Federal Financial Institutions Examination Council

Bank Secrecy Act Anti-Money Laundering Examination Manual

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision

Bank Secrecy Act Anti-Money Laundering Examination Manual

June 2005

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Table of Contents

EXPANDED OVERVIEW

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Introduction

This Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act (BSA) /Anti-Money Laundering (AML) Examination Manual provides guidance to examiners for carrying out BSA/AML and Office of Foreign Assets Control (OFAC) examinations. An effective BSA/AML compliance program requires sound risk management; therefore, the manual also provides guidance on identifying and controlling risks associated with money laundering and terrorist financing. The manual contains an overview of BSA/AML compliance program requirements, BSA/AML risks and risk management expectations, industry sound practices, and examination procedures. The development of this manual was a collaborative effort of the federal banking agencies[1] and the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, to ensure consistency in the application of the BSA/AML requirements. In addition, OFAC assisted in the development of the sections of the manual that relate to OFAC reviews. Refer to Appendices A ("BSA Laws and Regulations"), B ("BSA/AML Directives"), and C ("BSA/AML References") for guidance.

STRUCTURE OF MANUAL

In order to effectively apply resources and ensure compliance with BSA requirements, the manual is structured to allow examiners to tailor the BSA/AML examination scope and procedures to the specific risk profile of the banking organization. The manual consists of the following sections:

- Introduction.
- Core: Overview and Procedures.
- Expanded: Overview and Procedures.
- Appendices.

The core and expanded overview sections provide narrative guidance and background information on each topic; the procedures provide examiner guidance. The core sections serve as a platform for the BSA/AML examination and, for the most part, address legal and regulatory requirements of the BSA/AML compliance program. The scoping and planning section helps the examiner develop an appropriate examination plan. There may be instances where a topic is covered in both the core and expanded sections (e.g., funds transfers and foreign correspondent banking). In such instances, the core overview

[1] The five federal banking agencies that are members of the FFIEC are the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

and procedures address the BSA requirements while the expanded overview and procedures address the AML risks of the specific activity.

At a minimum, examiners should use the procedures included in the following core sections of this manual to ensure that the bank has an adequate BSA/AML compliance program commensurate with its risk profile:

- Scoping and Planning (refer to pages 170 to 173).
- BSA/AML Compliance Program (refer to pages 174 to 178).
- Developing Conclusions and Finalizing the Examination (refer to pages 210 to 213).

While separate and distinct from BSA/AML, the core sections also include an overview and procedures for examining a bank's policies, procedures, and processes for ensuring compliance with OFAC sanctions. The examiner should review the bank's OFAC risk assessment and audit to determine the extent to which a review of the bank's OFAC program should be conducted during the examination. Refer to "Office of Foreign Assets Control" procedures pages 207 to 209.

The expanded sections address specific lines of business, products, or entities that may present unique challenges and exposures for which banks should institute appropriate policies, procedures, and processes. Absent appropriate controls these lines of business, products, or entities could elevate BSA/AML risks. In addition, within the expanded section there is guidance on enterprise-wide BSA/AML risk management.

Not all of the core and expanded procedures will likely be applicable to every banking organization. The specific procedures that will need to be performed depend on the BSA/AML risk profile of the banking organization, the quality and quantity of independent testing, the financial institution's history of BSA/AML compliance, and other relevant factors.

BACKGROUND

In 1970, Congress passed the Currency and Foreign Transactions Reporting Act commonly known as the "Bank Secrecy Act,"[2] which established requirements for recordkeeping and reporting by private individuals, banks,[3] and other financial institutions. The BSA was designed to help identify the source, volume, and movement of currency and other monetary instruments transported or transmitted into or out of the United States or deposited in financial institutions. The statute sought to achieve that objective by requiring individuals, banks, and other financial institutions to file currency

[2] 31 USC 5311 *et seq.*, 12 USC 1829b, and 1951 – 1959. See also 12 USC 1818(s) (federally insured depository institutions) and 12 USC 1786(q) (federally insured credit unions).

[3] Under the BSA, as implemented by 31 CFR 103.11, the term "bank" includes each agent, agency, branch or office within the United States of commercial banks, savings and loan associations, thrift institutions, credit unions, and foreign banks.

reports with the U.S. Department of the Treasury (U.S. Treasury), properly identify persons conducting transactions, and maintain a paper trail by keeping appropriate records of financial transactions. These records enable law enforcement and regulatory agencies to pursue investigations of criminal, tax, and regulatory violations, if warranted, and provide evidence useful in prosecuting money laundering and other financial crimes.

The Money Laundering Control Act of 1986 augmented the BSA's effectiveness by the interrelated sections 8(s) and 21 to the Federal Deposit Insurance Act (FDI Act), which sections apply equally to banks of all charters.[4] The Money Laundering Control Act of 1986 precludes circumvention of the BSA requirements by imposing criminal liability on a person or financial institution that knowingly assists in the laundering of money, or that structures transactions to avoid reporting them. The 1986 statute directed banks to establish and maintain procedures reasonably designed to ensure and monitor compliance with the reporting and recordkeeping requirements of the BSA. As a result, on January 27, 1987, all federal banking agencies issued essentially similar regulations requiring banks to develop programs for BSA compliance.

The 1992 Annunzio-Wylie Anti-Money Laundering Act strengthened the sanctions for BSA violations and the role of the U.S. Treasury. Two years later, Congress passed the Money Laundering Suppression Act of 1994 (MLSA), which further addressed the U.S. Treasury's role in combating money laundering.

In April 1996, a Suspicious Activity Report (SAR) was developed to be used by all banking organizations in the United States. A banking organization is required to file a SAR whenever it detects a known or suspected criminal violation of federal law or a suspicious transaction related to money laundering activity or a violation of the BSA.

In response to the September 11, 2001, terrorist attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act). Title III of the Patriot Act is the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001. The Patriot Act is arguably the single most significant AML law that Congress has enacted since the BSA itself. Among other things, the Patriot Act criminalized the financing of terrorism and augmented the existing BSA framework by strengthening customer identification procedures; prohibiting financial institutions from engaging in business with foreign shell banks; requiring financial institutions to have due diligence procedures, and, in some cases, enhanced due diligence procedures for foreign correspondent and private banking accounts; and improving information sharing between financial institutions and the U.S. government. The Patriot Act and its implementing regulations also:

[4] 12 USC 1818(s) and 1829b, respectively.

- Expanded the AML program requirements to all financial institutions.[5] (Refer to Appendix D ("Statutory Definition of Financial Institution") for further clarification.)
- Increased the civil and criminal penalties for money laundering.
- Provided the Secretary of the Treasury with the authority to impose "special measures" on jurisdictions, institutions, or transactions that are of "primary money-laundering concern."
- Facilitated records access and required banks to respond to regulatory requests for information within 120 hours.
- Required federal banking agencies to consider a bank's AML record when reviewing bank mergers, acquisitions, and other applications for business combinations.

ROLE OF GOVERNMENT AGENCIES IN THE BSA

Certain government agencies play a critical role in implementing BSA regulations, developing examination guidance, ensuring compliance with the BSA, and enforcing the BSA. These agencies include the U.S. Treasury, FinCEN, and the federal banking agencies (Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision). Internationally there are various multilateral government bodies that support the fight against money laundering and terrorist financing, refer to Appendix E ("International Organizations") for additional information.

U.S. Treasury

The BSA authorizes the Secretary of the Treasury to require financial institutions to establish AML programs, file certain reports, and keep certain records of transactions. Certain BSA provisions have been extended to cover not only traditional depository institutions, such as banks, savings associations, and credit unions, but also non-bank financial institutions, such as money services businesses, casinos, brokers/dealers in securities, and futures commission merchants.

FinCEN

FinCEN, a bureau of the U.S. Treasury, is the delegated administrator of the BSA. In this capacity, FinCEN issues regulations and interpretive guidance, provides outreach to regulated industries, supports the examination functions performed by federal banking agencies, and pursues civil enforcement actions when warranted. FinCEN relies on the federal banking agencies to examine banks within their respective jurisdictions for compliance with the BSA. FinCEN's other significant responsibilities include providing investigative case support to law enforcement, identifying and communicating financial

[5] The Patriot Act expanded the AML program requirement to all financial institutions as that term is defined in 31 USC 5312(a)(2). However, as of the publication of this manual, only certain types of financial institutions are subject to final rules implementing the AML program requirements of 31 USC 5318(h)(1) as established by the Patriot Act. Those financial institutions that are not currently subject to a final AML program rule are temporarily exempted from the Patriot Act requirements to establish an AML program, as set forth in 31 CFR 103.170.

crime trends and patterns, and fostering international cooperation with its counterparts worldwide.

Federal Banking Agencies

The federal banking agencies are responsible for the oversight of the various banking entities operating in the United States, including foreign branch offices of U.S. banks. The federal banking agencies are charged with chartering (NCUA, OCC, and OTS), insuring (FDIC and NCUA), regulating, and supervising banks.[6] 12 USC 1818(s)(2) requires that the appropriate federal banking agency include a review of the BSA compliance program at each examination of an insured depository institution. The federal banking agencies may use their authority, as granted under section 8 of the FDI Act, to enforce compliance with appropriate banking rules and regulations, including compliance with the BSA.

The federal banking agencies require each bank under their supervision to establish and maintain a BSA compliance program.[7] In accordance with the Patriot Act, FinCEN's regulations, require certain financial institutions to establish an AML compliance program that guards against money laundering and terrorist financing and ensures compliance with the BSA and its implementing regulations. When the Patriot Act was passed, banks under the supervision of a federal banking agency were already required by law to establish and maintain a BSA compliance program that, among other things, requires the bank to identify and report suspicious activity promptly. For this reason, 31 CFR 103.120 states that a bank regulated by a federal banking agency is deemed to have satisfied the AML program requirements of the Patriot Act if the bank develops and maintains a BSA compliance program that complies with the regulation of its federal functional regulator[8] governing such programs. This manual will refer to the BSA compliance program requirements for each federal banking agency as the "BSA/AML compliance program."

Banks should take reasonable and prudent steps to combat money laundering and terrorist financing and to minimize their vulnerability to the risk associated with such activities. Some banking organizations have damaged their reputations and have been required to pay civil money penalties for failing to implement adequate controls within their organization resulting in noncompliance with the BSA. In addition, due to the AML

[6] The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision may collaborate with state banking agencies on the examination, oversight, and enforcement of BSA/AML for state-chartered banks.

[7] See 12 CFR 208.63 (Board of Governors of the Federal Reserve System); 12 CFR 326.8 (Federal Deposit Insurance Corporation); 12 CFR 748.2 (National Credit Union Administration); 12 CFR 21.21 (Office of the Comptroller of the Currency); and 12 CFR 563.177 (Office of Thrift Supervision).

[8] Federal functional regulator means: Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; National Credit Union Administration; Office of the Comptroller of the Currency; Office of Thrift Supervision; Securities and Exchange Commission; or Commodity Futures Trading Commission.

assessment required as part of the application process, BSA/AML concerns can have an impact on the bank's strategic plan. For this reason, the federal banking agencies' and FinCEN's commitment to provide guidance that assists banks in complying with the BSA remains a high supervisory priority.

The federal banking agencies work to ensure that the organizations they supervise understand the importance of having an effective BSA/AML compliance program in place. Management must be vigilant in this area, especially as business grows and new products and services are introduced. An evaluation of the bank's BSA/AML compliance program and its compliance with the regulatory requirements of the BSA has been an integral part of the supervision process for years. Refer to Appendix A ("BSA Laws and Regulations") for further information.

As part of a strong BSA/AML compliance program, the federal banking agencies seek to ensure that a bank has policies, procedures, and processes to identify and report suspicious transactions to law enforcement. The agencies' supervisory processes assess whether banks have established the appropriate policies, procedures, and processes based on their BSA/AML risk to identify and report suspicious activity and that they provide sufficient detail in reports to law enforcement agencies to make the reports useful for investigating suspicious transactions that are reported. Refer to Appendices B ("BSA/AML Directives") and C ("BSA/AML References") for guidance.

OFAC

OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under the President's wartime and national emergency powers, as well as under authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

OFAC requirements are separate and distinct from the BSA, but both OFAC and the BSA share a common national security goal. For this reason, many financial institutions view compliance with OFAC sanctions as related to BSA compliance obligations; supervisory examination for BSA compliance is logically connected to the examination of a financial institution's compliance with OFAC sanctions. Refer to the core overview section "Office of Foreign Assets Control" page 84 for guidance, and examination procedures for OFAC compliance on page 207.

MONEY LAUNDERING AND TERRORIST FINANCING

The BSA is intended to safeguard the U.S. financial system and the financial institutions that make up that system from the abuses of financial crime, including money laundering, terrorist financing, and other illicit financial transactions. Money laundering and terrorist

financing are financial crimes with potentially devastating social and financial effects. From the profits of the narcotics trafficker to the assets looted from government coffers by dishonest foreign officials, criminal proceeds have the power to corrupt and ultimately destabilize communities or entire economies. Terrorist networks are able to facilitate their activities if they have financial means and access to the financial system. In both money laundering and terrorist financing, criminals can exploit loopholes or other weaknesses in the legitimate financial system to launder criminal proceeds, otherwise support terrorism, and, ultimately, hide the actual purpose of their activity.

Banking organizations must develop, implement, and maintain effective AML programs that address the ever changing strategies of money launderers and terrorists and that attempt to gain access to the U.S. financial system. A sound BSA/AML compliance program is critical in deterring and preventing these types of activities at, or through, banks and other financial institutions. Refer to Appendix F ("Money Laundering and Terrorist Financing Red Flags") for examples of suspicious activities that may indicate money laundering or terrorist financing.

Money Laundering

Money laundering is the criminal practice of processing ill-gotten gains, or "dirty" money, through a series of transactions; in this way the funds are "cleaned" so that they appear to be proceeds from legal activities. Money laundering generally does not involve currency at every stage of the laundering process. Although money laundering is a diverse and often complex process, it basically involves three independent steps that can occur simultaneously:

Placement: The first and most vulnerable stage of laundering money is placement. The goal is to introduce the unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement. Placement techniques include structuring currency deposits in amounts to evade reporting requirements or commingling currency deposits of legal and illegal enterprises. An example may include: dividing large amounts of currency into less-conspicuous smaller sums that are deposited directly into a bank account, depositing a refund check from a canceled vacation package or insurance policy, or purchasing a series of monetary instruments (e.g., cashier's checks or money orders) that are then collected and deposited into accounts at another location or financial institution. (Refer to Appendix G "Structuring" for additional guidance.)

Layering: The second stage of the money laundering process is layering, which involves moving funds around the financial system, often in a complex series of transactions to create confusion and complicate the paper trail. Examples of layering include exchanging monetary instruments for larger or smaller amounts, or wiring or transferring funds to and through numerous accounts in one or more financial institutions.

Integration: The ultimate goal of the money laundering process is integration. Once the funds are in the financial system and insulated through the layering stage, the integration stage is used to create the appearance of legality through additional transactions. These

transactions further shield the criminal from a recorded connection to the funds by providing a plausible explanation for the source of the funds. Examples include the purchase and resale of real estate, investment securities, foreign trusts, or other assets.

Terrorist Financing

The motivation behind terrorist financing is ideological as opposed to profit-seeking, which is generally the motivation for most crimes associated with money laundering. Terrorism is intended to intimidate a population or to compel a government or an international organization to do or abstain from doing any specific act through the threat of violence. An effective financial infrastructure is critical to terrorist operations. Terrorist groups develop sources of funding that are relatively mobile to ensure that funds can be used to obtain material and other logistical items needed to commit terrorist acts. Thus, money laundering is often a vital component of terrorist financing.

Terrorists generally finance their activities through both unlawful and legitimate sources. Unlawful activities, such as extortion, kidnapping, and narcotics trafficking, have been found to be a major source of funding. Other observed activities include smuggling, fraud, theft, robbery, identity theft, use of conflict diamonds,[9] and improper use of charitable or relief funds. In the last case, donors may have no knowledge that their donations have been diverted to support terrorist causes.

Other legitimate sources have also been found to provide terrorist organizations with funding; these legitimate funding sources are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership, and personal employment.

Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to those methods used by other criminals that launder funds. For example, terrorist financiers use currency smuggling, structured deposits or withdrawals from bank accounts, purchases of various types of monetary instruments, credit/debit or stored value cards, and funds transfers. There is also evidence that some forms of informal banking (e.g., "hawala"[10]) have played a role in moving terrorist funds. Transactions through hawalas are difficult to detect given the lack of documentation, their size, and the nature

[9] Conflict diamonds originate from areas controlled by forces or factions opposed to legitimate and internationally recognized governments and that are used to fund military action in opposition to those governments, or in contravention of the decisions of the United Nations Security Council (www.un.org).

[10] "Hawala" refers to one specific type of informal value transfer system. FinCEN describes hawala as "a method of monetary value transmission that is used in some parts of the world to conduct remittances, most often by persons who seek to legitimately send money to family members in their home country. It has also been noted that hawala, and other such systems, are possibly being used as conduits for terrorist financing or other illegal activity." For additional information and guidance on hawalas and FinCEN's report to Congress in accordance with section 359 of the Patriot Act refer to FinCEN's web site: www.fincen.gov.

of the transactions involved. Funding for terrorist attacks does not always require large sums of money, and the associated transactions may not be complex.

Criminal Penalties for Money Laundering, Terrorist Financing, and Violations of the BSA

Penalties for money laundering and terrorist financing can be severe. A person convicted of money laundering can face up to 20 years in prison and a fine of up to $500,000.[11] Any property involved in a transaction or traceable to the proceeds of the criminal activity, including property such as loan collateral, personal property, and, under certain conditions, entire bank accounts (even if some of the money in the account is legitimate), may be subject to forfeiture. Pursuant to various statutes, banks and individuals may incur criminal and civil liability for violating AML and terrorist financing laws. For instance, pursuant to 18 USC 1956 and 1957, the Department of Justice may bring criminal actions for money laundering that may include criminal fines, imprisonment, and forfeiture actions.[12] In addition, banks risk losing their charters, and bank employees risk being removed and barred from banking.

Moreover, there are criminal penalties for willful violations of the BSA and its implementing regulations under 31 USC 5322 and for structuring transactions to evade BSA reporting requirements under 31 USC 5324(d). For example, a person, including a bank employee, willfully violating the BSA or its implementing regulations is subject to a criminal fine of up to $250,000 or five years in prison, or both.[13] A person who commits such a violation while violating another U.S. law, or engaging in a pattern of criminal activity, is subject to a fine of up to $500,000 or ten years in prison, or both.[14] A bank that violates certain BSA provisions, including 31 USC 5318(i) or (j), or special measures imposed under 31 USC 5318A, faces criminal money penalties up to the greater of $1 million or twice the value of the transaction.[15]

Civil Penalties for Violations of the BSA

Pursuant to 12 USC 1818(i) and 31 USC 5321, the federal banking agencies and FinCEN, respectively, can bring civil money penalty actions for violations of the BSA. Moreover, in addition to criminal and civil money penalty actions taken against them, individuals may be removed from banking pursuant to 12 USC 1818(e)(2) for a violation of the AML laws under Title 31 of the U.S. Code, as long as the violation was not inadvertent or unintentional. All of these actions are publicly available.

[11] 18 USC 1956.

[12] 18 USC 981 and 982.

[13] 31 USC 5322(a).

[14] Id.

[15] Id.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – Scoping and Planning

OBJECTIVE

Identify the bank's BSA/AML risks and develop the examination scope and plan. This examination process includes determining examination staffing needs, including technical expertise, and selecting examination procedures to be completed.

OVERVIEW

The BSA/AML examination is intended to assess the effectiveness of the bank's BSA/AML compliance program and the bank's compliance with the regulatory requirements pertaining to the BSA, including a review of risk management practices.

