTERPOL
- INTERPOL/Money Laundering
- 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)
- United Nations (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)

1415. How can a country transition from being an observer to membership in 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.

1416. What are associate members of FATF?

As of August 2010, 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)
- Inter-Governmental Action Group against Money Laundering in West Africa (GIABA)
- Middle East and North Africa Financial Action Task Force (MENAFATF)

1417. 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 August 2010, the 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)
- Inter-Governmental 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

Analysis of Forty Recommendations and Nine Special Recommendations

Definitions

1418. How is the term “financial institution” defined by FATF?

FATF 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

1419. How is the term "designated nonfinancial business and profession" defined by FATF?

FATF 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

1420. 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., a MSB must conduct $1,000 or more in money services business 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.

1421. How is the term "politically exposed person" (PEP) defined by FATF?

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 domestic individuals who hold prominent public positions also should be subject to enhanced due diligence (EDD).

1422. How is the term "designated categories of offenses for money laundering" defined by FATF?

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
- Extortion
- Forgery
- Piracy
- Insider trading and market manipulation

1423. 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.

1424. How is the term "designated threshold" defined by FATF?

FATF defines designated threshold as the minimum amount of a transaction or a series of transactions that should prompt customer due diligence (CDD), recordkeeping and/or suspicious activity reporting requirements.

FATF suggests the following designated thresholds:

- For transactions conducted by financial institutions under Recommendation 5: USD/EUR 15,000

- For transactions conducted by casinos under Recommendation 12: USD/EUR 3,000
- For transactions conducted by dealers in precious metals and stones when engaged in any cash transaction under Recommendations 12 and 16: USD/EUR 15,000

Forty Recommendations

1425. What are the key sections of the FATF's Forty Recommendations?

The FATF's Forty Recommendations are organized into four main categories:

- Legal/criminal justice systems
- Institutional/regulatory system for combating money laundering and terrorist financing
- Preventive measures that should be taken by financial institutions and certain businesses and professionals
- International cooperation

Each section is summarized below:

- **Legal Systems, Recommendations 1 – 3**, provide guidelines on the following:
    - Criminalization of money laundering for all serious offenses
    - Applying the crime of money laundering to a minimum range of predicate offenses that can be defined by category (e.g., racketeering, terrorism, drug trafficking, human trafficking), threshold (e.g., penalty of imprisonment), or a combination of the two
    - Applying the crime of money laundering to predicate offenses occurring in other countries (i.e., dual criminality)
    - Establishment of standards of knowledge (i.e., intent and knowledge required to prove the offense of money laundering) consistent with the Vienna and Palermo conventions
    - Establishment of criminal, civil or administrative liability
    - Enabling of authorities to confiscate (e.g., freeze, seize) property and/or proceeds from money laundering or predicate offenses; countries may choose to allow such confiscation without requiring a criminal conviction
- **Measures to be Taken by Financial Institutions and Nonfinancial Businesses and Professions to Prevent Money Laundering and Terrorist Financing, Recommendations 4 – 25**, provide guidelines on the following:
    - Assurance that secrecy laws do not inhibit the implementation of the Recommendations
    - Prohibition of anonymous accounts or accounts in obviously fictitious names
    - Establishment of risk-based customer due diligence (CDD) measures that identify, verify and monitor customers at various points throughout the relationship (e.g., upon establishing the relationship, when conducting transactions on behalf of the customer above a certain threshold, upon suspicion of money laundering or terrorist financing) for both new and existing customers
    - Establishment of EDD measures for high-risk customers who/that include, but are not limited to, the following:
        - Politically exposed person (PEP)
        - Cross-border correspondent banking
        - Non-face-to-face relationships
    - Establishment of actions (e.g., deny establishing relationship/conducting transaction, terminate the relationship, file a Suspicious Transaction Report [STR]) when unable to comply with due diligence standards
    - Third-party reliance
    - Retention of necessary records for a minimum of five years
    - Monitoring/investigating transaction activity

- Reporting of suspicious transactions to an FIU
- Establishment of safe harbor for financial institutions, directors, officers and employees
- Enforcement of confidentiality of reports of suspicious transactions to the FIU
- Requirements that financial institutions develop AML programs that include the development of policies, procedures and controls, the designation of an AML compliance officer, ongoing AML training, and independent testing
- Requirement that designated nonfinancial businesses and professions (NFBPs) (e.g., lawyers, notaries, accountants, dealers in precious metals and stones, casinos) report suspicious transactions, establish an AML program, and be subject to regulatory supervision
- Establishment of criminal, civil or administrative penalties for noncompliance
- Discontinuance of relationships with shell banks
- Implementation of measures to detect/monitor cross-border transportation of currency and bearer negotiable instruments
- Requirement to report all domestic and international currency transactions above a fixed amount
- Application of special attention to Non-Cooperative Countries and Territories (NCCT)
- Application of AML requirements to branches/subsidiaries located abroad
- Requirement of licensing/registration of financial institutions
- Establishment of guidelines and provision of feedback by regulatory authorities to assist financial institutions in applying national measures to combat money laundering and terrorist financing

- **Institutional and Other Measures Necessary in Systems for Combating Money Laundering and Terrorist Financing, Recommendations 26 – 34**, provide guidelines on the following:
  - Establishment of a financial intelligence unit (FIU)
  - Assignment of law enforcement authorities to money laundering and terrorist financing investigations
  - Establishment of mechanism(s) to share information
  - Authorization to monitor and ensure compliance with national measures to combat money laundering and terrorist financing
  - Provision of statistics on matters relevant to the effectiveness and efficiency of national measures to combat money laundering and terrorist financing
  - Transparency of legal persons/legal arrangements, such as information on beneficial ownership
- **International Cooperation, Recommendations 35 – 40**, provide guidance on mutual legal assistance, international cooperation and extradition.