SCOPING AND PLANNING PROCESS

Whenever possible, the scoping and planning process should be completed before entering the bank. During this process, it may be helpful to discuss BSA/AML matters with bank management, including the BSA compliance officer, either in person or by telephone. The scoping and planning process generally begins with an analysis of:

- Off-site monitoring information.
- Prior examination reports and workpapers.
- Request letter items completed by bank management. Refer to Appendix H ("Request Letter Items") for additional information.
- The bank's BSA/AML risk assessment.
- BSA-reporting databases (e.g., Currency and Banking Retrieval System (CBRS) and Currency and Banking Query System (CBQS)).
- Independent reviews or audits.

REVIEW OF THE BANK'S BSA/AML RISK ASSESSMENT

To accomplish the goals of the BSA/AML examination, the examiner must determine the BSA/AML risk profile of the bank as a part of the scoping and planning process. All banks must have a BSA/AML compliance program tailored to their particular risks. In evaluating the level of risk, a bank should not necessarily take any single indicator as determinative of the existence of lower or higher risk. The bank should also consult with all business lines in developing the risk assessment. The risk assessment process should weigh a number of factors, including the risk identification and measurement of products, services, customers, and geographic locations. Moreover, the application of these factors is fact-specific, and a conclusion regarding an account's risk should be based on a

consideration of all information. An effective risk assessment should be a composite of multiple factors, and depending upon the circumstances, certain factors may be weighed more heavily than others.

This risk assessment should assist a bank in effectively managing the BSA/AML risk and therefore, is critical in the development of applicable internal controls, as required for the BSA/AML compliance program. A graphic description of the BSA/AML compliance program link to the risk assessment process is provided in Appendix I ("Risk Assessment Link to the BSA/AML Compliance Program").

The scoping and planning process should be guided by the examiner's review of the bank's BSA/AML risk assessment. The examiner should review the risk assessment to determine if it is commensurate with the risk undertaken by the bank. If the bank has not developed a risk assessment, this fact should be discussed with management. For the purposes of the examination, whenever the bank has not completed a risk assessment, or the risk assessment is inadequate, the examiner must complete a risk assessment. Risk assessments should include a review of all factors pertinent to determining the bank's particular risk profile. BSA/AML risk assessment guidance is provided in Appendix J ("Quantity of Risk Matrix").

Assessing the Risk of Banking Operations

Although attempts to launder money, finance terrorism, or conduct other illegal activities through a bank can emanate from many different sources, certain products, services, customers, and geographic locations may be more vulnerable and have been historically abused by money launderers and criminals. Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same. Various factors, such as number and dollar volume, geographic location, and customer versus noncustomer, should be considered when making a risk assessment. Because of these variables, risks will vary from one bank to another. In formulating a risk-based BSA/AML compliance program, management should identify the significant risks to their bank and develop a risk assessment tailored to their circumstances.

An effective BSA/AML compliance program controls risks that may be associated with the bank's unique products, services, customers, and geographic locations. As new products and services are introduced, existing products and services change, and the bank expands through mergers and acquisitions, management's evaluation of the money laundering and terrorist financing should evolve. Furthermore, even without such changes, banks should periodically reassess their BSA/AML risks. The expanded sections provide detailed guidance and discussions on specific lines of business or products that may present unique challenges and exposures for which banks should institute appropriate policies, procedures, and processes. Absent appropriate controls these lines of business, products, or entities could elevate BSA/AML risks.

Products and Services

Certain products and services offered by banks may pose a higher risk of money laundering or terrorist financing depending on the nature of the specific product or service offered by the bank. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. Some of these products and services are listed below, but the list is not all inclusive:

- Electronic funds payment services – electronic cash (e.g., stored value and payroll cards), funds transfers (domestic and international), payable upon proper identification (PUPID) transactions, third-party payment processors, remittance activity, automated clearing house (ACH), and automated teller machines (ATMs).
- Electronic banking.
- Private banking – both domestic and international.
- Trust and asset management services.
- Monetary instruments.[16]
- Foreign correspondent accounts – pouch activity, payable through accounts, and U.S. dollar drafts.
- International trade finance (letters of credit).
- Special use or concentration accounts.
- Lending activities, particularly loans secured by cash collateral, marketable securities, and credit card lending.
- Nondeposit account services (e.g., nondeposit investment products, insurance, and safe deposit boxes).

Customers and Entities

Although any type of account is potentially vulnerable to money laundering or terrorist financing, by the nature of their business, occupation, or anticipated transaction activity, certain customers and entities may pose specific money laundering risks. However, it is essential that banks exercise judgment and neither define nor treat all members of a specific category of customer as posing the same level of risk. In assessing customer risk, it is essential that banks also factor other variables, such as services sought, source of funds, and geographic location. Within any category of business, there will be accountholders that pose varying levels of risk of money laundering. The expanded sections provide detailed guidance and discussions on specific customers and entities that that are detailed below:

- Foreign financial institutions, including banks and foreign money services providers (e.g., casas de cambio, exchange houses, money transmitters, and bureaux de change).

[16] Monetary instruments in this context include official bank checks, cashier's checks, money orders, and traveler's checks. Refer to the expanded overview section "Purchase and Sale of Monetary Instruments," on page 123 for further discussion on risk factors and risk mitigation regarding monetary instruments.

- Non-bank financial institutions (e.g., money services businesses, casinos and card clubs, brokers/dealers in securities, and dealers in precious metals, stones or jewels).
- Senior foreign political figures and their immediate family members and close associates (collectively known as politically exposed persons (PEPs)).[17]
- Nonresident alien (NRA)[18] and accounts of foreign individuals.
- Foreign corporations with transaction accounts, particularly offshore corporations (such as Private Investment Companies (PICs) and international business corporations (IBCs))[19] located in high-risk geographic locations.
- Deposit brokers, particularly foreign deposit brokers.
- Cash-intensive businesses (e.g., convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately-owned ATMs, vending machine operators, and parking garages).
- Non-governmental organizations and charities (foreign and domestic).
- Professional service providers (e.g., attorneys, accountants, doctors, or real estate brokers).

Geographic Locations

Identifying geographic locations that pose a higher risk is essential to a bank's BSA/AML compliance program. U.S. banks should understand and evaluate the specific risks associated with doing business in, opening accounts for customers from, or facilitating transactions involving certain geographic locations. However, geographic risk alone does not always determine an entity's or transactions' risk level, either positively or negatively.

High-risk geographic locations can be categorized as either international or domestic. International high-risk geographic locations generally include:

- Countries subject to OFAC sanctions, including state sponsors of terrorism.[20]
- Countries identified as supporting international terrorism under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State.[21]

[17] Refer to expanded overview "Politically Exposed Persons" on page 153 for additional guidance.

[18] NRA accounts may be identified by obtaining a list of financial institution customers who filed W-8s. Additional information can be found at www.irs.gov/formspubs.

[19] For explanations of PICs and IBCs and additional guidance refer to expanded overview "Corporate Entities (Domestic and Foreign)," page 164.

[20] A list of such countries, jurisdictions, and governments is available on OFAC's web site: www.treas.gov/ofac.

[21] A list of the countries supporting international terrorism appears in the Department of State's annual report "Patterns of Global Terrorism." This report is available on the Department of State's web site for its Counterterrorism Office: www.state.gov/s/ct/.

- Jurisdictions determined to be "of primary money laundering concern" by the Secretary of the Treasury, and jurisdictions subject to special measures imposed by the Secretary of the Treasury, through FinCEN, pursuant to section 311 of the Patriot Act.[22]
- Jurisdictions/countries identified as non-cooperative by the Financial Action Task Force on Money Laundering (FATF).[23]
- Major money laundering countries and jurisdictions identified in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR), in particular, countries which are identified as jurisdictions of primary concern.[24]
- Offshore financial centers (OFCs) as identified by the U.S. Department of State.[25]
- Other countries identified by the bank as high-risk because of its prior experiences, transaction history, or other factors (e.g., legal considerations, or allegations of official corruption).

Domestic high-risk geographic locations may include banking offices doing business within, or having customers located within, a U.S. Government-designated high-risk geographic location. Domestic high-risk geographic locations include:

- High Intensity Drug Trafficking Areas (HIDTAs).[26]
- High Intensity Financial Crime Areas (HIFCAs).[27]

[22] Notices of proposed rulemaking and final rules accompanying the determination "of primary money laundering concern," and imposition of a special measure (or measures) pursuant to section 311 of the Patriot Act are available on the FinCEN web site: www.fincen.gov.

[23] A current list of countries designated by FATF as non-cooperative countries and territories (NCCT) is available on the FATF web site: www.fatf-gafi.org.

[24] The INCSR, including the lists of high-risk money laundering countries and jurisdictions, may be accessed on the U.S. Department of State's web site (www.state.gov) on the Bureau of International Narcotics and Law Enforcement Affairs page.

[25] OFCs offer a variety of financial products and services. Typically, they are jurisdictions that have relatively large numbers of financial institutions engaged primarily in business with non-residents. OFCs are generally known to provide some or all of the following services: low or zero taxation; limited financial regulation; and banking secrecy and anonymity. Some OFCs offer the ability to form and maintain a variety of legal entities such as IBCs, "exempt" companies, trusts, investment funds, and insurance companies. To maintain the anonymity of the true beneficial owner of these entities, many are formed with nominee directors, nominee officeholders, and nominee shareholders. These financial institutions may have little or no physical presence in a given OFC, and the activity may be limited to the booking of the transaction. For additional information, including assessments of OFCs, see www.imf.org/external/ns/cs.aspx?id=55.

[26] A listing of these areas can be found at www.whitehousedrugpolicy.gov.

[27] A listing of these areas can be found at www.irs.gov/compliance/enforcement/article/0,,id=107488,00.html#hifca.

INDEPENDENT TESTING

As part of the scoping and planning process, examiners will obtain and evaluate the supporting documents of the independent testing (audit)[28] of the bank's BSA/AML compliance program. The scope and quality of the audit may provide examiners with a sense of particular risks in the bank, how these risks are being managed and controlled, and the status of compliance with the BSA. The independent testing scope and workpapers can assist examiners in understanding the audit coverage and the quality and quantity of transaction testing. This knowledge will assist the examiner in determining the examination scope, identifying areas requiring greater (or lesser) scrutiny, and identifying when expanded examination procedures may be necessary.

EXAMINATION PLAN

At a minimum, examiners should conduct the procedures included in the following sections of this manual to ensure that the bank has an adequate BSA/AML compliance program commensurate with its risk profile:

- Scoping and Planning (refer to pages 170 to 173).
- BSA/AML Compliance Program (refer to pages 174 to 178).
- Developing Conclusions and Finalizing the Examination (refer to pages 210 to 213).

The core section also includes an overview and procedures for examining a bank's policies, procedures, and processes for ensuring compliance with OFAC sanctions. The examiner should review the bank's OFAC risk assessment and audit to determine the extent to which a review of the bank's OFAC program should be conducted during the examination. Refer to "Office of Foreign Assets Control" procedures pages 207 to 209.

The examiner should develop an initial examination plan commensurate with the overall BSA/AML risk profile of the bank. This plan may change during the examination as a result of on-site findings. The examiner should prepare a request letter to the bank. Suggested request letter items are detailed in Appendix H ("Request Letter Items"). On the basis of the risk profile, the quality of audit, the previous examination findings, and the initial examination work, examiners should complete additional core and expanded examination procedures, as appropriate. At larger, more complex banking organizations, examiners may complete various types of examinations throughout the supervisory plan or cycle. These reviews may focus on one or more business lines (e.g., private banking, trade financing, or foreign correspondent banking relationships). The examiner should include an evaluation of the BSA/AML compliance program within the supervisory plan or cycle.

[28] The federal banking agencies' reference to "audit" does not confer an expectation that the required independent testing must be performed by a specifically designated auditor, whether internal or external. However, the person performing the independent testing must not be involved in any part of the bank's BSA/AML compliance program. The findings should be reported directly to the board of directors or an audit committee composed primarily or completely of outside directors.

Transaction Testing

Examiners perform transaction testing to evaluate the adequacy of the bank's compliance with regulatory requirements, determine the effectiveness of its policies, procedures, and processes, and evaluate suspicious activity monitoring systems. Transaction testing is an important factor in forming conclusions about the integrity of the bank's overall controls and risk management processes. Transaction testing must be performed at each examination. Transaction testing can be performed either through conducting the transaction testing procedures within the independent testing function (audit) section or completing the transaction testing procedures contained elsewhere within the core or expanded sections. The extent of transaction testing and activities where it is performed is based on various factors including the examiner's judgment of risks, controls, and the adequacy of the independent testing. Once on-site, the scope of the transaction testing can be expanded to address any issues or concerns identified during the examination.

INFORMATION AVAILABLE FROM BSA-REPORTING DATABASES

Examination planning should also include an analysis of the Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs), and CTR exemptions that the bank has filed. SARs, CTRs, and CTR exemptions may be downloaded from or obtained directly online from the BSA-reporting databases (e.g., CBRS and CBQS). Each federal banking agency has staff authorized to obtain this data from the BSA-reporting database. When requesting searches from the BSA-reporting database, the examiner should contact the appropriate person (or persons), within his or her agency, sufficiently in advance of the examination start date in order to obtain the requested information. When a bank has recently purchased or merged with another bank, the examiner should obtain SARs, CTRs, and CTR exemptions data on the acquired bank, as well.

Downloaded information can be displayed on an electronic spreadsheet, which contains all of the data included on the original document filed by the bank as well as the Internal Revenue Service (IRS) Document Control Number (DCN), and the date the document was entered into the BSA-reporting database. Downloaded information may be important to the examination, as it will help examiners:

- Identify high-volume currency customers.
- Assist in selecting accounts for transaction testing.
- Identify the number and characteristics of SARs filed.
- Identify the number and nature of exemptions.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – BSA/AML Compliance Program

OBJECTIVE

Assess the adequacy of the BSA/AML compliance program. Determine whether the bank has developed, administered, and maintained an effective program for compliance with the BSA and all of its implementing regulations.

OVERVIEW

Review of the bank's written policies, procedures, and processes is a first step in determining the overall adequacy of the BSA/AML compliance program. The completion of applicable core and, if warranted, expanded examination procedures is necessary to support the overall conclusions regarding the adequacy of the BSA/AML compliance program. Examination findings should be discussed with management, and significant findings must be included in the report of examination.

BSA/AML COMPLIANCE PROGRAM

The BSA/AML compliance program must be written, approved by the board of directors, and noted in the board minutes. A bank must have a BSA/AML compliance program commensurate with its respective BSA/AML risk profile. Refer to Appendix I ("Risk Assessment Link to the BSA/AML Compliance Program"). Furthermore, the program must be fully implemented and reasonably designed to meet the BSA requirements. Policy statements alone are not sufficient; practices must coincide with the bank's written policies, procedures, and processes. The BSA/AML compliance program must provide for the following minimum requirements:

- A system of internal controls to ensure ongoing compliance.
- Independent testing of BSA/AML compliance.
- Designate an individual or individuals responsible for managing BSA compliance (BSA compliance officer).
- Training for appropriate personnel.

In addition, a customer identification program (CIP) must be included as part of the BSA/AML compliance program. Refer to the core overview section "Customer Identification Program" on page 30 for additional guidance.

Internal Controls

The board of directors, acting through senior management, is ultimately responsible for ensuring that the bank maintains an effective BSA/AML internal control structure,

including suspicious activity monitoring and reporting. The board of directors and management should create a culture of compliance to ensure staff adherence to the bank's BSA/AML policies, procedures, and processes. Internal controls are the bank's policies, procedures, and processes designed to limit and control risks and to achieve compliance with the BSA. The level of sophistication of the internal controls should be commensurate with the size, structure, risks and complexity of the bank. Large complex banks are more likely to implement departmental internal controls for BSA/AML compliance. Departmental internal controls typically address risks and compliance requirements unique to a particular line of business or department and are part of a comprehensive BSA/AML compliance program.

Internal controls should:

- Identify banking operations (products, services, customers, and geographic locations) more vulnerable to abuse by money launderers and criminals; provide for periodic updates to the bank's risk profile; and provide for a BSA/AML compliance program tailored to manage risks.
- Inform the board of directors, or a committee thereof, and senior management, of compliance initiatives, identified compliance deficiencies, and corrective action taken, and notify directors and senior management of Suspicious Activity Reports (SARs) filed.[29]
- Identify a person or persons responsible for BSA/AML compliance.
- Provide for program continuity despite changes in management or employee composition or structure.
- Meet all regulatory recordkeeping and reporting requirements, meet recommendations for BSA/AML compliance and provide for timely updates in response to changes in regulations.
- Implement risk-based customer due diligence (CDD) policies, procedures, and processes.
- Identify reportable transactions and accurately file all required reports including SARs, Currency Transaction Reports (CTRs), and CTR exemptions. (Banks should consider centralizing the review and report-filing functions within the banking organization.)
- Provide for dual controls and segregation of duties. (Employees that complete the reporting forms (e.g., SARs, CTRs, and CTR exemptions) should not also be responsible for filing the reports or granting the exemptions).
- Provide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity.
- Provide for adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity covered by the BSA and its implementing regulations.
- Incorporate BSA compliance into the job descriptions and performance evaluations of appropriate personnel.

[29] Credit unions do not have a regulatory requirement to notify the board of directors of SAR filings, although many take this action as a matter of best practice.

The above list is not designed to be all-inclusive and should be tailored to reflect the bank's risk profile. Additional policy guidance for specific risk areas is provided in the expanded sections of this manual.

Independent Testing

Independent testing (audit) should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties. While the frequency of audit is not specifically defined in any statute, a sound practice is for the bank to conduct independent testing at least annually. Banks that do not employ outside auditors or consultants or have internal audit departments may comply with this requirement by using qualified persons who are not involved in the function being tested. The persons conducting the BSA/AML testing should report directly to the board of directors or to a designated board committee comprised primarily or completely of outside directors.

Those persons responsible for conducting an objective independent evaluation of the written BSA/AML compliance program should perform testing for specific compliance with the BSA, and evaluate pertinent management information systems (MIS). The audit should be risk based[30] and evaluate the quality of risk management for all banking operations, departments, and subsidiaries. Risk-based audit programs will vary depending on the bank's size, complexity, scope of activities, risk profile, quality of control functions, geographic diversity, and use of technology. An effective risk-based auditing program will cover all of the bank's activities. The frequency and depth of each activity's audit will vary according to the activity's risk assessment. Risk-based auditing enables the board of directors and auditors to use the bank's risk assessment to focus the audit scope on the areas of greatest concern. The testing should assist the board of directors and management in identifying areas of weakness or areas where there is a need for enhancements or stronger controls.

Independent testing should, at a minimum, include:

- An evaluation of the overall integrity and effectiveness of the BSA/AML compliance program, including policies, procedures, and processes.
- A review of the bank's risk assessment for reasonableness given the bank's risk profile (products, services, customers, and geographic locations).
- Appropriate transaction testing to verify the bank's adherence to the BSA recordkeeping and reporting requirements (e.g., CIP, SARs, CTRs, and CTR exemptions, information sharing requests).
- An evaluation of management's efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations, including progress in addressing outstanding supervisory actions, if applicable.
- A review of staff training for adequacy, accuracy, and completeness.

[30] Refer to Appendix J ("Quantity of Risk Matrix").

- A review of the effectiveness of the suspicious activity monitoring systems (manual, automated, or a combination) used for BSA/AML compliance. Related reports may include, but are not limited to:

  – Suspicious activity monitoring reports.
  – Large currency aggregation reports.
  – Monetary instrument records.
  – Funds transfer records.
  – Nonsufficient funds (NSF) reports.
  – Large balance fluctuation reports.
  – Account relationship reports.