1426. Are the Forty Recommendations applicable only to financial institutions?

No. The Forty Recommendations are applicable to DNFBPs and regulatory and law enforcement authorities in addition to financial institutions.

1427. Which of the Forty 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 – 25.

1428. What sources does FATF suggest a financial institution use to perform due diligence on its customers?

FATF suggests that a financial institution can obtain relevant information from the customer, from public sources, or from sources deemed as reliable by the financial institution.

1429. Under what circumstances does FATF suggest simplified or reduced CDD measures be applied?

In circumstances where the money laundering and terrorist financing risk is lower, it would be reasonable for a financial institution to apply simplified CDD. Examples where simplified CDD measures could apply would include the following types of customers:

- Financial institutions subject to AML requirements consistent with the Recommendations
- Public companies
- Government administrations or enterprises
- Customers with certain products/transactions (e.g., life insurance policies where the annual premium is under a predetermined threshold, insurance policies for pension schemes if there is no surrender clause)

Nine Special Recommendations

1430. What are the Nine Special Recommendations?

The Nine Special Recommendations are summarized below:

- The ratification and implementation of the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism
- The criminalization of terrorist financing and associated money laundering
- The freezing and confiscation of terrorist assets
- The reporting of suspicious transactions to authorities
- The international cooperation in regards to legal/investigative action relating to terrorist financing activity
- The assurance that money transmitters are licensed and registered
- Accurate originator information on fund transfers
- The assurance that nonprofit organizations are not misused or exploited
- Countries should apply measures to detect, restrain and punish the physical cross-border transportation of currency and bearer negotiable instruments

1431. FATF has issued guidance showing both Eight Special Recommendations and Nine Special Recommendations. How many Special Recommendations are there?

Following the September 11 terrorist attacks, FATF issued Eight Special Recommendations on October 1, 2001. A ninth recommendation, which focuses on the cross-border transfer of currency and monetary instruments and the ability to monitor their movement, was added on October 22, 2004.

1432. Are the Nine Special Recommendations applicable only to financial institutions?

No. The Nine Special Recommendations are applicable to DNFBPs and regulatory and law enforcement authorities in addition to financial institutions.

Non-Cooperative Countries and Territories and High-Risk Jurisdictions

1433. What are Non-Cooperative Countries and Territories (NCCTs)?

NCCTs are jurisdictions designated by FATF that have detrimental rules and practices that seriously hamper the international fight against money laundering and terrorist financing.

1434. What are the consequences of being on the NCCT list?

Recommendation 21 requires countries to pay considerable attention when building business relationships or conducting transactions with any person, company, or financial institution from a country or territory – including one that is listed as an NCCT – that does not or insufficiently applies the FATF Recommendations. A jurisdiction's inclusion on the NCCT list 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 NCCT not taking the necessary steps to correct their AML deficiencies.

A financial institution in the United States should review the NCCT list, as well as FATF Public Statements on high-risk jurisdictions (described below) 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 program.

1435. What additional countermeasures did FATF suggest to take against NCCTs beyond Recommendation 21?

FATF suggested implementing the following countermeasures against NCCTs:

- EDD requirements on customers and beneficial owners of individuals or businesses within NCCTs before establishing account relationships
- More intensive monitoring of transactions involving NCCTs
- Consideration of NCCT location of relevant 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 NCCTs

1436. What is a "high-risk jurisdiction" with respect to FATF's NCCT process?

High-risk jurisdictions are countries and territories that have strategic deficiencies in their AML/CFT infrastructure that may or may not be official members or observers of FATF. These high-risk jurisdictions are identified in public statements issued by FATF that include suggested measures for mitigating risks associated with transactions involving these jurisdictions.

1437. What is the difference between a "high-risk jurisdiction" and an NCCT?

FATF has not articulated a clear distinction between a "high-risk jurisdiction" and an NCCT. 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 an NCCT.

1438. What are the consequences of being designated as a high-risk jurisdiction?

The response by the international community may be very similar to that for NCCTs, though FATF, in all but one case, has specifically called for enhanced scrutiny rather than countermeasures in the case of high-risk jurisdictions. The lone exception to this method of response is the case of Iran: on several occasions since 2008, FATF has urged its members to apply countermeasures to protect their financial services sectors from money laundering and terrorist financing originating from that jurisdiction. The call for countermeasures against Iran was renewed in both February and June 2010.

1439. When did the NCCT process 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.

1440. What is the process of designating a jurisdiction as an NCCT?

FATF reviews select countries and territories against 25 criteria to assess their AML infrastructure. Findings from the review are submitted as a draft report and discussed at FATF's plenary meetings with the country under review.

Example criteria used to designate NCCTs can be grouped in the following categories:

- Loopholes in financial regulations (e.g., absence of or inadequate CDD, recordkeeping and suspicious activity reporting regulations, absence of or inadequate supervision of financial institutions, secrecy provisions that hinder investigations)
- Obstacles raised by other regulatory requirements (e.g., absence of or inadequate regulations to require registration of businesses and legal entities and identification of beneficial owners)
- Obstacles to international cooperation (e.g., prohibitive laws, evidence of unwillingness to cooperate with other jurisdictions, failure to criminalize money laundering)
- Inadequate resources for preventing and detecting money laundering activities (e.g., lack of resources in the public and private sector)

For a complete listing of the 25 criteria used to designate NCCTs, please review any one of the series of Reports on Non-Cooperative Countries and Territories published by FATF.

1441. How are countries and territories selected for review?

Countries are selected for review based on FATF members' experience. Generally, larger financial centers and countries with a history of being uncooperative were reviewed first. However, FATF cautions that certain jurisdictions with deficient anti-money laundering regimes may not be selected for review because they are not prioritized by FATF members.

1442. Who conducts the NCCT review of selected countries and territories?

FATF established regional groups (i.e., 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 to conduct the NCCT reviews.

What countries and territories have been listed as NCCTs?

Of the 47 jurisdictions examined in 2000 and 2001, 23 were listed as NCCTs – 15 in 2000 and an additional eight in 2001:

- Bahamas (2000)
- Cayman Islands (2000)
- Cook Islands (2000)
- Dominica (2000)
- Egypt (2001)
- Grenada (2001)
- Guatemala (2001)
- Hungary (2001)
- Indonesia (2001)
- Israel (2000)
- Lebanon (2000)
- Liechtenstein (2000)
- Marshall Islands (2000)
- Myanmar (2001)
- Nauru (2000)
- Nigeria (2001)
- Niue (2000)
- Panama (2000)
- Philippines (2000)
- Russia (2000)
- St. Kitts and Nevis (2000)
- St. Vincent and the Grenadines (2000)
- Ukraine (2001)

1443. What countries and territories are currently on the NCCT list?

As of October 13, 2006, when Myanmar was removed, there were no countries or territories remaining on the NCCT list.

1444. When did FATF last review new countries and territories for designation as an NCCT?

FATF has not designated any new jurisdictions since 2001. However, FATF continues to monitor countries and territories working to combat money laundering and terrorist financing and will act swiftly to designate an NCCT or a high-risk jurisdiction if it poses a threat to the global monetary system.

1445. Has FATF recently highlighted any high-risk jurisdictions of concern?

As of June 2010, FATF has issued statements of concern for the following countries and territories:

- Iran
- Democratic People's Republic of Korea (DPRK)
- São Tomé and Príncipe

Jurisdictions previously identified as high risk that have since made commitments to enhance their AML/CFT infrastructure include the following:

- Angola
- Antigua and Barbuda
- Azerbaijan
- Bolivia
- Ecuador
- Ethiopia
- Greece
- Indonesia
- Kenya
- Morocco
- Myanmar
- Nepal
- Nigeria
- Pakistan
- Paraguay
- Qatar
- Sri Lanka
- Sudan
- Syria
- Thailand
- Trinidad and Tobago
- Turkey
- Turkmenistan
- Yemen

1446. How is a country or territory removed from the NCCT or high-risk jurisdiction list?

Once designated as an NCCT, a jurisdiction must periodically report on its progress in plenary meetings (e.g., recent AML reforms, implementation plans) in order to have the designation removed. Of particular importance are reforms in the area of criminal law, financial supervision, customer identification, suspicious transaction reporting and international cooperation.

FATF established the International Co-operation Review Group (ICRG) specifically to engage NCCTs and high-risk jurisdictions, including members and non-members, and to assist them with complying with international AML/CFT standards.

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, a recommendation for delisting is made at a plenary meeting.

1447. Are recently delisted countries or territories subject to monitoring by FATF?

Yes. Recently delisted countries are subject to formal monitoring by FATF. This process, similar to the delisting process, involves the submission of progress reports, implementation plans of current and secondary regulations and periodic site visits, as well. Subjects of the monitoring include inspections of financial institutions; implementation of suspicious transaction reporting systems; performance of investigations and prosecutions related to money laundering; establishment of a regulatory financial intelligence unit, with judicial cooperation; and assessment of compliance culture in relevant sectors.

1448. Can a financial institution assume that a country is compliant with the Recommendations or has a strong AML infrastructure if it is not listed as an NCCT or high-risk jurisdiction?

No. The mutual evaluation process specifically assesses compliance with the Recommendations of member countries.

1449. What publications has FATF issued with regard to NCCTs and high-risk jurisdictions?

FATF has published an Annual Review of Non-Cooperative Countries and Territories, which provides information regarding actions taken within the NCCT program in the past year, including strategies going forward. FATF published the most recent report of this nature on October 12, 2007—no annual NCCT reports have since been published.

FATF also releases public statements identifying high-risk 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.

Mutual Evaluations

1450. How does FATF ensure that all its member countries are in compliance with the Recommendations?

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.