- An assessment of the overall process for identifying and reporting suspicious activity, including a review of filed or prepared SARs to determine their accuracy, timeliness, completeness, and effectiveness of the bank's policy.

Auditors should document the audit scope, procedures performed, transaction testing completed, and findings of the review. All audit documentation and workpapers should be available for examiner review. Any violations, policy or procedures exceptions, or other deficiencies noted during the audit should be included in an audit report and reported to the board of directors or a designated committee in a timely manner. The board or designated committee and the audit staff should track audit deficiencies and document corrective actions.

BSA Compliance Officer

The bank's board of directors must designate a qualified employee to serve as the BSA compliance officer.[31] The BSA compliance officer is responsible for coordinating and monitoring day-to-day BSA/AML compliance. The BSA compliance officer is also charged with managing all aspects of the BSA/AML compliance program and with managing the bank's adherence to the BSA and its implementing regulations; however, the board of directors is ultimately responsible for the bank's BSA/AML compliance.

While the title of the individual responsible for overall BSA/AML compliance is not important, his or her level of authority and responsibility within the bank is critical. The BSA compliance officer may delegate BSA/AML duties to other employees, but the officer should be responsible for overall BSA/AML compliance. The board of directors is responsible for ensuring that the BSA compliance officer has sufficient authority and resources (monetary, physical, and personnel) to administer an effective BSA/AML compliance program based on the bank's risk profile.

[31] The bank must designate one or more persons to coordinate and monitor day-to-day compliance. This requirement is detailed in the federal banking agencies' BSA compliance program regulations: 12 CFR 208.63 (Board of Governors of the Federal Reserve System); 12 CFR 326.8 (Federal Deposit Insurance Corporation); 12 CFR 748.2 (National Credit Union Administration); 12 CFR 21.21 (Office of the Comptroller of the Currency); and 12 CFR 563.177 (Office of Thrift Supervision).

The BSA compliance officer should be fully knowledgeable of the BSA and all related regulations. The BSA compliance officer should also understand the bank's products, services, customers, and geographic locations, and the potential money laundering and terrorist financing risks associated with those activities. The appointment of a BSA compliance officer is not sufficient to meet the regulatory requirement if that person does not have the expertise, authority, or time to satisfactorily complete the job.

The line of communication should allow the BSA compliance officer to regularly apprise the board of directors and senior management of ongoing compliance with the BSA. Pertinent BSA-related information, including the reporting of SARs filed with FinCEN, should be reported to the board of directors or an appropriate board committee so that these individuals can make informed decisions about overall BSA/AML compliance. The BSA compliance officer is responsible for carrying out the direction of the board and ensuring that employees adhere to the bank's BSA/AML policies, procedures, and processes.

Training

Banks must ensure that appropriate personnel are trained in applicable aspects of the BSA. Training should include regulatory requirements and the bank's internal BSA/AML policies, procedures, and processes. At a minimum, the bank's training program must provide training for all personnel whose duties require knowledge of the BSA. The training should be tailored to the person's specific responsibilities. In addition, an overview of the BSA/AML requirements should be given to new staff. Training should encompass information related to applicable operational lines, such as trust services, international, and private banking.

The board of directors and senior management should be informed of changes and new developments in the BSA, its implementing regulations and directives, and the federal banking agencies' regulations. While the board of directors may not require the same degree of training as banking operations personnel, they need to understand the importance of BSA/AML regulatory requirements, the ramifications of noncompliance, and the risks posed to the bank. Without a general understanding of the BSA, the board of directors cannot adequately provide BSA/AML oversight; approve BSA/AML policies, procedures, and processes; or provide sufficient BSA/AML resources.

Training should be ongoing and incorporate current developments and changes to the BSA and any related regulations. Changes to internal policies, procedures, processes, and monitoring systems should also be covered during training. The program should reinforce the importance that the board and senior management place on the bank's compliance with the BSA and ensure that all employees understand their role in maintaining an effective BSA/AML compliance program.

Examples of money laundering activity and suspicious activity monitoring and reporting can and should be tailored to each individual audience. For example, training for tellers

should focus on examples involving large currency transactions or other suspicious activities; training for the loan department should provide examples involving money laundering through lending arrangements.

Banks should document their training programs. Training and testing materials, the dates of training sessions, and attendance records should be maintained by the bank and be available for examiner review.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – Customer Identification Program

OBJECTIVE

Assess the bank's compliance with the statutory and regulatory requirements for the Customer Identification Program (CIP).

OVERVIEW

As of October 1, 2003, all banks and their operating subsidiaries must have a written CIP.[32] The CIP rule implements section 326 of the Patriot Act and requires each bank to implement a written CIP that is appropriate for its size and type of business and that includes certain minimum requirements. The CIP must be incorporated into the bank's BSA/AML compliance program, which is subject to approval by the bank's board of directors.[33]

The CIP is intended to enable the bank to form a reasonable belief that it knows the true identity of each customer. The CIP must include account opening procedures that specify the identifying information that will be obtained from each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each customer. Banks should conduct a risk assessment of their customer base and product offerings, and in determining the risks, consider:

- The types of accounts offered by the bank.
- The bank's methods of opening accounts.
- The types of identifying information available.
- The bank's size, location, and customer base.

Pursuant to the CIP rule, an "account" is a formal banking relationship to provide or engage in services, dealings, or other financial transactions, and includes a deposit account, a transaction or asset account, a credit account, or another extension of credit. An account also includes a relationship established to provide a safe deposit box or other safekeeping services or to provide cash management, custodian, or trust services.

[32] See 12 CFR 208.63(b), 211.5(m), 211.24(j) (Board of Governors of the Federal Reserve System); 12 CFR 326.8(b) (Federal Deposit Insurance Corporation); 12 CFR 748.2(b) (National Credit Union Administration); 12 CFR 21.21 (Office of the Comptroller of the Currency); 12 CFR 563.177(b) (Office of Thrift Supervision); and 31 CFR 103.121 (FinCEN).

[33] As of the publication date of this manual, nonfederally regulated private banks, trust companies, and credit unions do not have BSA/AML compliance program requirements; however, the bank's board must still approve the CIP.

An account does not include:

- Products or services for which a formal banking relationship is not established with a person, such as check cashing, funds transfer, or the sale of a check or money order.
- Any account that the bank acquires. This may include single or multiple accounts as a result of a purchase of assets, acquisition, merger, or assumption of liabilities.
- Accounts opened to participate in an employee benefit plan established under the Employee Retirement Income Security Act of 1974.

The CIP rule applies to a "customer." A customer is a "person" (an individual, a corporation, partnership, a trust, an estate, or any other entity recognized as a legal person) who opens a new account, an individual who opens a new account for another individual who lacks legal capacity, and an individual who opens a new account for an entity that is not a legal person (e.g., a civic club). A customer does not include a person who does not receive banking services, such as a person whose loan application is denied.[34] The definition of "customer" also does not include an existing customer as long as the bank has a reasonable belief that it knows the customer's true identity.[35] Excluded from the definition of customer are federally regulated banks, banks regulated by a state bank regulator, governmental entities, and publicly traded companies (as described in 31 CFR 103.22(d)(2)(ii) through (iv)).

CUSTOMER INFORMATION REQUIRED

The CIP must contain account opening procedures detailing the identifying information that must be obtained from each customer.[36] At a minimum, the bank must obtain the following basic information from each customer before opening the account:[37]

[34] When the account is a loan, the account is considered to be "opened" when the bank enters into an enforceable agreement to provide a loan to the customer.

[35] The bank may demonstrate that it knows an existing customer's true identity showing that before the issuance of the final CIP rule, it had comparable procedures in place to verify the identity of persons who had accounts with the bank as of October 1, 2003, though the bank may not have gathered the very same information about such persons as required by the final CIP rule. Alternative means include showing that the bank has had an active and longstanding relationship with a particular person, as evidenced by such things as a history of account statements sent to the person, information sent to the Internal Revenue Service (IRS) about the person's accounts without issue, loans made and repaid, or other services performed for the person over a period of time. Alternative means, however, may not suffice for persons that the bank has deemed to be high risk.

[36] When an individual opens a new account for an entity that is not a legal person or for another individual who lacks legal capacity, the identifying information for the individual opening the account must be obtained. By contrast, when an account is opened by an agent on behalf of another person, the bank must obtain the identifying information of the person on whose behalf the account is being opened.

[37] For credit card customers, the bank may obtain identifying information from a third-party source before extending credit.

- Name.
- Date of birth, for individuals.
- Address.[38]
- Identification number.[39]

Based on its risk assessments, a bank may require identifying information in addition to the items above for certain customers or product lines.

CUSTOMER VERIFICATION

The CIP must contain risk-based procedures for verifying the identity of the customer within a reasonable period of time after the account is opened. The verification procedures must use "the information obtained in accordance with [31 CFR 103.121] paragraph (b)(2)(i)," namely the identifying information obtained by the bank. A bank need not establish the accuracy of every element of identifying information obtained, but it must verify enough information to form a reasonable belief that it knows the true identity of the customer. The bank's procedures must describe when it will use documents, nondocumentary methods, or a combination of both.

Verification Through Documents

A bank using documentary methods to verify a customer's identity must have procedures that set forth the minimum acceptable documentation. The CIP rule gives examples of types of documents that have long been considered primary sources of identification. The rule reflects the federal banking agencies' expectations that banks will review an unexpired government-issued form of identification from most customers. This identification must provide evidence of a customer's nationality or residence and bear a photograph or similar safeguard; examples include a driver's license or passport. However, other forms of identification may be used if they enable the bank to form a reasonable belief that it knows the true identity of the customer. Nonetheless, given the availability of counterfeit and fraudulently obtained documents, a bank is encouraged to

[38] For an individual: a residential or business street address, or if the individual does not have such an address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, the residential or business street address of next of kin or of another contact individual, or a description of the customer's physical location. For a "person" other than an individual (such as a corporation, partnership, or trust): a principal place of business, local office, or other physical location.

[39] An identification number for a U.S. person is a taxpayer identification number (TIN) (or evidence of an application for one), and for a non-U.S. person is one or more of the following: a TIN; a passport number and country of issuance; an alien identification card number; or a number and country of issuance of any other unexpired government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard. TIN is defined by section 6109 of the Internal Revenue Code of 1986 (26 USC 6109) and the IRS regulations implementing that section (e.g., Social Security number or employer identification number).

review more than a single document to ensure that it has a reasonable belief that it knows the customer's true identity.

For a "person" other than an individual (such as a corporation, partnership, or trust), the bank should obtain documents showing the legal existence of the entity, such as certified articles of incorporation, an unexpired government-issued business license, a partnership agreement, or a trust instrument.

Verification Through Nondocumentary Methods

Banks are not required to use nondocumentary methods to verify a customer's identity. However, a bank using nondocumentary methods to verify a customer's identity must have procedures that set forth the methods the bank will use. Nondocumentary methods may include contacting a customer; independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement.

The bank's nondocumentary procedures must also address the following situations: An individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard; the bank is not familiar with the documents presented; the account is opened without obtaining documents (e.g., the bank obtains the required information from the customer with the intent to verify it); the customer opens the account without appearing in person; or the bank is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customer through documents.

Additional Verification for Certain Customers

The CIP must address situations where, based on its risk assessment of a new account opened by a customer that is not an individual, the bank will obtain information about individuals with authority or control over such accounts, including signatories, in order to verify the customer's identity. This verification method applies only when the bank cannot verify the customer's true identity using documentary or nondocumentary methods. For example, a bank may need to obtain information about and verify the identity of a sole proprietor or the principals in a partnership when the bank cannot otherwise satisfactorily identify the sole proprietorship or the partnership.

Lack of Verification

The CIP must also have procedures for circumstances in which the bank cannot form a reasonable belief that it knows the true identity of the customer. These procedures should describe:

- Circumstances in which the bank should not open an account.
- The terms under which a customer may use an account while the bank attempts to verify the customer's identity.
- When the bank should close an account, after attempts to verify a customer's identity have failed.
- When the bank should file a SAR in accordance with applicable law and regulation.

RECORDKEEPING REQUIREMENTS AND RETENTION

A bank's CIP must include recordkeeping procedures. At a minimum, the bank must retain the identifying information (name, address, date of birth for an individual, TIN, and any other information required by the CIP) obtained at account opening for a period of five years after the account is closed.[40] For credit cards, the retention period is five years after the account closes or becomes dormant.

The bank must also keep a description of the following for five years after the record was made:

- Any document that was relied on to verify identity, noting the type of document, the identification number, the place of issuance and, if any, the date of issuance and expiration date.
- The method and the results of any measures undertaken to verify identity.
- The results of any substantive discrepancy discovered when verifying identity.

COMPARISON WITH GOVERNMENT LISTS

The CIP must include procedures for determining whether the customer appears on any federal government list of known or suspected terrorists or terrorist organizations.[41] Banks will be contacted by the U.S. Treasury in consultation with their federal banking agency when a list is issued. At such time, banks must compare customer names against the list within a reasonable time of account opening or earlier, if required by the government, and they must follow any directives that accompany the list.

[40] Banks are not required to make and retain photocopies of any documents used in the verification process. However, if a bank does choose to do so, it should ensure that these photocopies are physically secured to adequately protect against possible identity theft. In addition, such photocopies should not be maintained with files and documentation relating to credit decisions to avoid any potential problems with consumer compliance regulations.

[41] As of the publication date of this manual, there are no designated government lists to verify specifically for CIP purposes. Customer comparisons to lists required by OFAC and the Patriot Act section 314(a) (31 CFR 103.100) requests remain separate and distinct requirements.

ADEQUATE CUSTOMER NOTICE

The CIP must include procedures for providing customers with adequate notice that the bank is requesting information to verify their identities. The notice must generally describe the bank's identification requirements and be provided in a manner that is reasonably designed to allow a customer to view it or otherwise receive the notice before the account is opened. Examples include posting the notice in the lobby, on a web site, or within loan application documents. Sample language is provided in the regulation:

> IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT - To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account. What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

RELIANCE ON ANOTHER FINANCIAL INSTITUTION

A bank is permitted to rely on another financial institution (including an affiliate) to perform some or all of the elements of the CIP, if reliance is addressed in the CIP and the following criteria are met:

- The relied-upon financial institution is subject to a final rule implementing the AML program requirements of 31 USC 5318(h) and is regulated by a federal functional regulator.[42]
- The customer has an account or is opening an account at the bank and at the other functionally regulated institution.
- Reliance is reasonable, under the circumstances.
- The other financial institution enters into a contract requiring it to certify annually to the bank that it has implemented its AML program, and that it will perform (or its agent will perform) the specified requirements of the bank's CIP.

USE OF THIRD PARTIES

The final rule does not alter a bank's authority to use a third party, such as an agent or service provider, to perform services on its behalf. Therefore, a bank is permitted to arrange for a third party, such as a car dealer or mortgage broker, acting as its agent in connection with a loan, to verify the identity of its customer. The bank can also arrange for a third party to maintain its records. However, as with any other responsibility performed by a third party, the bank is ultimately responsible for that third party's

[42] Federal functional regulator means: Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; National Credit Union Administration; Office of the Comptroller of the Currency; Office of Thrift Supervision; Securities and Exchange Commission; or Commodity Futures Trading Commission.

compliance with the requirements of the bank's CIP. As a result, banks should establish adequate controls and review procedures for such relationships. This requirement contrasts with the reliance provision of the rule that permits the relied-upon party to take responsibility.

OTHER LEGAL REQUIREMENTS

Nothing in the CIP rule relieves a bank of its obligations under any provision of the BSA or other AML laws, rules and regulations, particularly with respect to provisions concerning information that must be obtained, verified, or maintained in connection with any account or transaction.

The U.S. Treasury and the federal banking agencies have provided banks with Frequently Asked Questions (FAQs), which may be revised periodically. The FAQs and other related documents (e.g., the CIP rule) are available on FinCEN's and the federal banking agencies' web sites.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – Customer Due Diligence

OBJECTIVE

Assess the appropriateness and comprehensiveness of the bank's customer due diligence (CDD) policies, procedures, and processes for obtaining customer information and assess the value of this information in detecting, monitoring, and reporting suspicious activity.

OVERVIEW

The cornerstone of a strong BSA/AML compliance program is the adoption and implementation of comprehensive CDD policies, procedures, and processes for all customers, particularly those that present a high risk for money laundering and terrorist financing. The objective of CDD procedures should be to enable the bank to predict with relative certainty the types of transactions in which a customer is likely to engage. These procedures assist the bank in determining when transactions are potentially suspicious. The concept of CDD begins with verifying the customer's identity and assessing the risks associated with that customer. Procedures should also include enhanced CDD for high-risk customers and ongoing due diligence of the customer base.

Effective CDD policies, procedures, and processes provide the critical framework that enables the bank to comply with regulatory requirements and to report suspicious activity. An illustration of this concept is provided in Appendix K ("Customer Risk Versus Due Diligence and Suspicious Activity Monitoring"). CDD policies, procedures, and processes are critical to the bank because they can aid in:

- Detecting and reporting unusual or suspicious transactions that potentially expose the bank to financial loss, increased expenses, or reputational risk.
- Avoiding criminal exposure from persons who use or attempt to use the bank's products and services for illicit purposes.
- Adhering to safe and sound banking practices.

CUSTOMER DUE DILIGENCE GUIDANCE

BSA/AML policies, procedures, and processes should include CDD guidelines that:

- Are commensurate with the bank's BSA/AML risk profile, paying particular attention to high-risk customers.
- Contain a clear statement of management's overall expectations and establish specific staff responsibilities, including who is responsible for reviewing or approving changes to a customer's risk rating or profile, as applicable.

- Ensure that the bank possesses sufficient customer information to implement an effective suspicious activity monitoring system.
- Provide guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.
- Ensure the bank maintains current customer information.

CUSTOMER RISK

Management should have a thorough understanding of the money laundering or terrorist financing risks of the bank's customer base. Under this approach, the bank will obtain information at account opening sufficient to develop an understanding of normal and expected activity for the customer's occupation or business operations.

Much of the CDD information can be confirmed through an information-reporting agency, banking references (for larger accounts), correspondence and telephone conversations with the customer, and visits to the customer's place of business. Additional steps may include obtaining third-party references or researching public information (e.g., on the Internet or commercial databases).

CDD procedures should include periodic monitoring of the customer relationship to determine whether there are substantive changes to the original CDD information (e.g., change in employment or business operations).

Enhanced Due Diligence for High-Risk Customers

Customers that pose high money laundering or terrorist financing risks present increased exposure to banks and due diligence policies, procedures, and processes should be enhanced as a result. Enhanced due diligence for high-risk customers is especially critical in understanding their anticipated transactions and implementing a suspicious activity monitoring system that reduces the bank's reputation, compliance, and transaction risks. High-risk customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the bank. Guidance to identify high-risk customers may be found in the core overview section "Scoping and Planning," page 17.

The bank may determine that a customer poses a high risk because of the customer's business activity, ownership structure, anticipated or actual volume and types of transactions, including those transactions involving high-risk jurisdictions. If so, the bank should consider obtaining, both at account opening and throughout the relationship, the following information on the customer:

- Purpose of the account.
- Source of funds and wealth.
- Beneficial owners of the accounts, if applicable.
- Customer's (or beneficial owner's) occupation or type of business.

- Financial statements.
- Banking references.
- Domicile (where the business is incorporated).
- Proximity of the customer's residence, place of employment, or place of business to the bank.
- Description of the customer's primary trade area and whether international transactions are expected to be routine.
- Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers.
- Explanations for changes in account activity.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – Suspicious Activity Reporting

OBJECTIVE

Assess the bank's policies, procedures, and processes, and overall compliance with statutory and regulatory requirements for monitoring, detecting, and reporting suspicious activities.