1451. 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 assessment methodology used in evaluations/assessments, descriptions of what is necessary for an effective AML/CFT program, and guidance and interpretation concerning the methodology.

1452. What is the process for mutual evaluations?

The mutual evaluation process is designed to measure and evaluate the implementation progress of the Forty plus Nine Recommendations. It 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 mutual evaluation report (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

1453. 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 and draft the preliminary and final report 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.

1454. 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 also having experience with both financial institutions and designated nonfinancial businesses and professions (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.

1455. 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.

1456. 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.

1457. Are the results of the mutual evaluation available to the public?

Yes. Although this was not the case initially, in 2005, FATF began publishing the MERs on its website: www.fatf-gafi.org.

1458. What are key factors used when assessing compliance with the Forty plus Nine Recommendations?

It is important to note that the FATF's 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 (ML) and terrorist financing (TF) predicate offenses
- Evidentiary standards applied to ML/TF 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 ML/TF investigations initiated
- Number of prosecutions

- Number of convictions
- Existence of penalties for failures of noncompliance
- 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

1459. What rating scale is used to assess compliance with the Forty plus Nine Recommendations?

FATF uses the following rating scale to assess compliance with the Forty plus Nine 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

1460. What have been the results of MERs conducted in recent years?

Based on mutual evaluation reports (MERs) conducted between 2005 and 2010 on the following 31 countries – Australia, Austria, Belgium, Brazil, Canada, China, Finland, Germany, Greece, Hong Kong, Kingdom of Denmark, Iceland, India, Ireland, Italy, Japan, 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	10%	58%	32%	0%	0%
R2	Money Laundering Offense – Mental Element and Corporate Liability	19%	58%	23%	0%	0%
R3	Confiscation and Provisional Measures	23%	55%	23%	0%	0%
R4	Secrecy Laws Consistent with the Recommendations	74%	16%	10%	0%	0%
R5	Customer Due Diligence	0%	10%	74%	16%	0%
R6	Politically Exposed Persons	0%	23%	16%	61%	0%
R7	Correspondent Banking	10%	19%	19%	52%	0%
R8	New Technologies and Non-Face-to-Face Business	19%	32%	35%	13%	0%
R9	Third Parties and Introducers	3%	16%	26%	29%	26%
R10	Recordkeeping	45%	45%	10%	0%	0%
R11	Unusual Transactions	13%	29%	45%	13%	0%
R12	Designated Nonfinancial Businesses and Professions – R.5, 6, 8-11	0%	0%	35%	65%	0%
R13	Suspicious Transaction Reporting	6%	48%	45%	0%	0%
R14	Protection and No Tipping-Off	65%	26%	10%	0%	0%
R15	Internal Controls, Compliance and Audit	0%	55%	35%	10%	0%
R16	Designated Nonfinancial Businesses and Professions – R.13-15, 21	0%	10%	42%	48%	0%
R17	Sanctions	0%	32%	65%	3%	0%
R18	Shell Banks	23%	26%	48%	3%	0%
R19	Other Forms of Reporting	87%	3%	6%	3%	0%
R20	Other Nonfinancial Businesses and Professions and Secure Transaction Techniques	68%	26%	3%	3%	0%
R21	Special Attention for Higher Risk Countries	10%	26%	39%	26%	0%
R22	Foreign Branches and Subsidiaries	6%	35%	29%	29%	0%
R23	Regulation, Supervision and Monitoring	0%	32%	65%	3%	0%
R24	Designated Nonfinancial Businesses and Professions – Regulation, Supervision and Monitoring	0%	6%	29%	65%	0%
R25	Guidelines and Feedback	13%	35%	39%	13%	0%
R26	Financial Intelligence Unit	13%	71%	13%	3%	0%
R27	Law Enforcement Authorities	35%	55%	10%	0%	0%
R28	Powers of Competent Authorities	74%	26%	0%	0%	0%
R29	Supervisors	6%	55%	35%	3%	0%

No.	Recommendation	Compliant	Largely Compliant	Partially Compliant	Noncompliant	N/A
R30	Resources, Integrity and Training	3%	45%	48%	3%	0%
R31	National Cooperation	19%	74%	6%	0%	0%
R32	Statistics	0%	48%	45%	6%	0%
R33	Legal Persons – Beneficial Owners	3%	6%	58%	32%	0%
R34	Legal Arrangements – Beneficial Owners	0%	3%	42%	19%	35%
R35	Conventions	6%	52%	42%	0%	0%
R36	Mutual Legal Assistance	23%	71%	6%	0%	0%
R37	Dual Criminality	65%	29%	6%	0%	0%
R38	Mutual Legal Assistance on Confiscation and Freezing	26%	61%	13%	0%	0%
R39	Extradition	29%	68%	3%	0%	0%
R40	Other Forms of International Cooperation	48%	48%	3%	0%	0%
SR1	Implement United Nations Instruments	3%	32%	61%	3%	0%
SR2	Criminalize Terrorist Financing	13%	48%	35%	3%	0%
SR3	Freeze and Confiscate Terrorist Assets	3%	23%	61%	13%	0%
SR4	Suspicious Transaction Reporting	13%	52%	29%	6%	0%
SR5	International Cooperation	10%	71%	19%	0%	0%
SR6	AML Requirements for Money/Value Transfer Services	6%	39%	42%	13	0%
SR7	Wire Transfer Rules	6%	26%	35%	32%	0%
SR8	Nonprofit Organizations	10%	32%	42%	16%	0%
SR9	Cross-Border Declaration and Disclosure	10%	23%	42%	26%	0%