OVERVIEW

Suspicious activity reporting forms the cornerstone of the BSA reporting system. It is critical to the United States' ability to utilize financial information to combat terrorism, terrorist financing, money laundering, and other financial crimes. Within this system, FinCEN and the federal banking agencies recognize that, as a practical matter, it is not possible for a bank to detect and report all potentially illicit transactions that flow through the bank. Examiners should focus on evaluating a bank's policies, procedures, and processes to identify and research suspicious activity. However, as part of the examination process, examiners should review individual Suspicious Activity Report (SAR) filing decisions to determine the effectiveness of the suspicious activity monitoring and reporting process. Above all, examiners and banks should recognize that the quality of SAR data is paramount to the effective implementation of the suspicious activity reporting system.

Banks, bank holding companies, and their subsidiaries are required by federal regulations[43] to file a SAR with respect to:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating $5,000 or more when a suspect can be identified.
- Criminal violations aggregating $25,000 or more regardless of a potential suspect.
- Transactions conducted or attempted by, at, or through the bank (or an affiliate) and aggregating $5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect that the transaction:

  – May involve potential money laundering or other illegal activity (e.g., terrorism financing).
  – Is designed to evade the BSA or its implementing regulations.

[43] See 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Board of Governors of the Federal Reserve System); 12 CFR 353 (Federal Deposit Insurance Corporation); 12 CFR 748 (National Credit Union Administration); 12 CFR 21.11 (Office of the Comptroller of the Currency); 12 CFR 563.180 (Office of Thrift Supervision) (does not apply to Savings and Loan Holding Companies); and 31 CFR 103.18 (FinCEN).

- Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

A transaction includes a deposit; a withdrawal; a transfer between accounts; an exchange of currency; an extension of credit; a purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security; or any other payment, transfer, or delivery by, through, or to a bank.

Safe Harbor for Banks from Civil Liability for Suspicious Activity Reporting

Federal law (31 USC 5318(g)(3)) provides protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to the SAR instructions. Specifically, the law provides that a bank and its directors, officers, employees, and agents that make a disclosure to the appropriate authorities of any possible violation of law or regulation, including a disclosure in connection with the preparation of SARs, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure." The safe harbor applies to SARs filed within the required reporting thresholds as well as to SARs filed voluntarily on any activity below the threshold.

SYSTEMS TO IDENTIFY, RESEARCH, AND REPORT SUSPICIOUS ACTIVITY

Policies, procedures, and processes should indicate the persons responsible for the identification, research, and reporting of suspicious activities. Appropriate policies, procedures, and processes should be in place to monitor and identify unusual activity. The level of monitoring should be dictated by the bank's assessment of risk, with particular emphasis on high-risk products, services, customers, and geographic locations. Monitoring systems typically include employee identification or referrals, manual systems, automated systems, or any combination. The bank should ensure adequate staff is assigned to the identification, research, and reporting of suspicious activities taking into account the bank's overall risk profile and the volume of transactions.

Upon identification of unusual activity, additional research is typically conducted. Customer due diligence (CDD) information will assist banks in evaluating if the unusual activity is considered suspicious. (For additional information, refer to core overview section "Customer Due Diligence" discussion on page 37.) After thorough research and analysis, decisions to file or not to file a SAR should be documented. If applicable, reviewing and understanding suspicious activity monitoring across the organization's

affiliates, business lines, and risk types (e.g., reputation, compliance, or transaction) may enhance a banking organizations' ability to detect suspicious activity and thus minimize the potential for financial losses, increased expenses, and reputational risk to the organization. Refer to "Enterprise-Wide BSA/AML Compliance Program" expanded overview section on page 93 for further guidance.

Manual Transaction Monitoring

A manual transaction monitoring system consists of a review of various reports generated by the bank's management information systems (MIS) or vendor systems. Some bank's MIS are supplemented by vendor systems designed to identify reportable currency transactions and to maintain required funds transfer records. Many of these vendor systems include filtering models for identification of unusual activity. Examples of MIS reports include currency activity reports, funds transfer reports, monetary instrument sales reports, large item reports, significant balance change reports, and nonsufficient funds (NSF) reports. The process may involve review of daily reports, reports that cover a period of time (e.g., rolling 30-day reports, monthly reports), or a combination of both types of reports. The type and frequency of reviews and resulting reports used should be commensurate with the bank's BSA/AML risk profile and appropriately cover its high-risk products, services, customers, and geographic locations.

MIS or vendor system-generated reports typically use a discretionary dollar threshold. Thresholds selected by management for the production of transaction reports should enable management to detect unusual activity. Upon identification of unusual activity, assigned personnel should review CDD and other pertinent information to determine whether the activity is suspicious. Management should periodically evaluate the appropriateness of filtering criteria and thresholds used in the monitoring process. Each bank should evaluate and identify filtering criteria most appropriate for their bank. Typical manual transaction monitoring reports are as follows. In addition, the programming of the bank's monitoring systems should be independently reviewed for reasonable filtering criteria.

Currency Activity Reports: Most vendors offer reports that identify all currency activity or currency activity greater than $10,000. These reports assist bankers with filing Currency Transaction Reports (CTRs) and identifying suspicious currency activity. Most bank information service providers offer currency activity reports that can filter transactions using various parameters, for example:

- Currency activity including multiple transactions greater than $10,000.
- Currency activity (single and multiple transactions) below the $10,000 reporting requirement (e.g., between $7,000 and $10,000).
- Currency transactions involving multiple lower dollar transactions (e.g., $3,000) that over a period of time (e.g., 15 days) aggregate to a substantial sum of money (e.g., $30,000).

Such filtering reports, whether implemented through a purchased vendor software system or through requests from information service providers, will significantly enhance a bank's ability to identify and evaluate unusual currency transactions.

Funds Transfer Records: The BSA requires banks to maintain records of funds transfer in amounts of $3,000 and above. Periodic review of this information can assist banks in identifying patterns of unusual activity. A periodic review of the funds transfer records in banks with low funds transfer activity is usually sufficient to identify unusual activity. For banks with more significant funds transfer activity, use of spreadsheet or vendor software is an efficient way to review funds transfer activity for unusual patterns. Most vendor software systems include standard suspicious activity filter reports. These reports typically focus on identifying certain high-risk geographic locations and larger dollar funds transfer transactions for individuals and businesses. Each bank should establish its own filtering criteria for both individuals and businesses. Noncustomer funds transfer transactions and payable upon proper identification (PUPID) transactions should also be reviewed for unusual activity.

Monetary Instrument Records: Records for monetary instrument sales are required by the BSA. Such records can assist the bank in identifying possible currency structuring through the purchase of cashier's checks, official bank checks, money orders, or traveler's checks in amounts of $3,000 to $10,000. A periodic review of these records can also help identify frequent purchasers of monetary instruments and common payees.

Automated Account Monitoring

Automated account-monitoring systems typically use computer programs, developed in-house or purchased from vendors, to identify individual transactions, patterns of unusual activity, or deviations from expected activity. These systems can capture a wide range of account activity, such as deposits, withdrawals, funds transfers, automated clearing house (ACH) transactions, and automated teller machine (ATM) transactions, directly from the bank's core data processing system. Banks that are large, operate in many locations, or have a large volume of high-risk customers typically use automated account-monitoring systems.

Current types of automated systems include rule-based and intelligent systems. Rule-based systems detect unusual transactions that are outside of system-developed or management-established "rules." Such systems can consist of few or many rules, depending on the complexity of the in-house or vendor product. These rules are applied using a series of transaction filters or a rules engine. Rule-based automated systems are more sophisticated than the basic manual system, which only filters on one rule (e.g., transaction greater than $10,000). Rule-based automated monitoring systems can apply complex or multiple filters. For example, rules-based automated monitoring systems can apply first to all accounts, then to a subset or risk category of accounts (such as all customers with direct deposit or all restaurants). Rule-based monitoring systems can also filter individual customer-account profiles.

Intelligent systems are adaptive systems that can change their analysis over time on the basis of activity patterns, recent trends, changes in the customer base, and other relevant data. Intelligent systems review transactions in context with other transactions and the customer profile. In doing so, these systems increase their information database on the customer, account type, category, or business, as more transactions and data are stored in the system.

Understanding the filtering criteria of a software-based monitoring system is critical to assessing the effectiveness of automated account monitoring systems. System filtering criteria should be developed through a review of specific high-risk customers, products, and services. System filtering criteria, including specific profiles and rules, should be based on what is reasonable and expected for each type of customer. Monitoring customers purely on the basis of historical activity can be misleading if their activity is not actually consistent with similar types of customers. For example, a customer may have a historical transaction activity that is substantially different from what would normally be expected from that type of customer (e.g., a check-cashing business that deposits large sums of currency versus withdrawing currency to fund the cashing of checks).

The authority to establish or change expected activity profiles should be clearly defined and should generally require the approval of the BSA compliance officer or senior management. Controls should ensure limited access to the monitoring system. Management should document or be able to explain filtering criteria, thresholds used, and how both are appropriate for the bank's risks. Management should also periodically review the filtering criteria and thresholds established to ensure that they are still effective. In addition, the bank's programming methodology should be independently validated.

Identifying Underlying Crime

Banks are required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing,[44] and certain other crimes above prescribed dollar thresholds. However, banks are not obligated to investigate or confirm the underlying predicate crime (e.g., terrorist financing, money laundering, tax evasion, identity theft, and various types of fraud). Investigation is the responsibility of law enforcement. When evaluating suspicious activity and completing the SAR, banks should, to the best of their ability, identify the characteristics of the suspicious activity. Part III, section 35, of the SAR provides 20 different characteristics of suspicious activity. Although an "Other" category is available, the use of this category should be limited to situations that cannot be broadly identified within the 20 characteristics provided.

[44] If a bank knows, suspects, or has reason to suspect that a customer may be linked to terrorist activity against the United States, the bank should immediately call FinCEN's Financial Institutions Terrorist Hotline at the toll-free number: 1-866-556-3974. Similarly, if any other suspected violation - such as an ongoing money laundering scheme - requires immediate attention, the bank should notify the appropriate federal banking and law enforcement agencies. In either case, the bank must also file a SAR.

Law Enforcement Inquiries and Requests

Banks should establish policies, procedures, and processes for identifying subjects of law enforcement requests, monitoring the transaction activity of those subjects, identifying unusual or suspicious activity related to those subjects, and filing, as applicable, SARs related to those subjects. Law enforcement inquiries and requests can include criminal subpoenas, national security letters (NSLs), and section 314(a) requests.

Mere receipt of any law enforcement inquiry, does not, by itself, require the filing of a SAR by the bank. Nonetheless, a law enforcement inquiry may be relevant to a bank's overall risk assessment of its customers and accounts. It is incumbent upon a bank to assess all of the information it knows about its customer, including the receipt of a law enforcement inquiry, in accordance with its risk-based BSA/AML compliance program. The bank should determine whether a SAR should be filed based on all customer information available.

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.[45]
- Information from credit bureaus.[46]
- Financial records from financial institutions.[47]

NSLs are highly confidential.[48] Pursuant to 12 USC 3414(a)(3) and (5)(D), no bank, or officer, employee or agent of the institution, can disclose to any person that a government authority or the FBI has sought or obtained access to records through a Right to Financial Privacy Act NSL. Banks that receive NSLs must take appropriate measures to ensure the confidentiality of the letters and should have procedures in place for processing and maintaining the confidentiality of NSLs.

If a bank files a SAR after receiving a 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 bank.

---

[45] Electronic Communications Privacy Act, 18 USC 2709.

[46] Fair Credit Reporting Act, 15 USC 1681u.

[47] Right to Financial Privacy Act of 1978, 12 USC 3401 *et seq.*

[48] Refer to the *SAR Activity Review*, Issue 8, April 2005 for further information on NSLs which is available at www.fincen.gov.

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

SAR DECISION-MAKING PROCESS

The bank should have policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity. The process should ensure that all applicable information (e.g., criminal subpoenas, NSLs, or section 314(a) requests) is effectively evaluated.

Banks are encouraged to document SAR decisions. Thorough documentation provides a record of the SAR decision-making process, including final decisions not to file a SAR. The decision to file a SAR is an inherently subjective judgment. Examiners should focus on whether the bank has an effective SAR decision-making process, not individual SAR decisions. Examiners may review individual SAR decisions as a means to test the effectiveness of the SAR monitoring, reporting, and decision-making process. In those instances where the bank has an established SAR decision-making process, has followed existing policies, procedures, and processes and has determined not to file a SAR, the bank should not be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.

TIMING OF A SAR FILING

The SAR rules require that a SAR be filed no later than 30 calendar days from the date of the initial detection of the suspicious activity, unless no suspect can be identified. In that case, the time period for filing a SAR is extended to 60 days. Organizations may need to review transaction or account activity for a customer to determine whether to file a SAR. The need for a review of customer activity or transactions does not necessarily indicate a need to file a SAR. The time period for filing a SAR starts when the organization, during its review 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.[49]

Whenever possible, an expeditious review of the transaction or the account is recommended and can be of significant assistance to law enforcement. In any event, the review should be completed in a reasonable period of time. For violations requiring immediate attention, such as when a reportable violation is ongoing, a bank is required to immediately notify, by telephone, an "appropriate law enforcement authority" and as necessary the bank's primary regulator, in addition to filing a timely SAR. An "appropriate law enforcement authority" would generally be the local office of the Internal Revenue Service Criminal Investigation Division or the FBI. Notifying law enforcement of a suspicious activity does not relieve a bank of its obligation to file a SAR.

[49] Bank Secrecy Act Advisory Group, "Section 5 – Issues and Guidance" *The SAR Activity Review – Trends, Tips & Issues*, October 2000, page 27.

BOARD OF DIRECTORS' NOTIFICATION

Banks are required by the SAR regulations of their federal banking agency to notify the board of directors or an appropriate board committee that SARs have been filed.[50] However, the regulations do not mandate a particular notification format and banks should have flexibility in structuring their format. Therefore, banks may, but are not required to, provide actual copies of SARs to the board of directors or a board committee. Alternatively, banks may opt to provide summaries, tables of SARs filed for specific violation types, or other forms of notification. Regardless of the notification format used by the bank, management should provide sufficient information on its SAR filings to the board of directors or an appropriate committee in order to fulfill its fiduciary duties.[51]

SAR FILING ON CONTINUING ACTIVITY

One purpose of filing SARs is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. This objective is accomplished by the filing of a SAR that identifies the activity of concern. If this activity continues over a period of time, such information should be made known to law enforcement (and the federal banking agencies). FinCEN's guidelines suggest that banks should report continuing suspicious activity by filing a report at least every 90 days.[52] This practice will notify law enforcement of the continuing nature of the activity, as well as remind the bank that it should continue to review the suspicious activity to determine whether other actions may be appropriate, such as bank management determining that it is necessary to terminate a relationship with the customer or employee that is the subject of the filing.

The bank should develop policies, procedures, and processes indicating when to escalate issues or problems identified as result of repeat SAR filings on accounts. The procedures should include:

- Review by senior management and legal staff (e.g., BSA compliance officer or SAR committee).
- Criteria for when analysis of the overall customer relationship is necessary.
- Criteria for when to close the account.
- Criteria for when to notify law enforcement, if applicable.

---

[50] Credit unions do not have a regulatory requirement to notify the board of directors of SAR filings, although many take this action as a matter of a sound practice.

[51] As noted in the *SAR Activity Review*, Issue 2, June 2001, "In the rare instance when suspicious activity is related to an individual in the organization, such as the president or one of the members of the board of directors, the established policy that would require notification of a SAR filing to such an individual should not be followed. Deviations to established policies and procedures so as to avoid notification of a SAR filing to a subject of the SAR should be documented and appropriate uninvolved senior organizational personnel should be so advised."

[52] Id.

SAR QUALITY

Banks are required to file SAR forms that are complete, thorough, and timely. Banks should include all known suspect information on the SAR form, and the importance of the accuracy of this information cannot be overstated. Inaccurate information on the SAR form, or an incomplete or disorganized narrative, may make further analysis difficult, if not impossible. However, there may be legitimate reasons why certain information may not be provided in a SAR, such as when the filer does not have the information. A thorough and complete narrative may make the difference in whether the described conduct and its possible criminal nature are clearly understood by law enforcement. Because the SAR narrative section is the only area summarizing suspicious activity, the narrative section, as stated on the SAR form, is "critical." Thus, a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.

By their nature, SAR narratives are subjective, and examiners generally should not criticize the bank's interpretation of the facts. Nevertheless, banks should ensure that SAR narratives are complete, thoroughly describe the extent and nature of the suspicious activity, and is included within the SAR form (e.g., no attachments to the narrative section will be included within the BSA-reporting database). More specific guidance is available in Appendix L ("SAR Quality Guidance") to assist banks in writing and assist examiners in evaluating, SAR narratives. In addition, comprehensive guidance is available from FinCEN ("Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative") at www.fincen.gov.

PROHIBITION OF SAR DISCLOSURE

No bank, and no director, officer, employee, or agent of a bank, that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. Thus, any person subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR, except when such disclosure is requested by FinCEN or an appropriate law enforcement or federal banking agency, shall decline to produce the SAR or to provide any information that would disclose that a SAR has been prepared or filed, citing 31 CFR 103.18(e) and 31 USC 5318(g)(2). FinCEN and the bank's federal banking agency should be notified of any such request and of the bank's response. Furthermore, FinCEN and the federal banking agencies take the position that banks' internal controls for the filing of SARs should minimize the risks of disclosure.

RECORD RETENTION

Banks must retain copies of SARs and supporting documentation for five years from the date of the report.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – Currency Transaction Reporting

OBJECTIVE

Assess the bank's compliance with statutory and regulatory requirements for the reporting of large currency transactions.

OVERVIEW

A bank must file a Currency Transaction Report (CTR) (FinCEN Form 104) for each transaction in currency[53] (deposit, withdrawal, exchange or other payment or transfer) of more than $10,000 by, through, or to the bank. Certain types of currency transactions need not be reported, such as those involving "exempt persons," a group which can include retail or commercial customers meeting specific criteria for exemption. Refer to the core overview section "Currency Transaction Reporting Exemptions" on page 51.

AGGREGATION OF CURRENCY TRANSACTIONS

Multiple currency transactions totaling more than $10,000 during any one business day are treated as a single transaction if the bank has knowledge that they are by or on behalf of the same person. Transactions throughout the bank should be aggregated when determining multiple transactions. Types of currency transactions subject to reporting requirements individually or by aggregation include, but are not limited to, denomination exchanges, individual retirement accounts (IRAs), loan payments, automated teller machine (ATM) transactions, purchases of certificates of deposit, deposits and withdrawals, funds transfers paid for in currency, and monetary instrument purchases. Banks are strongly encouraged to develop systems necessary to aggregate currency transactions throughout the bank. Management should ensure that an adequate system is implemented that will appropriately report currency transactions subject to the BSA requirement.

FILING TIME FRAMES AND RECORD RETENTION REQUIREMENTS

A completed CTR must be filed with FinCEN within 15 days after the date of the transaction (25 days if filed magnetically or electronically). The bank must retain copies of CTRs for five years from the date of the report. (31 CFR 103.27(a)(3)).

[53] Currency is defined as coin and paper money of the United States or any other country as long as it is customarily accepted as money in the country of issue.

CTR BACKFILING

If a bank has failed to file CTRs on reportable transactions, the bank should begin filing CTRs and should contact the Internal Revenue Service (IRS) Detroit Computing Center[54] to request a determination on whether the backfiling of unreported transactions is necessary.

[54] The IRS Detroit Computing Center is a central repository for the BSA reports that banks must file. The IRS Detroit Computing Center can be contacted at 800-800-2877.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – Currency Transaction Reporting Exemptions

OBJECTIVE

Assess the bank's compliance with statutory and regulatory requirements for exemptions from the currency transaction reporting requirements.