The following areas are some of the common deficiencies that have been identified in the MERs:

- Ineffective customer due diligence (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 risk associated with correspondent banking customers
- Inadequate processes to identify and manage risks associated with politically exposed persons (PEPs)
- Inadequate processes to manage risk 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 designated nonfinancial businesses and professions (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 the 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 counterpart's use of information, precondition of treaty, dual criminality stipulation)

1461. 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
- 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

1462. What were the key findings of the mutual evaluation of the United States conducted in 2006?

The United States was rated compliant with 30 percent of the recommendations, largely compliant with 57 percent, partially compliant with 4 percent and noncompliant with 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 last 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.

Key statistics provided in the MER included the following for fiscal year 2005:

- At the federal level, 1,075 defendants were convicted of money laundering violations.
- 54 defendants were convicted of terrorist financing offenses; an additional 72 cases were pending.
- $764.4 million was seized.
- $12.5 million in terrorist-related assets was frozen/blocked.

Specific areas highlighted as needing improvement included CDD 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).

ACRONYMS AND GLOSSARY

Acronyms	
ABA	American Bankers Association
ACH	Automated Clearing House
ACSSS	American Council of State Savings Supervisors
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
APG	Asia/Pacific Group on Money Laundering
APO	Army Post Office
APT	Asset Protection Trust
ATA	Anti-Terrorism Assistance Program
ATM	Automated Teller Machine
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
BMPE	Black Market Peso Exchange
BOE	Bank of England
BPI	Bribe Payers Index
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

Acronyms	
CCL	The Commerce Control List
CCS	Commercial Crime Services
CDD	Customer Due Diligence
CEA	Commodity Exchange Act
CFATF	Caribbean Financial Action Task Force
CFR	Code of Federal Regulations
CFTC	Commodities Futures Trading Commission
CIA	Central Intelligence Agency
CIBO	Customer Identification Beneficial Ownership
CIP	Customer Identification Program
CISADA	Comprehensive Iran Sanctions, Accountability and Divestment Act
CMIR	Report of International Transportation of Currency or Monetary Instruments
CMP	Civil Money Penalty
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
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
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
DOEP	Designation of Exempt Person
DOJ	Department of Justice
DOS	Department of State
DOT	Department of The Treasury
DPA	Deferred Prosecution Agreement
DPL	Denied Persons List
EAG	Eurasian Group on Combating Money Laundering and Financing Of Terrorism

Acronyms	
EAR	Export Administration Regulation
EB	Bureau of Economic and Business Affairs
EDD	Enhanced Due Diligence
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
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
FDIC	Federal Deposit Insurance Corporation
FEST	Foreign Emergency Support Team
FFIEC	Federal Financial Institutions Examination Council
FI	Financial Institution
FINCEN	Financial Crimes Enforcement Network
FINRA	Financial Industry Regulatory Authority
FIU	Financial Intelligence Unit
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
GAFISUD	Financial Action Task Force of South America Against Money Laundering
GAO	Government Accountability Office
GCB	Global Corruption Barometer
GDP	Gross Domestic Product
GTFP	The Global Trade Finance Program
GIABA	Groupe Inter-Gouvernemental D'action Contre Le Blanchiment En Afrique
GTO	Geographic Targeting Order
GUI	Graphical User Interface
HIDTA	High Intensity Drug Trafficking Area

Acronyms	
HIFCA	High Risk Money Laundering and Related Financial Crimes Area
HKMA	Hong Kong Monetary Authority
IAIS	International Association of Insurance Supervisors
IB	Introducing Broker
IBC	International Business Corporation
ICC	International Chamber of Commerce
ICE	Immigration and Customs Enforcement
IFC	International Finance Corporation
IEEPA	International Emergency Economic Powers Act
IGRE ACT	Internet Gambling Regulation and Enforcement Act
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
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
ISO	Independent Sales Organization
IT	Information Technology
ITAR	International Traffic In Arms Regulations
ITPP	Identity Theft Prevention Program
IVTS	Informal Value Transfer System
JFIU	Joint Financial Intelligence Unit (Hong Kong)
KYC	Know Your Customer
LC	Letter of Credit
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

Acronyms	
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
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
NCTC	National Counterterrorism Center
NCUA	National Credit Union Association
NDIC	National Drug Intelligence Center
NDIP	Non Deposit Investment Product
NFA	National Futures Association
NGA	National Geospatial – Intelligence Agency
NGO	Nongovernmental Organization
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

Acronyms	
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 Internal Affairs
OIA	Office of Intelligence and Analysis, Criminal Division
ONDCP	Office of National Drug Control Policy
OSFI	Office of the Superintendent of Financial Institutions
OTP	One Time Passwords
OTS	Office of Thrift Supervision
PACS	PATRIOT Act Communication System
PASPA	Professional and Amateur Sports Protection Act of 1992
PEP	Politically Exposed Person
PFUIG	Prohibition on Funding of Unlawful Internet Gambling
PIC	Private Investment Company
PIN	Personal Identification Numbers
POB	Place of Birth
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
S/CT	State's Office of the Coordinator for Counterterrorism
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 Service 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

Acronyms	
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
TBML	Trade Based Money Laundering
TBML/FT	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
TOPOFF	Top Officials
TPSP	Third-Party Service Provider
TTU	Trade Transparency Units
UIGE Act	Unlawful Internet Gambling Enforcement Act Of 2006
UN	United Nations
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
USC	United States Code
USML	U.S. Munitions List
USSS	United States Secret Service
WB	World Bank
WCO	World Customs Organisation
WGEI	Working Group on Evaluations and Implementation
WTO	World Trade Organisation

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.
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.
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.

Glossary of Select Key Terms	
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.
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.
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.

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, redeemer or cashier of traveler's checks, 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 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.
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 Fund 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.

Glossary of Select Key Terms	
Futures Commission Merchant (FCM)	An FCM is a person or entity registered, or required to register, as an FCM with the Commodities 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.
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.
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.
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.
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.

Glossary of Select Key Terms	
Money services business (MSB)	Any organization offering one or more of the following services is classified as a MSB: • Issuer, seller or redeemer of money orders • Issuer, seller or redeemer of traveler's checks • Check casher • Currency dealer or exchanger • Issuer, seller or redeemer of stored-value cards • 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) 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 Institution 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.
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.

Glossary of Select Key Terms	
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.
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.
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.

Glossary of Select Key Terms	
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. For further guidance on safe harbor, please see the Safe Harbor section.
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.
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 National 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, also 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 Money Services Businesses.
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 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

Key U.S. AML Laws and Regulations	
12 USC 1952	Reports on ownership and control
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 301	Short title
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

Key U.S. AML Laws and Regulations	
Title III: Subtitle B: Section 352	Anti-money laundering programs (AML programs)
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 103	Financial recordkeeping and reporting of currency and foreign transactions
31 CFR 103.11, 31 CFR 103.90, 31 CFR 103.175	Meaning of terms/definitions
31 CFR 103.15	Reports by mutual funds of suspicious transactions (SAR)
31 CFR 103.16	Reports by insurance companies of suspicious transactions (SAR)
31 CFR 103.17	Reports by futures commission merchants and introducing brokers in commodities of suspicious transactions (SAR)
31 CFR 103.18	Reports by banks of suspicious transactions (SAR)

Key U.S. AML Laws and Regulations	
31 CFR 103.19	Reports by brokers or dealers in securities of suspicious transactions (SAR)
31 CFR 103.20	Reports by money services businesses (MSB) of suspicious transactions (SAR)
31 CFR 103.21	Reports by casinos of suspicious transactions (SAR)
31 CFR 103.22	Reports of transactions in currency (CTR)
31 CFR 103.22(d)	Transactions of exempt persons (CTR exemptions)
31 CFR 103.23	Reports of transportation of currency or monetary instruments (CMIR)
31 CFR 103.24	Reports of foreign bank and financial accounts (FBAR)
31 CFR 103.25	Reports of transactions with foreign financial agencies
31 CFR 103.26	Reports of certain domestic coin and currency transactions
31 CFR 103.27	Filing of reports (CTR, CMIR, FBAR)
31 CFR 103.29	Purchases of bank checks and drafts, cashier's checks, money orders and traveler's checks
31 CFR 103.30	Reports relating to currency in excess of $10,000 received in a trade or business (Form 8300)
31 CFR 103.33	Records to be made and retained by financial institutions (funds transfer recordkeeping and transmittal requirements)
31 CFR 103.34	Additional records to be made and retained by banks
31 CFR 103.35	Additional records to be made and retained by brokers or dealers in securities
31 CFR 103.36	Additional records to be made and retained by casinos
31 CFR 103.37	Additional records to be made and retained by currency dealers or exchangers
31 CFR 103.38	Nature of records and retention period
31 CFR 103.41	Registration of money services businesses (MSB)
31 CFR 103.57	Civil penalty
31 CFR 103.59	Criminal penalty
31 CFR 103.63	Structured transactions
31 CFR 103.64	Special rules for casinos
31 CFR 103.100	Information sharing between federal law enforcement agencies and financial institutions (314(a))
31 CFR 103.110	Voluntary information sharing among financial institutions (314(b))
31 CFR 103.120	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 103.121	Customer identification programs for banks, savings associations, credit unions, and certain nonfederally regulated banks (CIP)
31 CFR 103.122	Customer identification programs for broker-dealers (CIP)
31 CFR 103.123	Customer identification programs for futures commission merchants and introducing brokers (CIP)
31 CFR 103.125	Anti-money laundering programs for money services businesses (MSB) (AML program)
31 CFR 103.130	Anti-money laundering programs for mutual funds (AML program)
31 CFR 103.131	Customer identification programs for mutual funds (CIP)
31 CFR 103.135	Anti-money laundering programs for operators of credit card systems (AML program)
31 CFR 103.137	Anti-money laundering programs for insurance companies (AML program)