OVERVIEW

U.S. Treasury regulations have historically recognized that the routine reporting of some types of large currency transactions does not necessarily aid law enforcement authorities and may place unreasonable burdens on banks. Consequently, a bank may exempt certain types of customers from currency transaction reporting.

The Money Laundering Suppression Act of 1994 (MLSA) established a two-phase exemption process. Under Phase I exemptions, transactions in currency by banks, governmental departments or agencies, and public or listed companies and their subsidiaries are exempt from reporting. Under Phase II exemptions, transactions in currency by smaller businesses that meet specific criteria laid out in FinCEN's regulations may be exempted from reporting. To exempt a customer from CTR reporting, a bank must file a Designation of Exempt Person form (TD F 90-22.53).

PHASE I CTR EXEMPTIONS (31 CFR 103.22(d)(2)(i)-(v))

FinCEN's rule identifies five categories of Phase I exempt persons:

- A bank, to the extent of its domestic operations.
- A federal, state or local government agency or department.
- Any entity exercising governmental authority within the United States.
- Any entity (other than a bank) whose common stock is listed on the New York, American, or Nasdaq stock exchanges (with some exceptions).
- Any subsidiary (other than a bank) of any "listed entity" that is organized under U.S. law and at least 51 percent of whose common stock is owned by the listed entity.

Filing Time Frames

Banks must file a one-time Designation of Exempt Person form to exempt a Phase I entity from currency transaction reporting. The exemption of a Phase I entity covers all transactions in currency with the exempted entity, not only transactions in currency conducted through an account. The form must be filed with the Internal Revenue Service (IRS) within 30 days after the first transaction in currency that the bank wishes to exempt.

Annual Review

The information supporting each designation of a Phase I exempt person must be reviewed and verified by the bank at least once per year.

PHASE II CTR EXEMPTIONS (31 CFR 103.22(d)(2)(vi)-(vii))

A business that does not fall into any of the Phase I categories may still be exempted under the Phase II exemptions if it qualifies as either a "non-listed business" or as a "payroll customer."

Non-Listed Businesses

A "non-listed business" is defined as a commercial enterprise to the extent of its domestic operations and only with respect to transactions conducted through its exemptible accounts and that (i) has maintained a transaction account at the exempting bank for at least 12 months; (ii) frequently[55] engages in transactions in currency with the bank in excess of $10,000, and (iii) 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.

Ineligible Businesses

Certain businesses are ineligible for treatment as an exempt non-listed business, (31 CFR 103.22(d)(6)(viii)). An ineligible business is defined as a business engaged primarily in one or more of the following specified activities:

- Serving as a financial institution or as agents for financial institution of any type.
- Purchasing or selling motor vehicles of any kind, vessels, aircraft, farm equipment, or mobile homes.
- Practicing law, accounting, or medicine.
- Auctioning of goods.
- Chartering or operation of ships, buses, or aircraft.
- Operating a pawn brokerage.
- Engaging in gaming of any kind (other than licensed pari-mutuel betting at race tracks).
- Engaging in investment advisory services or investment banking services.

[55] FinCEN has issued a directive ("Guidance on Interpreting 'Frequently' Found in the Criteria for Exempting a 'Non-Listed Business' under 31 CFR 103.22(d)(2)(vi)(B), November 2002," www.fincen.gov) which states, "In general, a customer that is being considered for exemption as a non-listed business should be conducting at least eight large currency transactions throughout the year. In essence, this means the customer conducts a large currency transaction approximately every six weeks. The fact a customer conducts fewer than eight large currency transactions annually would generally indicate that any large currency transactions conducted do not relate to a recurring or routine need."

- Operating a real estate brokerage.
- Operating in title insurance activities and real estate closings.
- Engaging in trade union activities.
- Engaging in any other activity that may, from time to time, be specified by FinCEN.

A business that engages in multiple business activities may qualify for an exemption as a non-listed business as long as no more than 50 percent of its gross revenues per year[56] are derived from one or more of the ineligible business activities listed in the rule.

Payroll Customers

A "payroll customer" is defined solely with respect to withdrawals for payroll purposes from existing exemptible accounts and as a person who: (i) has maintained a transaction account at the bank for at least 12 months; (ii) operates a firm that regularly withdraws more than $10,000 in order to pay its U.S. employees in currency; and (iii) 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.

Filing Time Frames

After a bank has decided to exempt a Phase II customer, the bank must file an initial Designation of Exempt Person form (TD F 90-22.53) within 30 days after the first customer transaction the bank wishes to exempt.

Annual Review

The information supporting each designation of a Phase II exempt person must be reviewed and verified by the bank at least once per year. Moreover, consistent with this annual review, a bank must review and verify at least once each year that management monitors these Phase II accounts for suspicious transactions.

Biennial Renewals

Additionally, for Phase II customers, the form must be refiled every two years, on or before March 15, as part of the biennial renewal process. Under the biennial renewal process applicable to Phase II customers, a bank must include the following information on the biennial renewal: (i) any change in control of the exempt person known to the bank (or for which the bank has reason to know) and (ii) a certification that the bank has

[56] Questions often arise in determining the "gross revenue" of gaming activities, such as lottery sales. FinCEN has ruled that for the purpose of determining if a business derives more than 50 percent of its gross revenue from gaming, the term gross revenue is intended to encompass the amount of money that a business actually earns from a particular activity, rather than the sales volume of such activity conducted by the business. For example, if a business engages in lottery sales, the "gross revenue" from this activity would be the amount of money that the business actually earns from lottery sales, rather than the amount of money that the business takes in on behalf of the state lottery system. See FinCEN Ruling 2002-1, www.fincen.gov.

applied its suspicious activity monitoring system to transactions in currency of the exempt person as necessary, but at least annually.

SAFE HARBOR FOR FAILURE TO FILE CTRs

The rules (31 CFR 103.22(d)(8)) provide a safe harbor that a bank is not liable for the failure to file a CTR for a transaction in currency by an exempt person, unless the bank knowingly provides false or incomplete information or has reason to believe that the customer does not qualify as an exempt customer. In the absence of any specific knowledge or information indicating that a customer no longer meets the requirements of an exempt person, the bank is entitled to a safe harbor from civil penalties to the extent it continues to treat that customer as an exempt customer until the date of the customer's annual review.

EFFECT ON OTHER REGULATORY REQUIREMENTS

The exemption procedures do not create any exemption, or have any effect at all, on the requirement that banks file SARs. For example, the fact that a customer is an exempt person has no effect on a bank's obligation to retain records of funds transfers by that person, or to retain records in connection with the sale of monetary instruments to that person.

If a bank has improperly exempted accounts, the examiner may require management to revoke the exemption. In any case, the bank should begin filing CTRs and should contact the Internal Revenue Service (IRS) Detroit Computing Center[57] to request a determination on whether the backfiling of unreported transactions is necessary.

Additional information about the currency transaction exemption process can be found on FinCEN's web site at www.fincen.gov.

[57] The IRS Detroit Computing Center is a central repository for the BSA reports that banks must file. The IRS Detroit Computing Center can be contacted at 800-800-2877.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – Information Sharing

OBJECTIVE

Assess the financial institution's compliance with the statutory and regulatory requirements for the "Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity" (section 314 Information Requests).

OVERVIEW

On September 26, 2002, final regulations (31 CFR 103.100 and 31 CFR 103.110) implementing section 314 of the Patriot Act became effective. The regulations established procedures for information sharing to deter money laundering and terrorist activity.

INFORMATION SHARING BETWEEN LAW ENFORCEMENT AND FINANCIAL INSTITUTIONS - SECTION 314(a) OF THE PATRIOT ACT (31 CFR 103.100)

A federal law enforcement agency investigating terrorist activity or money laundering may request that FinCEN solicit, on its behalf, certain information from a financial institution or a group of financial institutions. The law enforcement agency must provide a written certification to FinCEN attesting that there is credible evidence of engagement or reasonably suspected engagement in terrorist activity or money laundering for each individual, entity, or organization about which the law enforcement agency is seeking information. The law enforcement agency also must provide specific identifiers, such as a date of birth and address, which would permit a financial institution to differentiate among common or similar names. Upon receiving a completed written certification from a law enforcement agency, FinCEN may require a financial institution to search its records to determine whether it maintains or has maintained accounts for, or has engaged in transactions with, any specified individual, entity, or organization.

Upon receiving an information request, a financial institution must conduct a one-time search of its records to identify accounts or transactions of a named suspect. Unless otherwise instructed by an information request, financial institutions must search their records for current accounts, accounts maintained during the preceding 12 months, and transactions conducted outside of an account by or on behalf of a named suspect during the preceding six months. The financial institution must search its records and report any positive matches to FinCEN within 14 days, unless otherwise specified in the information request.

FinCEN has provided financial institutions with General Instructions and Frequently Asked Questions (FAQs) relating to the section 314(a) process. Unless otherwise instructed by an information request, financial institutions must search the records specified in the General Instructions. A financial institution may obtain additional or replacement copies of the General Instructions or FAQs by contacting FinCEN.

If a financial institution identifies any account or transaction, it must report to FinCEN that it has a match. No details should be provided to FinCEN other than the fact that the financial institution has a match. A negative response is not required. A financial institution may provide a list of named suspects to a third-party service provider or vendor to perform or facilitate record searches as long as the institution takes the necessary steps, through the use of an agreement or procedures, to ensure that the third party safeguards and maintains the confidentiality of the information.

Financial institutions should develop and implement comprehensive policies, procedures, and processes for responding to section 314(a) requests. The regulation restricts the use of the information provided in a section 314(a) request (31 CFR 103.100(b)(2)(iv)).[58] A financial institution may only use the information to report the required information to FinCEN, to determine whether to establish or maintain an account or engage in a transaction, or to assist in BSA/AML compliance. While the section 314(a) list could be used to determine whether to establish or maintain an account, FinCEN strongly discourages financial institutions from using this as the sole factor in reaching a decision to do so unless the request specifically states otherwise. Unlike the OFAC lists, section 314(a) lists are not permanent "watch lists." In fact, section 314(a) lists generally relate to one-time inquiries and are not updated or corrected if an investigation is dropped, a prosecution is declined, or a subject is exonerated. Further, the names do not correspond to convicted or indicted persons; rather a 314(a) subject need only be "reasonably suspected" based on credible evidence of engaging in terrorist acts or money laundering. Moreover, FinCEN advises that inclusion on a section 314(a) list should not be the sole factor used to determine whether to file a Suspicious Activity Report (SAR). Financial institutions should establish a process for determining when and if a SAR should be filed.

Actions taken pursuant to information provided in a request from FinCEN do not affect a financial institution's obligations to comply with all of the rules and regulations of OFAC nor do they affect a financial institution's obligations to respond to any legal process. Additionally, actions taken in response to a request do not relieve a financial institution of its obligation to file a SAR and immediately notify law enforcement, if necessary, in accordance with applicable laws and regulations.

A financial institution cannot disclose to any person, other than to FinCEN, the institution's primary bank regulator, or the federal law enforcement agency on whose behalf FinCEN is requesting information, the fact that FinCEN has requested or obtained information. A financial institution should designate one or more point-of-contacts for receiving information requests. FinCEN has stated that an affiliated group of financial institutions may establish one point-of-contact to distribute the section 314(a) list to

[58] If the request contains multiple suspects, it is often referred to as a "314(a) list."

respond to requests. However, the section 314(a) lists cannot be shared with any foreign office, branch or affiliate (unless the request specifically states otherwise), and the lists cannot be shared with affiliates, or subsidiaries of bank holding companies, if the affiliates or subsidiaries are not financial institutions as described in 31 USC 5312(a)(2).

Each financial institution must maintain adequate procedures to protect the security and confidentiality of requests from FinCEN. The procedures to ensure confidentiality will be considered adequate if the financial institution applies procedures similar to those it has established to comply with section 501 of the Gramm-Leach-Bliley Act (15 USC 6801) for the protection of its customers' nonpublic personal information. Financial institutions may keep a log of all section 314(a) requests received and of any positive matches identified and reported to FinCEN.

Additionally, documentation that all required searches were performed is essential. This may be accomplished by maintaining copies of the cover page of the request with a bank sign-off that the records were checked, the date of the search, and search results (e.g., positive or negative). For positive matches, copies of the form returned to FinCEN and the supporting documentation should be retained. If the financial institution elects to maintain copies of the section 314(a) requests, it should not be criticized for doing so, as long as it appropriately secures them and protects their confidentiality. Audits should include an evaluation of compliance with these guidelines within their scope.

In March 2005, FinCEN began distributing section 314(a) subject lists through a secure web site. Every two weeks, or if an emergency request is transmitted, the bank's designated point of contact will receive notification from FinCEN that there are new postings to FinCEN's secure site. The point of contact will be able to access the current, and one prior, section 314(a) subject lists and download the files in various formats for searching. In addition, the banks can use FinCEN's web site to notify FinCEN of positive matches. Those banks receiving the section 314(a) subject lists by facsimile transmission will continue to receive the lists in that manner.

Each bank should contact its primary federal regulator for guidance to ensure it obtains the section 314(a) list and for updating contact information.[59]

VOLUNTARY INFORMATION SHARING - SECTION 314(b) OF THE PATRIOT ACT (31 CFR 103.110)

Section 314(b) encourages financial institutions and associations of financial institutions located in the United States to share information in order to identify and report activities that may involve terrorist activity or money laundering. Section 314(b) also provides specific protection from civil liability. To avail itself of this statutory safe harbor from liability, a financial institution or an association must notify FinCEN of its intent to engage in information sharing and that it has established and will maintain adequate

[59] Refer to the FinCEN web site www.fincen.gov, for section 314(a) contacts for each primary regulator.

procedures to protect the security and confidentiality of the information. Failure to comply with the requirements of 31 CFR 103.110 will result in loss of safe harbor protection for information sharing and may result in a violation of privacy laws or other laws and regulations.

If a financial institution chooses to voluntarily participate in section 314(b), policies, procedures, and processes should be developed and implemented for sharing and receiving of information.

A notice to share information is effective for one year.[60] The financial institution should designate a point-of-contact for receiving and providing information. A financial institution should establish a process for sending and receiving information sharing requests. Additionally, a financial institution must take reasonable steps to verify that the other financial institution or association of financial institutions with which it intends to share information has also submitted the required notice to FinCEN. FinCEN provides participating financial institutions with access to a list of other participating financial institutions and their related contact information.

If a financial institution receives such information from another financial institution, it must also limit use of the information and maintain its security and confidentiality (see 31 CFR 103.110(b)(4)). Such information may be used only to identify and, where appropriate, report on money laundering and terrorist activities; to determine whether to establish or maintain an account; to engage in a transaction; or to assist in BSA compliance. The procedures to ensure confidentiality will be considered adequate if the financial institution applies procedures similar to the ones it has established to comply with section 501 of the Gramm-Leach-Bliley Act (15 USC 6801) for the protection of its customers' nonpublic personal information. The safe harbor does not extend to sharing of information across international borders. In addition, section 314(b) does not authorize a financial institution to share a SAR, nor does it permit the financial institution to disclose the existence or nonexistence of a SAR. If a financial institution shares information under section 314(b) about the subject of a prepared or filed SAR, the information shared should be limited to underlying transactional and customer information. A financial institution may use information obtained under section 314(b) to determine whether to file a SAR, but the intention to prepare or file a SAR cannot be shared with another financial institution. Financial institutions should establish a process for determining when and if a SAR should be filed.

Actions taken pursuant to information obtained through the voluntary information sharing process do not affect a financial institution's obligations to respond to any legal process. Additionally, actions taken in response to information obtained through the voluntary information sharing process do not relieve a financial institution of its obligation to file a SAR and to immediately notify law enforcement, if necessary, in accordance with all applicable laws and regulations.

[60] Instructions on submitting a notification form are available on FinCEN's web site: www.fincen.gov.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – Purchase and Sale of Monetary Instruments

OBJECTIVE

Assess the bank's compliance with statutory and regulatory requirements for the recording of information required for the purchase and sale of monetary instruments for currency in amounts between $3,000 and $10,000, inclusive. This section covers the regulatory requirements as set forth by the BSA. Refer to the expanded sections of this manual for additional discussions and procedures on specific money laundering risks for purchase and sale of monetary instruments activities.

OVERVIEW

Banks sell a variety of monetary instruments (e.g., bank checks or drafts, including foreign drafts, money orders, cashier's checks, and traveler's checks) in exchange for currency. Purchasing these instruments in amounts of less than $10,000 is a common method used by money launderers to evade large currency transaction reporting requirements. Once converted from currency, criminals typically deposit these instruments in accounts with other banks to facilitate the movement of funds through the payment system. In many cases, the persons involved do not have an account with the bank from which the instruments are purchased.

PURCHASER VERIFICATION

Under 31 CFR 103.29 banks are required to verify the identity of persons purchasing monetary instruments for currency in amounts between $3,000 and $10,000, inclusive, and to maintain records of all such sales.

Banks may either verify that the purchaser of monetary instruments is a deposit accountholder with identifying information on record with the bank or a bank may verify the identity of the purchaser by viewing a form of identification that contains the customer's name and address and that the financial community accepts as a means of identification when cashing checks for noncustomers. The bank must obtain additional information for purchasers who do not have deposit accounts. The method used to verify the identity of the purchaser must be recorded.

ACCEPTABLE IDENTIFICATION

The U.S. Treasury's Administrative Ruling 92-1 provides guidance on how a bank can verify the identity of an elderly or disabled customer who does not possess the normally acceptable forms of identification. A bank may accept a Social Security card or a Medicare/Medicaid card along with another form of documentation bearing the

customer's name and address. Additional forms of documentation include a utility bill, a tax bill, or a voter registration card. The forms of alternate identification a bank decides to accept should be included in its formal policies, procedures, and processes.

CONTEMPORANEOUS PURCHASES

Contemporaneous purchases of the same or different types of instruments totaling $3,000 or more must be treated as one purchase. Multiple purchases during one business day totaling $3,000 or more must be aggregated and treated as one purchase if the bank has knowledge that the purchases have occurred.

INDIRECT CURRENCY PURCHASES OF MONETARY INSTRUMENTS

Banks may implement a policy requiring customers who are deposit accountholders and who want to purchase monetary instruments in amounts between $3,000 and $10,000 with currency to first deposit the currency into their deposit accounts. Nothing within the BSA, or its implementing regulations prohibits a bank from instituting such a policy.

However, FinCEN takes the position[61] that when a customer purchases a monetary instrument in amounts between $3,000 and $10,000 using currency that the customer first deposits into the customer's account, the transaction is still subject to the recordkeeping requirements of 31 CFR 103.29. This requirement applies whether the transaction is conducted in accordance with a bank's established policy or at the request of the customer. Generally, when a bank sells monetary instruments to deposit accountholders, the bank will already maintain most of the information required by 31 CFR 103.29 in the normal course of its business.

RECORDKEEPING AND RETENTION REQUIREMENTS

Under 31 CFR 103.29, a bank's records of sales must contain, at a minimum, the following information:

- If the purchaser **has a deposit account** with the bank:
  - Name of the purchaser.
  - Date of purchase.
  - Types of instruments purchased.
  - Serial numbers of each of the instruments purchased.

[61] FinCEN's "Guidance on Interpreting Financial Institution Policies in Relation to Recordkeeping Requirements under 31 CFR 103.29," November 2002, www.fincen.gov.

- Dollar amounts of each of the instruments purchased in currency.
- Specific identifying information, if applicable.[62]

- If the purchaser **does not have a deposit account** with the bank:

  - Name and address of the purchaser.
  - Social Security or alien identification number of the purchaser.
  - Date of birth of the purchaser.
  - Date of purchase.
  - Types of instruments purchased.
  - Serial numbers of each of the instruments purchased.
  - Dollar amounts of each of the instruments purchased.
  - Specific identifying information for verifying the purchaser's identity (e.g., state of issuance and number on driver's license).

If the purchaser cannot provide the required information at the time of the transaction or through the bank's own previously verified records, the transaction should be refused. The records of monetary instrument sales must be retained for five years and be available to the appropriate agencies upon request.

[62] The bank must verify that the person is a deposit accountholder or must verify the person's identity. Verification may be either through a signature card or other file or record at the bank, provided the deposit accountholder's name and address were verified previously and that information was recorded on the signature card or other file or record, or by examination of a document that is normally acceptable within the banking community and that contains the name and address of the purchaser. If the deposit accountholder's identity has not been verified previously, the bank shall record the specific identifying information (e.g., state of issuance and number of driver's license) of the document examined.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – Funds Transfers

OBJECTIVE

Assess the bank's compliance with statutory and regulatory requirements for funds transfers. This section covers the regulatory requirements as set forth by the BSA. Refer to the expanded sections of this manual for discussions and procedures regarding specific money laundering risks for funds transfer activities.

OVERVIEW

Funds transfer systems enable the instantaneous transfer of funds, including both domestic and cross-border transfers. Consequently these systems can present an attractive method to disguise the source of funds derived from illegal activity. The BSA was amended by the Annunzio-Wylie Anti-Money Laundering Act of 1992 to authorize the U.S. Treasury and the Federal Reserve Board to prescribe regulations for domestic and international funds transfers.

In 1995, the U.S. Treasury and the Board of Governors of the Federal Reserve System issued a final rule on recordkeeping requirements concerning payment orders by banks (31 CFR 103.33).[63] The rule requires each bank involved in funds transfers[64] to collect and retain certain information in connection with funds transfers of $3,000 or more.[65] The information required to be collected and retained depends on the bank's role in the particular funds transfer (originator's bank, intermediary bank, or beneficiary's bank).[66] The requirements may also vary depending on whether an originator or beneficiary is an

[63] 31 CFR 103.33(e) is the recordkeeping rule for banks, and 31 CFR 103.33(f) imposes similar requirements for non-bank financial institutions that engage in funds transfers. The procedures in this core overview address only the rules for banks in 31 CFR 103.33(e).

[64] Funds transfer is defined under 31 CFR 103.11. Funds transfers governed by the Electronic Fund Transfer Act of 1978, as well as any other funds transfers that are made through an automated clearing house, an automated teller machine, or a point-of-sale system, are excluded from this definition and exempt from the requirements of 103.33(e), (f) and (g).

[65] 31 CFR 103.33(e)(6) provides exceptions to the funds transfer requirements. 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 not subject to the recordkeeping requirements for funds transfers. Additionally, exceptions are provided from the recordkeeping requirements for funds transfers where the originator and beneficiary are: a bank; a wholly owned domestic subsidiary of a bank chartered in the United States; a broker or dealer in securities; a wholly-owned domestic subsidiary of a broker or dealer in securities; the United States; a state or local government; or a federal, state or local government agency or instrumentality.

[66] These terms are defined under 31 CFR 103.11.

established customer of a bank and whether a payment order is made in person or otherwise.

Also in 1995, the U.S. Treasury issued a final rule that requires all financial institutions to include certain information in transmittal orders for funds transfers of $3,000 or more (31 CFR 103.33).[67] This requirement is commonly referred to as the "Travel Rule."

RESPONSIBILITIES OF ORIGINATOR'S BANKS

Recordkeeping Requirements

For each payment order in the amount of $3,000 or more that a bank accepts as an originator's bank, the bank must obtain and retain the following records (31 CFR 103.33(e)(1)(i)):

- Name and address of the originator.
- Amount of the payment order.
- Date of the payment order.
- Any payment instructions.
- Identity of the beneficiary's institution.
- As many of the following items as are received with the payment order:
  - Name and address of the beneficiary.
  - Account number of the beneficiary.
  - Any other specific identifier of the beneficiary.

Additional Records for Non-Established Customers

If the originator is not an established customer of the bank, collect and retain the information listed above. In addition, the originator's bank must collect and retain other information, depending on whether the payment order is made in person.

Payment Orders Made in Person

If the payment order is made in person, the originator's bank must verify the identity of the person placing the payment order before it accepts the order. If it accepts the payment order, the originator's financial institution must obtain and retain the following records:

- Name and address of the person placing the order.
- Type of identification reviewed.

[67] The rule applies to both banks and non-banks (31 CFR 103.33(g)). Because it is broader in scope, the Travel Rule uses more expansive terms, such as "transmittal order" instead of "payment order" and "transmittor's financial institution" instead of "originating bank." The broader terms include the bank-specific terms.

- Number of the identification document (e.g., driver's license).
- The person's taxpayer identification number (TIN) (e.g., Social Security number (SSN) or employer identification number (EIN)) or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof. If the originator's bank has knowledge that the person placing the payment order is not the originator, the originator's bank must obtain and record the originator's TIN (e.g., SSN or EIN) or, if none, the alien identification number or passport number and country of issuance, or a notation of the lack thereof.

Payment Orders Not Made in Person

If a payment order is not made in person, the originator's bank must obtain and retain the following records:

- Name and address of the person placing the payment order.
- The person's TIN (e.g., SSN or EIN) or, if none, the alien identification number or passport number and country of issuance , or a notation in the record of the lack thereof, and a copy or record of the method of payment (e.g., check or credit card transaction) for the funds transfer. If the originator's bank has knowledge that the person placing the payment order is not the originator, the originator's bank must obtain and record the originator's TIN (e.g., SSN or EIN) or, if none, the alien identification number or passport number and country of issuance, or a notation of the lack thereof.

Retrievability

Information retained must be retrievable by reference to the name of the originator. When the originator is an established customer of the bank and has an account used for funds transfers, information retained must also be retrievable by account number (31 CFR 103.33(e)(4)). Records must be maintained for five years.

Travel Rule Requirement

For funds transmittals of $3,000 or more, the transmittor's financial institution must include the following information in the transmittal order at the time that a transmittal order is sent to a receiving financial institution (31 CFR 103.33(g)(1)):

- Name of the transmittor, and, if the payment is ordered from an account, the account number of the transmittor.
- Address of the transmittor.
- Amount of the transmittal order.
- Date of the transmittal order.
- Identity of the recipient's financial institution.

- As many of the following items as are received with the transmittal order:

  - Name and 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 transmittor's financial institution.

There are no recordkeeping requirements in the Travel Rule.

RESPONSIBILITIES OF INTERMEDIARY INSTITUTIONS

Recordkeeping Requirements

For each payment order of $3,000 or more that a bank accepts as an intermediary bank, the bank must retain a record of the payment order.

Travel Rule Requirements

For funds transmittals of $3,000 or more, the intermediary financial institution must include the following information if received from the sender in a transmittal order at the time that order is sent to a receiving financial institution (31 CFR 103.33(g)(2)):

- Name and account number of the transmittor.
- Address of the transmittor.
- Amount of the transmittal order.
- Date of the transmittal order.
- Identity of the recipient's financial institution.
- As many of the following items as are received with the transmittal order:

  - Name and 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 transmittor's financial institution.

Intermediary financial institutions must pass on all of the information received from a transmittor's financial institution or the preceding financial institution, but they have no duty to obtain information not provided by the transmittor's financial institution or the preceding financial institution.

RESPONSIBILITIES OF BENEFICIARY'S BANKS

Recordkeeping Requirements

For each payment order of $3,000 or more that a bank accepts as a beneficiary's bank, the bank must retain a record of the payment order.

If the beneficiary is not an established customer of the bank, the beneficiary's institution must retain the following information for each payment order of $3,000 or more.

Proceeds Delivered in Person

If proceeds are delivered in person to the beneficiary or its representative or agent, the institution must verify the identity of the person receiving the proceeds and retain a record of the following:

- Name and address.
- The type of document reviewed.
- The number of the identification document.
- The person's TIN, or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof.
- If the institution has knowledge that the person receiving the proceeds is not the beneficiary, the institution must obtain and retain a record of the beneficiary's name and address, as well as the beneficiary's identification.

Proceeds Not Delivered in Person

If proceeds are not delivered in person, the institution must retain a copy of the check or other instrument used to effect the payment, or the institution must record the information on the instrument. The institution must also record the name and address of the person to which it was sent.

Retrievability

Information retained must be retrievable by reference to the name of the beneficiary. When the beneficiary is an established customer of the institution and has an account used for funds transfers, information retained must also be retrievable by account number (31 CFR 103.33(e)(4)).

There are no Travel Rule requirements for beneficiary banks.

EXPIRATION OF THE CONDITIONAL CUSTOMER INFORMATION FILE EXCEPTION - TRAVEL RULE

From 1998 to 2004, a conditional exception to the Travel Rule generally permitted banks to include a customer's coded name or pseudonym in a transmittal order, provided that the bank maintained the customer's full information in an automated customer information file (CIF). FinCEN revoked this exception, known as the "CIF exception," as of July 1, 2004. After that date institutions must use a customer's true name and address to comply with the Travel Rule. At this time, banks may still be examined where transactions subject to the CIF exception may be included in the examiner's sample for transaction testing.

ABBREVIATIONS AND ADDRESSES

Although the Travel Rule does not permit the use of coded names or pseudonyms, the rule does allow the use of abbreviated names, names reflecting different accounts of a corporation (e.g., XYZ Payroll Account), and trade and assumed names of a business (doing business as) or the names of unincorporated divisions or departments of the business.

Customer Address

The term "address," as used in 31 CFR 103.33(g), is not defined. Previously issued guidance from FinCEN had been interpreted as not allowing the use of mailing addresses in a transmittal order when a street address is known to the transmittor's financial institution. However, in the November 28, 2003, *Federal Register* notice,[68] FinCEN issued a regulatory interpretation that states the Travel Rule should allow the use of mailing addresses, including post office boxes, in the transmittor address field of transmittal orders in certain circumstances.

The regulatory interpretation states that, for purposes of 31 CFR 103.33(g), the term "address" means either the transmittor's street address or the transmittor's address maintained in the financial institution's automated CIF (such as a mailing address including a post office box) as long as the institution maintains the transmittor's address[69] on file and the address information is retrievable upon request by law enforcement.

[68] See 68 *Federal Register* 66708 at www.fincen.gov.

[69] Consistent with the final rules issued under section 326 of the Patriot Act an "address" for purposes of the Travel Rule is as follows: for a person, is a residential or business street address, an Army Post Office Box or a Fleet Post Office Box, or the residential or business street address of next of kin or another contact person for persons who do not have a residential or business address. For a person other than an individual (such as a corporation, partnership, or trust), "address" is a principal place of business, local office, or other physical location. However, while the section 326 rules apply only to new customers opening accounts on or after October 1, 2003, and while the rule exempt funds transfers from the definition of "account," for banks, the Travel Rule applies to all transmittals of funds of $3,000 or more, whether or not the transmittor is a customer for purposes of the section 326 rules.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – Foreign Correspondent Account Recordkeeping and Due Diligence

OBJECTIVE

Assess the bank's compliance with statutory and regulatory requirements for correspondent accounts for foreign shell banks, foreign correspondent account recordkeeping, and due diligence programs to detect and report money laundering and suspicious activity. Refer to the expanded sections of the manual for discussions and procedures regarding other money laundering risks associated with foreign correspondent accounts.

OVERVIEW

One of the central goals of the Patriot Act was to protect access to the U.S. financial system by requiring certain records and due diligence programs for foreign correspondent accounts. In addition, the Patriot Act prohibits accounts with foreign shell banks. Foreign correspondent accounts, as noted in past U.S. Senate investigative reports,[70] are a gateway into the U.S. financial system. This section of the manual covers the regulatory requirements established by sections 312, 313, and 319(b) of the Patriot Act and by the implementing regulations at 31 CFR 103.177, 103.181, and 103.185. Additional discussions and procedures regarding specific money laundering risks for foreign correspondent banking activities, such as pouch activity, cash letters, U.S. dollar drafts, and payable through accounts, are included in the expanded sections.

FOREIGN SHELL BANK PROHIBITION AND FOREIGN CORRESPONDENT ACCOUNT RECORDKEEPING

On October 28, 2002, final regulations (31 CFR 103.177 and 103.185) implementing sections 313 and 319(b) of the Patriot Act became effective. The regulations implemented new provisions of the BSA that relate to foreign correspondent accounts.[71] Under 31 CFR 103.177 a bank is prohibited from establishing, maintaining,

[70] "Correspondent Banking: A Gateway for Money Laundering," See Senate Hearing 107-84. The report appears on p. 273 of volume 1 of the hearing records entitled "Role of U.S. Correspondent Banking in International Money Laundering" held on March 1, 2, and 6, 2001.

[71] For purposes of 31 CFR 103.177 and 103.185, a "correspondent account" is an account established by a bank for a foreign bank to receive deposits from, to make payments or other disbursements on behalf of a foreign bank, or to handle other financial transactions related to the foreign bank. An "account" means any formal banking or business relationship established to provide regular services, dealings, and other financial transactions. It includes a demand deposit, savings deposit, or other transaction or asset account and a credit account or other extension of credit (31 CFR 103.175(d)).

administering, or managing a correspondent account in the United States for, or on behalf of, a foreign shell bank. A foreign shell bank is defined as a foreign bank without a physical presence in any country.[72] An exception, however, permits a bank to maintain a correspondent account for a foreign shell bank that is a regulated affiliate.[73] Section 313 also requires that a bank take reasonable steps to ensure that a correspondent account for a foreign bank is not being used to provide banking services indirectly to foreign shell banks.

Certifications

A bank that maintains a correspondent account in the United States for a foreign bank must maintain records in the United States identifying the owners of each foreign bank.[74] A bank must also record the name and street address of a person who resides in the United States and who is authorized, and has agreed, to be an agent to accept service of legal process.[75] Under 31 CFR 103.185, a bank must produce these records within seven days upon receipt of a written request from a federal law enforcement officer.

The U.S. Treasury, working with the industry and federal banking and law enforcement agencies, developed a "certification process" to assist banks in complying with the recordkeeping provisions. This process includes certification and recertification forms. While banks are not required to use these forms, a bank will be "deemed to be in compliance" with the regulation if it obtains a completed certification form from the foreign financial institution and receives a recertification once every three years.

[72] "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 post office box) in a country in which the foreign financial institution is authorized to conduct banking activities, at which location the foreign financial institution:
  - Employs one or more persons 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 financial institution to conduct banking activities.

[73] A "regulated affiliate" is a shell bank that is affiliated with a depository institution, credit union, or foreign bank that maintains a physical presence in the United States or in another jurisdiction. The regulated affiliate shell bank must also be subject to supervision by the banking authority that regulates the affiliated entity.

[74] To minimize the recordkeeping burdens, ownership information is not required for foreign financial institutions that file a form FR Y-7 ("Annual Report of Foreign Banking Organizations") with the Federal Reserve or for those foreign financial institutions that are publicly traded. "Publicly traded" refers to shares that are traded on an exchange or an organized over-the-counter market that is regulated by a foreign securities authority as defined in section 3(a)(50) of the Securities Exchange Act of 1934.

[75] "Service of legal process" means that the agent is willing to accept legal documents, such as subpoenas, on behalf of the foreign bank.

Account Closure

The regulation also contains specific provisions as to when banks must obtain the required information or close correspondent accounts. Banks must obtain certifications (or recertifications) or otherwise obtain the required information within 30 calendar days after the date an account is established and at least once every three years thereafter. If the bank is unable to obtain the required information, it must close all correspondent accounts with the foreign bank within a commercially reasonable time.

Verification

A bank should review certifications for reasonableness and accuracy. If a bank at any time knows, suspects, or has reason to suspect that any information contained in a certification (or recertification), or that any other information it relied on is no longer correct, the bank must request that the foreign bank verify or correct such information, or take other appropriate measures to ascertain its accuracy. Therefore, banks should review certifications for potential problems that may warrant further review, such as use of post office boxes or forwarding addresses. If the bank has not obtained the necessary or corrected information within 90 days, it must close the account within a commercially reasonable time. During this time, the bank may not permit the foreign bank to establish any new financial positions or execute any transactions through the account, other than those transactions necessary to close the account. Also, a bank may not establish any other correspondent account for the foreign bank until it obtains the required information.

A bank must also retain the original of any document provided by a foreign bank, and retain the original or a copy of any document otherwise relied on for the purposes of the regulation, for at least five years after the date that the bank no longer maintains any correspondent account for the foreign bank.

Subpoenas

Under section 319(b) of the Patriot Act, the Secretary of the Treasury or the U.S. Attorney General may issue a subpoena or summons to any foreign bank that maintains a correspondent account in the United States to obtain records relating to that account, including records maintained abroad, or to obtain records relating to the deposit of funds into the foreign bank. If the foreign bank fails to comply with the subpoena or fails to initiate proceedings to contest that subpoena, the Secretary of the Treasury or the U.S. Attorney General (after consultations with each other) may, by written notice, direct a bank to terminate its relationship with a foreign correspondent bank. If a bank fails to terminate the correspondent relationship within ten days of receipt of notice, it could be subject to a civil money penalty of up to $10,000 per day until the correspondent relationship is terminated.

Requests for AML Records by Federal Regulator

Also, upon request by its federal regulator, a bank must provide or make available records related to AML compliance of the bank or one of its customers, within 120 hours from the time of the request.

SPECIAL DUE DILIGENCE PROGRAM FOR FOREIGN CORRESPONDENT ACCOUNTS

Section 312 of the Patriot Act added new subsection (i) to 31 USC 5318 of the BSA. This section requires each U.S. bank that establishes, maintains, administers, or manages a correspondent account in the United States for a non-U.S. person to take certain AML measures for such accounts. In particular, banks must establish appropriate, specific, and, where necessary, enhanced due diligence policies, procedures, and processes that are reasonably designed to enable the bank to detect and report instances of money laundering through those accounts. This requirement applies to a correspondent relationship with any foreign financial institution, even if it is not a traditional banking institution. In addition to this general requirement, which applies to all correspondent accounts for non-U.S. persons, section 312 of the Patriot Act specifies additional standards for correspondent accounts maintained for certain foreign banks. For a correspondent account maintained for a foreign bank operating under an offshore license or a license granted by a jurisdiction designated as being of concern for money laundering, a bank must take reasonable steps to identify the owners of the foreign financial institution, conduct enhanced scrutiny of the correspondent account to guard against money laundering, and ascertain whether the foreign bank provides correspondent accounts to other foreign banks and, if so, conduct appropriate related due diligence.

Interim Final Rule

On July 23, 2002, the U.S. Treasury stated through the *Federal Register* that a final rule implementing section 312 could not reasonably be completed by the statutory effective date of July 23, 2002.[76] Accordingly, the U.S. Treasury published an interim final rule that deferred the application of the due diligence provisions for correspondent accounts of section 5318(i) to financial institutions other than banks. Thus, banks must comply with section 5318(i) pending Treasury's issuance of a final rule. The interim final rule for banks is promulgated at 31 CFR 103.181.[77] The preamble to the *Federal Register* notice that accompanied the interim final rule provided guidance to those financial institutions,

[76] See 67 *Federal Register* 48348 at www.fincen.gov.

[77] For the interim final regulation at 31 CFR 103.181, a correspondent account is an account established to receive deposits from, make payments on behalf of a foreign financial institution, or handle other financial transactions related to such institution. An account means any formal banking or business relationship established to provide regular services, dealings, and other financial transactions, and includes a demand deposit, savings deposit, or other transaction or asset account and a credit account or other extension of credit (31 USC 5318A(e)).

including banks, for which the application of section 5318(i) has not been deferred. Subsection 5318(i) applies to all accounts, regardless of when they were opened.