Key U.S. AML Laws and Regulations	
31 CFR 103.140	Anti-money laundering programs for dealers in precious metals, precious stones or jewels (AML program)
31 CFR 103.170	Exempted anti-money laundering programs for certain financial institutions
31 CFR 103.176	Due diligence programs for correspondent accounts for foreign financial institutions
31 CFR 103.177	Prohibition on correspondent accounts for foreign shell banks; records concerning owners of foreign banks and agents for service of legal process
31 CFR 103.178	Due diligence programs for private banking accounts
31 CFR 103.185	Summons or subpoena of foreign bank records; termination of correspondent relationship
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
12 CFR 500	Foreign assets control regulations (OFAC)
12 CFR 500.101	Relation of this part to other laws and regulations
12 CFR 500.201	Transactions involving designated foreign countries or their nationals
12 CFR 500.202	Transactions with respect to securities registered or inscribed in the name of a designated national
12 CFR 500.203	Effect of transfers violating the provisions of this chapter
12 CFR 500.204	Importation of and dealings in certain merchandise
12 CFR 500.205	Holding of certain types of blocked property in interest-bearing accounts
12 CFR 500.206	Exemption of information and informational materials
12 CFR 500.301	Foreign country
12 CFR 500.302	National
12 CFR 500.303	Nationals of more than one foreign country
12 CFR 500.305	Designated national
12 CFR 500.306	Specially designated national
12 CFR 500.307	Unblocked national
12 CFR 500.308	Person
12 CFR 500.309	Transactions
12 CFR 500.310	Transfer
12 CFR 500.311	Property; property interests
12 CFR 500.312	Interest
12 CFR 500.313	Property subject to the jurisdiction of the United States
12 CFR 500.314	Banking institution
12 CFR 500.316	License
12 CFR 500.317	General license
12 CFR 500.318	Specific license
12 CFR 500.319	Blocked account

Key U.S. AML Laws and Regulations	
12 CFR 500.320	Domestic bank
12 CFR 500.321	United States; continental United States
12 CFR 500.322	Authorized trade territory; member of the authorized trade territory
12 CFR 500.323	Occupied area
12 CFR 500.325	National Securities Exchange
12 CFR 500.326	Custody of safe deposit boxes
12 CFR 500.327	Blocked estate of a decedent
12 CFR 500.328	Status of those portions of Korea under control of the government of the Republic of Korea; and of the diplomatic and consular representatives of those countries
12 CFR 500.329	Person subject to the jurisdiction of the United States
12 CFR 500.330	Person Within the United States
12 CFR 500.331	Merchandise
12 CFR 500.332	Information and informational materials
12 CFR 500.401	Reference to amended sections
12 CFR 500.402	Effect of amendment of sections of this chapter or of other orders
12 CFR 500.403	Termination and acquisition of the interest of a designated national
12 CFR 500.404	Transactions between principal and agent
12 CFR 500.405	Exportation of securities, etc., to designated foreign countries
12 CFR 500.406	Drafts under irrevocable letters of credit; documentary drafts
12 CFR 500.407	Administration of blocked estates of decedents
12 CFR 500.408	Access to certain safe deposit boxes prohibited
12 CFR 500.409	Certain payments to designated foreign countries and nationals through third countries
12 CFR 500.410	Currency, coins and postage and other stamps
12 CFR 500.411	Dealings abroad in commodities subject to the regulations
12 CFR 500.412	Process vs. manufacture
12 CFR 500.413	Participation in certain development projects in Vietnam
12 CFR 500.501	General and specific licensing procedures
12 CFR 500.502	Effect of subsequent license or authorization
12 CFR 500.503	Exclusion from licenses and authorizations
12 CFR 500.504	Certain judicial proceedings with respect to property of designated nationals
12 CFR 500.505	Certain persons unblocked
12 CFR 500.508	Payments to blocked accounts in domestic banks
12 CFR 500.509	Entries in certain accounts for normal service charges
12 CFR 500.510	Payments to the United States, states and political sub-divisions
12 CFR 500.511	Transactions by certain business enterprises
12 CFR 500.513	Purchase and sale of certain securities
12 CFR 500.514	Payment of dividends and interest on and redemption and collection of securities
12 CFR 500.515	Transfers of securities to blocked accounts in domestic banks
12 CFR 500.516	Voting and soliciting of proxies on securities