As a practical matter, banks will be unable to craft and implement final comprehensive due diligence policies and procedures pursuant to the dictates of 31 USC 5318(i) until the U.S. Treasury issues a final rule. In the interim, examiners will focus on a bank's policies, procedures, and processes to comply with the two basic provisions of 31 USC 5318(i) regarding correspondent banking:

- General due diligence for correspondent accounts maintained for all foreign financial institutions (31 USC 5318(i)(1)).
- Enhanced due diligence for correspondent accounts maintained for certain foreign banks (31 USC 5318(i)(2)).

FinCEN and the federal banking agencies anticipate that revised examination procedures will be developed on an interagency basis upon U.S. Treasury's issuance of a final rule.

General Due Diligence

Subsection 5318(i)(1) requires banks to establish due diligence policies, procedures, and controls reasonably designed to detect and report money laundering through correspondent accounts established, maintained, administered, or managed in the United States for a foreign financial institution. In the interim period, a due diligence program under subsection 5318(i)(1) will be reasonable if it establishes policies, procedures, and processes to assess the risks posed by foreign correspondent accounts, and focuses compliance efforts on the correspondent accounts that pose a high risk of money laundering. The preamble to the *Federal Register* notice that accompanied the interim final rule stated that a bank should give priority to conducting due diligence on:

- High-risk foreign financial institutions for which it maintains correspondent deposit accounts or equivalent accounts.
- Correspondent accounts used to provide services to third parties.
- High-risk correspondent accounts maintained for foreign financial institutions other than foreign banks, such as money transmitters.

In the interim, a reasonable due diligence policy should comport with existing sound practices and standards for banks that maintain correspondent accounts for foreign financial institutions. The policy should provide evidence of the bank's good faith efforts to incorporate due diligence procedures for those correspondent accounts it maintains for foreign financial institutions that pose an increased risk of money laundering.

Examples of existing sound practices and standards include the following:

- The New York Clearing House Association, L.L.C., "The New York Clearing House Issues Anti-Money Laundering Guidelines for Correspondent Banking," (March 2002) at www.nych.org.
- Basel Committee on Banking Supervision, "Customer Due Diligence for Banks," (October 2001) at www.bis.org.

A due diligence program that does not adopt all of the sound practices and standards described in industry and other available guidance could be considered reasonable if the bank has a justifiable reason for not adopting a particular sound practice or standard, based on the particular type of accounts held by the bank.

Risk Assessment of Foreign Financial Institutions

A bank's general due diligence program should include policies, procedures, and processes to assess the risks posed by the bank's foreign financial institution customers. A bank's resources are most appropriately directed at those accounts that pose a more significant money laundering risk. The following factors may be used to help identify potential risk characteristics of a foreign correspondent customer. Nevertheless, management should weigh and evaluate each risk factor to arrive at a risk determination for each customer and then prioritize oversight resources. Relevant risk factors include the following:

- The foreign financial institution's jurisdiction of organization, chartering, and licensing.
- Products and services offered by the foreign financial institution.
- Markets (including customer base) and locations served by the foreign financial institution.
- Purpose of the account (e.g., a proprietary operating account or a customer-directed account).
- Anticipated activity (e.g., dollar amount, number, and types of transactions) of the account.
- The nature and duration of the bank's relationship with the foreign financial institution (and, if relevant, with any affiliate of the foreign financial institution).
- Any information known or reasonably available to the bank about the foreign financial institution's AML record, including public information in standard industry guides, periodicals, and major publications.

Enhanced Due Diligence for Certain Foreign Banks

Subsection 5318(i)(2) requires banks to establish enhanced due diligence policies and procedures when opening or maintaining a correspondent account in the United States requested or maintained by, or on behalf of, certain foreign banks operating under:

- An offshore banking license.[78]
- A banking license issued by a foreign country that has been designated as non-cooperative with international AML principles or procedures by an intergovernmental group or organization of which the United States is a member, and with whose designation the United States representative to the group or organization concurs.
- A banking license issued by a foreign country that has been designated by the Secretary of the Treasury as warranting special measures due to money laundering concerns.

Under subsections 5318(i)(2)(B)(i) through (iii), a bank must establish policies, procedures, and controls to ensure that for each such foreign bank subject to enhanced due diligence, the bank takes reasonable steps to:

- Ascertain, for any such foreign bank whose shares are not publicly traded, the identity of each of the owners of the foreign bank, and the nature and extent of the ownership interest of each such owner.[79]
- Conduct enhanced scrutiny of any accounts held by such banks to guard against money laundering and report any suspicious transactions in accordance with SAR regulations.
- Ascertain whether such foreign bank provides correspondent accounts to other foreign banks and, if so, to ascertain the identity of those foreign banks and conduct due diligence as appropriate under the requirements of subsection 5318(i)(1) (i.e., the bank's general due diligence program). Considering risk factors such as the location and size of the foreign correspondent bank and number of its foreign financial institution customers, the bank should determine the extent to which enhanced due diligence of a foreign correspondent bank's foreign financial institution customers is necessary.

Banks should focus enhanced due diligence measures on those correspondent accounts that are maintained by a foreign bank deemed by 31 USC 5318(i)(2)(A) to pose a particularly high risk of money laundering on the basis of the bank's overall assessment of the risk posed by the foreign bank. In addition, banks should apply any or all of the steps listed above, as appropriate, to a foreign financial institution identified by the bank's general due diligence program as representing an increased risk of money laundering.

[78] The Patriot Act defines an offshore banking license as a license to conduct banking activities that, as a condition of the license, prohibits the licensed entity from conducting banking activities with the citizens of, or with the local currency of, the country that issued the license. Refer to 31 USC 5318(i)(4)(A).

[79] The preamble to the *Federal Register* notice that accompanied the interim final rule (67 *Federal Register* 48348) stated that for purposes of subsection 5318(i)(2)(B)(i), an owner is deemed to be any person who directly or indirectly owns, controls, or has voting power over 5 percent or more of any class of securities of a foreign bank, the shares of which are not publicly traded. "Publicly traded" means shares that are traded on an exchange or an organized over-the-counter market that is regulated by a foreign securities authority, as defined in section 3(a)(50) of the Securities Exchange Act of 1934 (15 USC 78c(a)(50)).

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – Private Banking Due Diligence Program (Non-U.S. Persons)

OBJECTIVE

Assess the bank's compliance with the statutory and regulatory requirements to implement policies, procedures, and controls to detect and report money laundering and suspicious activity through private banking accounts established, administered, or maintained for non-U.S. persons. Refer to the expanded sections of the manual for discussions and procedures regarding other money laundering risks associated with private banking.

OVERVIEW

Private banking can be broadly defined as personalized financial services to wealthy clients. The Patriot Act amended the BSA to define a "private banking account" as an account, or combination of accounts, that meets the following criteria:

- Requires minimum aggregate deposits of funds or other assets of not less than $1 million.
- Is established on behalf of one or more individuals who have a direct or beneficial ownership interest in the account.
- Is assigned to, or 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 and beneficial owner of the account.[80]

Section 312 of the Patriot Act added new subsection (i) to 31 USC 5318 of the BSA. This section requires each U.S. financial institution that establishes, maintains, administers, or manages a private banking account (based on the above definition) in the United States for a non-U.S. person to take certain anti-money laundering measures with respect to such accounts. In particular, banks must establish appropriate, specific, and, where necessary, enhanced due diligence policies, procedures, and controls that are reasonably designed to enable the bank to detect and report instances of money laundering through private banking accounts established, administered, or maintained in the United States for non-U.S. persons. In addition to this general requirement, section 312 described minimum standards for private banking accounts requested or maintained by, or on behalf of, non-U.S. persons, to ensure that, at a minimum, the bank takes reasonable steps to:

[80] See 31 USC 5318(i)(4)(B). This specific definition of "private banking account" applies only to the special due diligence requirements of 31 USC 5318(i).

- Ascertain the identity of the nominal and beneficial owners of, and the source of funds deposited into, private banking accounts, as needed to guard against money laundering and report any suspicious transactions.
- Conduct enhanced scrutiny of any private banking account that is requested or maintained by, or on behalf of, a senior foreign political figure, or any immediate family member or close associate of a senior foreign political figure (also known as politically exposed persons (PEPs)).[81] This enhanced scrutiny is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.

The overview and procedures set forth in this section are intended to evaluate the bank's due diligence program concerning private banking accounts offered to non-U.S. persons. Additional procedures for specific risk areas of private banking are included in the expanded examination procedures section "Private Banking" on page 253.

Interim Final Rule

On July 23, 2002, the U.S. Treasury stated through the *Federal Register* that a final rule implementing section 312 could not reasonably be completed by the statutory effective date of July 23, 2002.[82] Accordingly, the U.S. Treasury published an interim final rule that deferred the application of the private banking provisions of section 5318(i) to financial institutions other than banks, securities brokers and dealers, futures commission merchants, and introducing brokers. Thus, banks must comply with section 5318(i) pending the U.S. Treasury's issuance of a final rule. The interim final rule for banks is promulgated at 31 CFR 103.181.[83] The preamble to the *Federal Register* notice that accompanied the interim final rule provided guidance to those financial institutions for which the application of section 5318(i) has not been deferred, which includes banks. 31 USC 5318(i) applies to all accounts, regardless of when they were opened.

As a practical matter, banks will be unable to craft and implement final comprehensive due diligence policies, procedures, and controls pursuant to the dictates of section 5318(i) until the U.S. Treasury issues a final rule. In the interim, examiners will focus on a bank's policies, procedures, and processes to comply with the provisions of 31 USC 5318(i) regarding private banking. FinCEN and the federal banking agencies anticipate that revised examination procedures will be developed on an interagency basis upon U.S. Treasury's issuance of a final rule.

[81] See the expanded procedures section "Politically Exposed Persons" page 259.

[82] See 67 *Federal Register* 48348 at www.fincen.gov.

[83] For the purposes of the interim final rule, the term "bank" includes: banks, thrifts, savings associations, credit unions, foreign banking organizations (FBOs), and Edge Act and agreement corporations.

DUE DILIGENCE

A private banking due diligence program must be reasonably designed to detect and report money laundering and the existence of the proceeds of foreign corruption. In the interim, a reasonable due diligence policy is one that (i) comports with existing sound practices and standards for banks that maintain private banking accounts for non-U.S. persons, (ii) evidences good faith efforts to incorporate the minimum due diligence standards described previously, and (iii) focuses on those private banking accounts that present a high risk of money laundering. Examples of existing sound practices and standards include the following:

- The Board of Governors of the Federal Reserve System, "Private Banking Activities" (SR letter 97-19 (SUP), June 30, 1997) at www.federalreserve.gov.
- U.S. Treasury, the federal bank regulators, and the U.S. Department of the State, "Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Corruption," (January 2001) at www.treas.gov/press/releases/docs/guidance.htm.
- The Wolfsberg Group, "Wolfsberg AML Principles on Private Banking" (1st revision May 2002) at www.wolfsberg-principles.com.
- Bank for International Settlements (BIS) Basel Committee on Banking Supervision, "Customer Due Diligence for Banks" (October 2001) at www.treas.gov/press/releases/docs/guidance.htm.

A due diligence program that does not adopt all of the sound practices and standards described in the government and industry guidance listed previously could be considered reasonable. An institution should have a justifiable reason for not adopting a particular sound practice or standard, based on the particular type of accounts held by the bank.

Risk Assessment of Private Banking Accounts for Non-U.S. Persons

Banks should develop policies, procedures, and processes to assess the risks posed by private banking accounts for non-U.S. persons and direct their resources most appropriately at those accounts that pose a more significant money laundering risk. The following factors may be used to help identify potential risk characteristics of a private banking customer. Nevertheless, management should weigh and evaluate each risk factor to arrive at a risk determination for each customer. Relevant risk factors may include the following:

- Nature of customer's business (i.e., source of wealth). The nature of the private banking customer's business, the source of the customer's wealth, and the extent to which the customer's business history presents an increased risk for money laundering. This factor should be considered for private banking accounts opened for senior foreign political figures, to the extent needed to reasonably detect and report transactions that may involve the proceeds of foreign corruption.

- Purpose of an account and anticipated activity. The size, purpose, type of accounts involved in the relationship, and anticipated activity of the account (e.g., dollar amount, number, and types of transactions).
- Customer history. The nature and duration of the bank's relationship with the private banking customer.
- Jurisdiction. The private banking customer's location of domicile and business. This review would include considering the extent to which the relevant jurisdiction is internationally recognized as presenting a greater risk for money laundering or, conversely, if it is considered to have more robust AML standards.
- Available information. Any information known or reasonably available to the institution about the private banking customer. The scope and depth of such a review will depend on the nature of the information uncovered.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – Special Measures

OBJECTIVE

Assess the bank's compliance with statutory and regulatory requirements for special measures issued under section 311 of the Patriot Act.

OVERVIEW

Section 311 of the Patriot Act added 31 USC 5318A to the BSA, which authorizes the Secretary of the Treasury to require domestic financial institutions and domestic financial agencies to take certain special measures against foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts of primary money laundering concern. Section 311 provides the Secretary of the Treasury with a range of options that can be adapted to target specific money laundering and terrorist financing concerns. Section 311 is implemented through various orders and regulations that are incorporated into 31 CFR Part 103.[84] As set forth in section 311, certain special measures may be imposed by an order without prior public notice and comment, but such orders must be of limited duration and must be issued together with a Notice of Proposed Rulemaking.

Section 311 establishes a process for the Secretary of the Treasury to follow, and identifies federal agencies to consult before the Secretary of the Treasury may conclude that a jurisdiction, financial institution, class of transactions, or type of account is of primary money laundering concern. The statute also provides similar procedures, including factors and consultation requirements, for selecting the specific special measures to be imposed against a jurisdiction, financial institution, class of transactions, or type of account that is of primary money laundering concern.

It is important to note that, while a jurisdiction, financial institution, class of transactions, or type of account may be designated of primary money laundering concern in an order issued together with a Notice of Proposed Rulemaking, special measures of unlimited duration can only be imposed by a final rule issued after notice and an opportunity for comment.

[84] Notices of proposed rulemaking and final rules accompanying the determination "of primary money laundering concern," and imposition of a special measure (or measures) pursuant to section 311 of the Patriot Act are available on the FinCEN web site: www.fincen.gov.

TYPES OF SPECIAL MEASURES

The following five special measures can be imposed, either individually, jointly, or in any combination:

Recordkeeping and Reporting of Certain Financial Transactions

Under the first special measure, banks may be required to maintain or to file reports concerning the aggregate amount of transactions or the specifics of each transaction with respect to a jurisdiction, financial institution, class of transactions, or type of account that is of primary money laundering concern. The statute contains minimum information requirements for these records and reports and permits the Secretary of the Treasury to impose additional information requirements.

Information Relating to Beneficial Ownership

Under the second special measure, banks may be required to take reasonable and practicable steps, as determined by the Secretary of the Treasury, to obtain and retain information concerning the beneficial ownership of any account opened or maintained in the United States by a foreign person (other than a foreign entity whose shares are subject to public reporting requirements or are listed and traded on a regulated exchange or trading market), or a representative of such foreign person, that involves a jurisdiction, financial institution, class of transactions, or type of account that is of primary money laundering concern.

Information Relating to Certain Payable Through Accounts

Under the third special measure, banks that open or maintain a payable through account involving a jurisdiction, financial institution, class of transactions, or type of account that is of primary money laundering concern, may be required to: (i) identify each customer (and representative) who is permitted to use the account or whose transactions are routed through the account; and (ii) obtain information about each such customer (and representative) that is substantially comparable to that which a United States depository institution obtains in the ordinary course of business with respect to its customers residing in the United States.[85]

Information Relating to Certain Correspondent Accounts

Under the fourth special measure, banks that open or maintain a correspondent account in the United States involving a jurisdiction, financial institution, class of transactions, or type of account that is of primary money laundering concern may be required to: (i) identify each customer (and representative) who is permitted to use the account or whose transactions are routed through the account; and (ii) obtain information about each such customer (and representative) that is substantially comparable to that which a United

[85] Refer to expanded overview section "Payable Through Accounts" on page 102 for additional guidance.

States depository institution obtains in the ordinary course of business with respect to its customers residing in the United States.[86]

Prohibitions or Conditions on Opening or Maintaining Certain Correspondent or Payable Through Accounts

Under the fifth, and strongest, special measure, banks may be prohibited from opening or maintaining any correspondent account or payable through account for, or on behalf of, a foreign financial institution if the account involves a jurisdiction, financial institution, class of transactions, or type of account that is of primary money laundering concern. The imposition of this measure can prohibit U.S. banks from establishing, maintaining, administering or managing a correspondent or payable through account for, or on behalf of, any financial institution from a specific foreign jurisdiction. This measure may also be applied to specific foreign financial institutions and their subsidiaries.

The regulations that implement these prohibitions may require banks to review their account records to determine that they maintain no accounts directly for, or on behalf of, such entities. In addition to the direct prohibition, banks may also be:

- Prohibited from knowingly providing indirect access to the specific entities through its other banking relationships.
- Required to notify correspondent accountholders that they must not provide the specific entity with access to the account maintained at the U.S. bank.
- Required to take reasonable steps to identify any indirect use of its accounts by the specific entity.

SPECIAL MEASURES GUIDANCE

Orders and regulations implementing specific special measures taken under section 311 of the Patriot Act are not static; they can be issued or rescinded over time as the Secretary of the Treasury determines that a subject jurisdiction, institution, class of transactions, or type of account is no longer of primary money laundering concern. In addition, special measures imposed against one jurisdiction, institution, class of transactions, or type of account may vary from those imposed in other situations. Examiners should also note that compliance with special measures is not necessarily absolute; an order or rule imposing a special measure may establish a standard of due diligence that banks must apply to comply with the particular special measure.

Accordingly, this manual does not detail specific final special measures, since any such listing could quickly become dated. Examiners reviewing compliance with this section should visit FinCEN's web site www.fincen.gov for current information on final special measures. Examiners should only examine for those special measures that are final, and should not review banks against those that are proposed.

[86] Refer to core overview section "Foreign Correspondent Account Recordkeeping and Due Diligence," on page 68 and expanded overview section "Correspondent Accounts (Foreign)" on page 98 for additional guidance.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – Foreign Bank and Financial Accounts Reporting

OBJECTIVE

Assess the bank's compliance with statutory and regulatory requirements for the reporting of foreign bank and financial accounts.

OVERVIEW

Each person[87] (including a bank) subject to U.S. jurisdiction with a financial interest in, or signature authority over, a bank, a securities, or any other financial account in a foreign country must file a Report of Foreign Bank and Financial Accounts (FBAR) with the Internal Revenue Service (IRS) (TD F 90-22.1) if the aggregate value of these financial accounts exceeds $10,000 at any time during the calendar year. A bank must file this form on its own accounts that meet this definition; the bank may be obligated to file these forms for customer accounts in which the bank has a financial interest or over which it has signature authority.

A FBAR must be filed with the commissioner of the IRS on or before June 30 of each calendar year for foreign financial accounts exceeding $10,000 maintained at any time during the previous calendar year.

[87] As defined in 31 CFR 103.11(z), the term "person" means an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, 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 cognizable as legal personalities.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – International Transportation of Currency or Monetary Instruments Reporting

OBJECTIVE

Assess the bank's compliance with statutory and regulatory requirements for the reporting of international shipments of currency or monetary instruments.