Key U.S. AML Laws and Regulations	
12 CFR 500.517	Access to safe deposit boxes under certain conditions
12 CFR 500.518	Payments for living, traveling and similar personal expenses in the United States
12 CFR 500.519	Limited payments from accounts of United States citizens abroad
12 CFR 500.520	Payments from accounts of United States citizens in employ of United States in foreign countries and certain other persons
12 CFR 500.521	Certain remittances for necessary living expenses
12 CFR 500.522	Certain remittances to United States citizens in foreign countries
12 CFR 500.523	Transactions incident to the administration of decedents' estates
12 CFR 500.524	Payment from, and transactions in the administration of certain trusts and estates
12 CFR 500.525	Certain transfers by operation of law
12 CFR 500.526	Transactions involving blocked life insurance policies
12 CFR 500.527	Certain transactions with respect to United States patents, trademarks and copyrights
12 CFR 500.528	Certain transactions with respect to blocked foreign patents, trademarks and copyrights authorized
12 CFR 500.529	Powers of attorney
12 CFR 500.530	Exportation of powers of attorney or instructions relating to certain types of transactions
12 CFR 500.533	Exportations, re-exportations and incidental transactions
12 CFR 500.535	Exchange of certain securities
12 CFR 500.536	Certain transactions with respect to merchandise affected by 12 CFR 500.204
12 CFR 500.549	Proof of origin
12 CFR 500.550	Transactions related to information and informational materials
12 CFR 500.551	Reimports
12 CFR 500.552	Research samples
12 CFR 500.553	Prior contractual commitments not a basis for licensing
12 CFR 500.554	Gifts of North Korean, North Vietnamese, Cambodian or South Vietnamese origin
12 CFR 500.556	Joint bank accounts
12 CFR 500.557	Proceeds of insurance policies
12 CFR 500.558	Accounts of blocked partnerships
12 CFR 500.559	Accounts of North Korean, North Vietnamese, Cambodian or South Vietnamese sole proprietorships
12 CFR 500.560	Bank accounts of official representatives of foreign governments in North Korea, North Vietnam, Cambodia or South Vietnam
12 CFR 500.561	Transfers of abandoned property under state laws
12 CFR 500.563	Transactions incident to travel to and within North Korea
12 CFR 500.565	Family remittances to nationals of Vietnam and Cambodia
12 CFR 500.566	Certain transactions authorized on behalf of North Korean nationals incident to their travel and maintenance expenses
12 CFR 500.567	U.S. assets of certain designated country corporations
12 CFR 500.568	U.S. assets of blocked decedents
12 CFR 500.570	Cambodian property unblocked

Key U.S. AML Laws and Regulations	
12 CFR 500.571	Transactions related to telecommunications authorized
12 CFR 500.572	Humanitarian projects authorized
12 CFR 500.573	Certain donations of funds and goods to meet basic human needs authorized
12 CFR 500.574	Executory contracts and related transactions authorized
12 CFR 500.575	Certain services to Vietnamese nationals authorized
12 CFR 500.576	Authorization of transactions concerning certain development projects in Vietnam
12 CFR 500.577	Authorization of bank transactions with respect to Vietnam by certain international organizations
12 CFR 500.578	Vietnamese property unblocked
12 CFR 500.579	Authorization for release of certain blocked transfers by banking institutions subject to U.S. jurisdiction
12 CFR 500.580	Authorization of U.S. dollar clearing transactions involving North Korea
12 CFR 500.581	Financial transactions related to diplomatic missions authorized
12 CFR 500.582	Importation of North Korean-origin magnesite and magnesia
12 CFR 500.583	News organization offices
12 CFR 500.584	Energy sector projects in North Korea
12 CFR 500.585	Payments for services rendered by North Korea to United States aircraft authorized
12 CFR 500.586	Authorization of new transactions concerning certain North Korean property
12 CFR 500.601	Records and reports
12 CFR 500.602	Reporting of claims of U.S. nationals against North Korea
12 CFR 500.701	Penalties
12 CFR 500.801	Procedures
12 CFR 500.802	Delegation by the Secretary of the Treasury
12 CFR 500.803	Customs procedures; merchandise specified in 12 CFR 500.204
31 CFR 132	Prohibition on funding of unlawful Internet gambling

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
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

Useful Websites	
Customs and Border Protection (CBP)	www.cbp.gov
Department of Homeland Security (DHS)	www.dhs.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
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 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
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

Useful Websites	
Office of Terrorism and Financial Intelligence (OTFI)	www.treas.gov/offices/enforcement/
Office of the Comptroller of the Currency (OCC)	www.occ.treas.gov
Office of Thrift Supervision (OTS)	www.ots.treas.gov
Organisation for Economic Co-operation and Development (OECD)	www.oecd.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
The 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
Trade Transparency Unit	www.ice.gov/partners
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 business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. We help solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Our highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: 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, and implementation support. Whether Protiviti selects and/or consults on your automated AML system, we can maximize its benefits.

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
Vienna
Woodbridge

BRAZIL

São Paulo*

CANADA

Kitchener-Waterloo
Toronto

MEXICO

Mexico City

PERU

Lima*

VENEZUELA

Caracas*

ASIA-PACIFIC

AUSTRALIA

Brisbane
Canberra
Melbourne
Sydney

CHINA

Beijing
Hong Kong
Shanghai
Shenzhen

INDIA

Mumbai
New Delhi

INDONESIA

Jakarta**

JAPAN

Osaka
Tokyo

SINGAPORE

Singapore

SOUTH KOREA

Seoul

* Protiviti Member Firm
** Protiviti Alliance Member

EUROPE

BELGIUM

Brussels

FRANCE

Paris

GERMANY

Frankfurt
Munich

ITALY

Milan
Rome
Turin

SPAIN

Madrid

THE NETHERLANDS

Amsterdam

UNITED KINGDOM

London

MIDDLE EAST

BAHRAIN

Bahrain*

KUWAIT

Kuwait City*

OMAN

Muscat*

UNITED ARAB EMIRATES

Abu Dhabi*
Dubai*

protiviti®
Risk & Business Consulting.
Internal Audit.