OVERVIEW

Each person[88] (including a bank) who physically transports, mails, or ships currency or monetary instruments in excess of $10,000 at one time out of or into the United States (and each person who causes such transportation, mailing, or shipment), must file a Report of International Transportation of Currency or Monetary Instruments (CMIR) (FinCEN Form 105). A CMIR must be filed with the appropriate Bureau of Customs and Border Protection officer or with the commissioner of Customs at the time of entry into or departure from the United States. When a person receives currency or monetary instruments in an amount exceeding $10,000 at one time that have been shipped from any place outside the United States, a CMIR must be filed with the appropriate Bureau of Customs and Border Protection officer or with the commissioner of Customs within 15 days of receipt of the instruments (unless a report has already been filed). The report is to be completed by or on behalf of the person requesting transfer of the currency or monetary instruments. However, banks are not required to report these items if they are mailed or shipped through the postal service or by common carrier.[89] In addition, a commercial bank or trust company organized under the laws of any state or of the United States is not required to report overland shipments of currency or monetary instruments if they are shipped to or received from an established customer maintaining a deposit relationship with the bank and if the bank reasonably concludes the amounts do not exceed what is commensurate with the customary conduct of the business, industry, or profession of the customer concerned.

Management should implement applicable policies, procedures, and processes for CMIR filing. Management should review the international transportation of currency and monetary instruments and determine whether a customer's activity is usual and customary for the type of business. If not, a Suspicious Activity Report should be considered.

[88] Id.

[89] In contrast, a bank is required to file a CMIR to report shipments of currency or monetary instruments to foreign offices when those shipments are performed directly by bank personnel, such as currency shipments handled by bank employees using bank-owned vehicles.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – Office of Foreign Assets Control

OBJECTIVE

Assess the bank's risk-based Office of Foreign Assets Control (OFAC) program to evaluate whether it is appropriate for the bank's OFAC risk, taking into consideration its products, services, customers, transactions, and geographic locations.

BACKGROUND

OFAC is an office of the U.S. Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against entities such as targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction.

OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and to freeze assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, therefore they are multilateral in scope, and involve close cooperation with allied governments. Other sanctions are specific to the interests of the United States. OFAC has been delegated responsibility by the Secretary of the Treasury for developing, promulgating, and administering U.S. sanctions programs.[90]

All U.S. persons,[91] including U.S. banks, bank holding companies, and non-bank subsidiaries must comply with OFAC's regulations.[92] The federal banking agencies

[90] Trading With the Enemy Act (TWEA), 50 USC App 1-44; International Emergency Economic Powers Act (IEEPA), 50 USC 1701 et seq.; Antiterrorism and Effective Death Penalty (AEDPA), 8 USC 1189, 18 USC 2339B; United Nations Participation Act (UNPA), 22 USC 287c; Cuban Democracy Act (CDA), 22 USC 6001-10; The Cuban Liberty and Democratic Solidarity Act (Libertad Act), 22 USC 6021-91; The Clean Diamonds Trade Act, Pub. L. No. 108-19; Foreign Narcotics Kingpin Designation Act (Kingpin Act), 21 USC 1901-1908, 8 USC 1182; Burmese Freedom and Democracy Act of 2003, Pub. L. No. 108-61, 117 Stat. 864 (2003); The Foreign Operations, Export Financing and Related Programs Appropriations Act, Sec 570 of Pub. L. No. 104-208, 110 Stat. 3009-116 (1997); The Iraqi Sanctions Act, Pub. L. No. 101-513, 104 Stat. 2047-55 (1990); The International Security and Development Cooperation Act, 22 USC 2349 aa8-9; The Trade Sanctions Reform and Export Enhancement Act of 2000, Title IX, Pub. L. No. 106-387 (October 28, 2000).

[91] All U.S. persons must comply with OFAC regulations, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, all U.S. incorporated entities and their foreign branches. In the case of certain programs, such as those regarding Cuba and North Korea, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S. origin goods to comply.

[92] Additional information is provided in "Foreign Assets Control Regulations for the Financial Community," which is available on OFAC's web site www.treas.gov/ofac/.

evaluate OFAC compliance systems to ensure that all banks subject to their supervision comply with the sanctions.[93] Unlike the BSA, the laws and OFAC-issued regulations apply not only to U.S. banks, their domestic branches, agencies, and international banking facilities, but also to their foreign branches, and often overseas offices and subsidiaries. In general, the regulations require the following:

- Block accounts and other property of specified countries, entities, and individuals.
- Prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals.

Blocked Transactions

U.S. law requires that assets and accounts be blocked when such property is located in the United States, is held by U.S. individuals or entities, or comes into the possession or control of U.S. individuals or entities. For example, if a funds transfer comes from offshore and is being routed through a U.S. bank to an offshore bank, and there is an OFAC designated party on the transaction, it must be blocked. The definition of assets and property is broad and is specifically defined within each sanction program. Assets and property includes anything of direct, indirect, present, future, or contingent value (including all types of bank transactions). Banks must block transactions that:

- Are by or on behalf of a blocked individual or entity;
- Are to or through a blocked entity; or
- Are in connection with a transaction in which a blocked individual or entity has an interest.

For example, if a U.S. bank receives instructions to make a funds transfer payment that falls into one of these categories, it must execute the payment order and place the funds into a blocked account.[94] A payment order cannot be canceled or amended after it is received by a U.S. bank in the absence of an authorization from OFAC.

Prohibited Transactions

In some cases, an underlying transaction may be prohibited, but there is no blockable interest in the transaction (i.e., the transaction should not be accepted, but there is no OFAC requirement to block the assets). In these cases, the transaction is simply rejected, i.e., not processed. For example, the Sudanese Sanctions Regulations prohibit transactions in support of commercial activities in Sudan. Therefore, a U.S. bank would have to reject a funds transfer between two companies, which are not Specially Designated Nationals or Blocked Persons (SDNs), involving an export to a company in Sudan that also is not an SDN. Because Sudanese Sanctions would only require blocking

[93] 31 CFR chapter V.

[94] A blocked account is a segregated interest-bearing account (at a commercially reasonable rate), which holds the customer's property until the target is delisted, the sanctions program is rescinded, or the customer obtains an OFAC license authorizing the release of the property.

transactions with the Government of Sudan or SDNs, there would be no blockable interest in the funds between the two companies. However, because the transactions would constitute support of Sudanese commercial activity, which is prohibited, the U.S. bank can not process the transaction and would simply reject the transaction.

It is important to note that the OFAC regime specifying prohibitions against certain countries, entities, and individuals is separate and distinct from the provision within the BSA's Customer Identification Program (CIP) regulation (31 CFR 103.121) that requires banks to compare new accounts against government lists of known or suspected terrorists or terrorist organizations within a reasonable period of time after the account is opened. OFAC lists have not been designated government lists for purposes of the CIP rule. Refer to core overview section "Customer Identification Program" on page 30 for further guidance. However, OFAC's requirements stem from other statutes not limited to terrorism, and OFAC sanctions apply to transactions, in addition to account relationships.

OFAC Licenses

OFAC has the authority, through a licensing process, to permit certain transactions that would otherwise be prohibited under its regulations. OFAC can issue a license to engage in an otherwise prohibited transaction when it determines that the transaction does not undermine the U.S. policy objectives of the particular sanctions program, or is otherwise justified by U.S. national security or foreign policy objectives. OFAC can also promulgate general licenses, which authorize categories of transactions, such as allowing reasonable service charges on blocked accounts, without the need for case-by-case authorization from OFAC. These licenses can be found in the regulations for each sanctions program (31 CFR, Chapter V (Regulations)) and may be accessed from OFAC's web site. Before processing transactions that may be covered under a general license, banks should verify that such transactions meet the relevant criteria of the general license.[95]

Specific licenses are issued on a case-by-case basis and require an application directed to: Licensing Division, Office of Foreign Assets Control, 1500 Pennsylvania Avenue, NW, Washington, D.C. 20220. A specific license is a written document issued by OFAC authorizing a particular transaction or set of transactions. To receive a specific license, the person or entity who would like to undertake the transaction must submit an application to OFAC. If the transaction conforms with U.S. foreign policy under a particular program, the license will be issued. If a bank's customer claims to have a specific license, the bank should verify that the transaction conforms to the terms of the license and obtain and retain a copy of the authorizing license.

[95] License information is available on OFAC's web site www.treas.gov/ofac, or by contacting OFAC's Licensing area at 202-622-2480.

OFAC Reporting

Banks must report all blockings to OFAC within ten days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30).[96] Once assets or funds are blocked, they should be placed in a blocked account. Prohibited transactions that are rejected must also be reported to OFAC within ten days of the occurrence

Banks must keep a full and accurate record of each blocked or rejected transaction for at least five years after the date of the transaction. For blocked property, records must be maintained for the period the property is blocked and for five years after the date the property is unblocked.

Additional information concerning OFAC regulations, such as Sanctions Program and Country Summaries brochures; the SDN list, including both entities and individuals; recent OFAC actions; and Frequently Asked Questions, can be found on OFAC's web site.[97]

OFAC PROGRAM

While not required by specific regulation, but as a matter of sound banking practice and in order to ensure compliance, banks should establish and maintain an effective, written OFAC program commensurate with their OFAC risk profile (based on products, services, customers, and geographic locations). The program should identify high-risk areas, provide for appropriate internal controls for screening and reporting, establish independent testing for compliance, designate a bank employee or employees as responsible for OFAC compliance, and create training programs for appropriate personnel in all relevant areas of the bank. A bank's OFAC program should be commensurate with its respective OFAC risk profile.

OFAC Risk Assessment

A fundamental element of a sound OFAC program is the bank's assessment of its specific product lines, customer base, nature of transactions and identification of the high-risk areas for OFAC transactions. The initial identification of high-risk customers for purposes of OFAC may be performed as part of the bank's CIP and CDD procedures. As OFAC sanctions can reach into virtually all areas of its operations, banks should consider all types of transactions, products and services when conducting their risk assessment and establishing appropriate policies, procedures and processes. An effective risk assessment should be a composite of multiple factors (as described in more detail below), and depending upon the circumstances, certain factors may be weighed more heavily than others.

[96] The annual report is to be filed on form TD F 90-22.50.

[97] This information is available on OFAC's web site www.treas.gov/ofac, or by contacting OFAC's Hotline at 800-540-6322.

Another consideration for the risk assessment is account and transaction parties. New accounts should be compared with OFAC lists prior to being opened or shortly thereafter. However, the extent to which the bank includes account parties other than accountholders (e.g., beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories, and powers of attorney) in the initial OFAC review during the account opening process, and during subsequent database reviews of existing accounts, will depend on the bank's risk profile and available technology.

Based on the bank's OFAC risk profile for each area and available technology, the bank should establish policies, procedures, and processes for reviewing transactions and transaction parties (e.g., issuing bank, payee, endorser or jurisdiction). Currently, OFAC provides guidance on transactions parties on checks. The guidance states if a bank knows or has reason to know that a transaction party on a check is an OFAC target, the bank's processing of the transaction would expose the bank to liability, especially personally handled transactions in a high-risk area. For example, if a bank knows or has a reason to know that a check transaction involves an OFAC-prohibited party or country, OFAC would expect timely identification and appropriate action.

In evaluating the level of risk, a bank should exercise judgment and take into account all indicators of risk. Although not an exhaustive list, examples of products, services, customers, and geographic locations that may carry a higher level of OFAC risk include:

- International funds transfers.
- Nonresident alien accounts.
- Foreign customer accounts.
- Cross-border automated clearing house (ACH).
- Commercial letters of credit.
- Transactional electronic banking.
- Foreign correspondent bank accounts.
- Payable through accounts.
- International private banking.
- Overseas branches or subsidiaries.

Appendix M ("Quantity of Risk – OFAC Procedures") provides guidance to examiners on assessing OFAC risks facing a bank. The risk assessment can be used to assist the examiner in determining the scope of the OFAC examination. Additional information on compliance risk is posted by OFAC on its web site under "Frequently Asked Questions" (http://www.treas.gov/offices/enforcement/ofac/faq/#finance).

Once the bank has identified its areas with high OFAC risk, it should develop appropriate policies, procedures, and processes to address the associated risks. Banks may tailor these policies, procedures, and processes to the specific nature of a business line or product. Furthermore, banks are encouraged to periodically reassess their OFAC risks.

Internal Controls

An effective OFAC program should include internal controls for identifying suspect accounts and transactions and reporting to OFAC. Internal controls should include the following elements:

Flag and Review Suspect Transactions

The bank's policies, procedures, and processes should address how the bank will flag and review transactions and accounts for possible OFAC violations, whether conducted manually, through interdiction software, or a combination of both. For screening purposes, the bank should clearly define its criteria for comparing names provided on the OFAC list with the names in the bank's files or on transactions and for flagging transactions or accounts involving sanctioned countries. The bank's policies, procedures, and processes should also address how it will determine whether an initial OFAC hit is a valid match or a false hit.[98] A high volume of false hits may indicate a need to review the bank's interdiction program.

The screening criteria used by banks to identify name variations and misspellings should be based on the level of OFAC risk associated with the particular product or type of transaction. For example, in a high-risk area with a high-volume of transactions, the bank's interdiction software should be able to flag close name derivations for review. The SDN list attempts to provide name derivations; however, the list may not include all derivations. More sophisticated interdiction software may be able to catch variations of an SDN's name not included on the SDN list. Low-risk banks or areas and those with low volumes of transactions may decide to manually filter for OFAC compliance. Decisions to use interdiction software and the degree of sensitivity of that software should be based on a bank's assessment of its risk and the volume of its transactions. In determining the frequency of OFAC checks and the filtering criteria used (e.g., name derivations), banks should consider the likelihood of incurring a violation and available technology. In addition, banks should periodically reassess their OFAC filtering system. For example, if a bank identifies a name derivation of an OFAC target, then OFAC suggests that the bank add the name to its filtering process.

New accounts should be compared with the OFAC lists prior to being opened or shortly thereafter (e.g., during nightly processing). Banks that perform OFAC checks after account opening should have procedures in place to prevent transactions, other than initial deposits, from occurring until the OFAC check is completed. Prohibited transactions conducted prior to completing an OFAC check may be subject to possible penalty action. In addition, banks should have policies, procedures and processes in place to check existing customers when there are additions or changes to the OFAC list. The frequency of the review should be based on the bank's OFAC risk. For example, banks with a low OFAC risk level may periodically (e.g., monthly or quarterly) compare

[98] Due diligence steps for determining a valid match are provided in "Using OFAC's Hotline" on OFAC's web site www.treas.gov/ofac.

the customer base against the OFAC list. Transactions such as funds transfers, letters of credit, and non-customer transactions should be checked against OFAC lists prior to being executed. When developing OFAC policies, procedures, and processes, the bank should keep in mind that OFAC considers the continued operation of an account or the processing of transactions post-designation, along with the adequacy of their OFAC compliance program, to be a factor in determining penalty actions. The bank should maintain documentation of its OFAC checks on new accounts, the existing customer base and specific transactions.

If a bank uses a third party, such as an agent or service provider, to perform OFAC checks on its behalf, as with any other responsibility performed by a third party, the bank is ultimately responsible for that third party's compliance with the OFAC requirements. As a result, banks should establish adequate controls and review procedures for such relationships.

Updating OFAC Lists

A bank's OFAC program should include policies, procedures, and processes for timely updating of the lists of blocked countries, entities, and individuals and disseminating such information throughout the bank's domestic operations and its offshore offices, branches and, in the case of Cuba and North Korea, foreign subsidiaries.

Reporting

An OFAC program should also include policies, procedures, and processes for handling items that are valid blocked or rejected items under the various sanctions programs. In the case of interdictions related to narcotics trafficking or terrorism, banks should notify OFAC as soon as possible by phone or e-hotline about potential hits with a follow-up in writing within ten days. Most other items should be reported through usual channels within ten days of the occurrence. The policies, procedures and processes should also address the management of blocked accounts. Banks are responsible for tracking the amount of blocked funds, the ownership of those funds, and interest paid on those funds. Total amounts blocked, including interest, must be reported to OFAC by September 30 of each year (information as of June 30). When a bank acquires or merges with another bank, both banks should take into consideration the need to review and maintain such records and information.

Banks no longer need to file Suspicious Activity Reports (SARs) on blocked narcotics or terrorism related transactions, as long as the bank files the required blocking report with OFAC. However, because blocking reports require only limited information, if the bank in possession of additional information not included on the blocking report filed with OFAC, a separate suspicious activity report should be filed with FinCEN including that information. In addition, the bank should file a SAR if the transaction itself would be considered suspicious in the absence of a valid OFAC match.[99]

[99] See FinCEN Release Number 2004-02 "Unitary Filing of Suspicious Activity and Blocking Reports" (69 *Federal Register* 76847, December 23, 2004).

Maintaining License Information

OFAC recommends that banks consider maintaining copies of customers' OFAC licenses on file. This will allow the bank to verify whether a customer is initiating a legal transaction. Banks should also be aware of the expiration date on the license. If it is unclear whether a particular transaction is authorized by a license, the bank should confirm with OFAC. Maintaining copies of licenses will also be useful if another bank in the payment chain requests verification of a license's validity. Copies of licenses should be maintained for five years, following the most recent transaction conducted in accordance with the license.

Independent Testing

Every bank should conduct an independent test of its OFAC program that is performed by the internal audit department, outside auditors, consultants, or other qualified independent parties. An in-depth audit should generally be conducted at least once a year. For large banks, the frequency and area of the independent test should be based on the known or perceived risk of specific business areas. For smaller banks, the audit should be consistent with the bank's OFAC risk profile or be based on a perceived risk. The person(s) responsible for testing should conduct an objective, comprehensive evaluation of OFAC policies, procedures, and processes. The audit scope should be comprehensive enough to assess OFAC compliance risks and evaluate the adequacy of the OFAC program.

Responsible Individual

It is recommended that every bank designate a qualified individual(s) to be responsible for the day-to day compliance of the OFAC program, including the reporting of blocked or rejected transactions to OFAC and the oversight of blocked funds. This individual must have an appropriate level of knowledge about OFAC regulations commensurate with the bank's OFAC risk profile.

Training

The bank should provide adequate training for all appropriate employees. The scope and frequency of the training should be consistent with the bank's OFAC risk profile and appropriate to employee responsibilities.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Overview – Developing Conclusions and Finalizing the Examination

OBJECTIVE

Formulate conclusions, communicate findings to management, prepare report comments, develop an appropriate supervisory response, and close the examination.

OVERVIEW

In the final phase of the BSA/AML examination, the examiner should assemble all findings from the procedures completed. From those findings, the examiner should develop conclusions about the BSA/AML compliance program's adequacy, discuss preliminary conclusions with bank management, present these conclusions in a written format for inclusion in the report of examination, and determine what regulatory response, if any, is appropriate.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Enterprise-Wide BSA/AML Compliance Program

OBJECTIVE

Assess the holding companies' or lead financial institution's[100] program for BSA/AML compliance.

OVERVIEW

Similar to the approach to consolidated credit, market, and operational risk, effective control of BSA/AML risk may call for coordinated risk management. An enterprise-wide BSA/AML compliance program coordinates the specific regulatory requirements throughout an organization inside a larger risk management framework. Such frameworks enable an organization to have a consolidated understanding of its risk exposure to money laundering and terrorist financing across all business units, functions, and legal entities. For example, the holding company or lead financial institution should have a centralized function to evaluate BSA/AML risk and world-wide exposure to a given customer, particularly those considered high-risk or suspicious, consistent with applicable laws.[101]

Many organizations, typically those that are more complex and may include international operations, implement an enterprise-wide BSA/AML compliance program that manages risks in an integrated fashion across affiliates, business lines, and risk types (e.g., reputation, compliance, or transaction). Some larger and more complex banking organizations are seeking to manage their risks by developing enterprise-wide approaches to their BSA/AML compliance program. Such programs manage risk at both operational and strategic levels.

While there are currently no regulatory requirements for holding companies or lead financial institutions to adopt an enterprise-wide BSA/AML compliance program, many organizations view this as an essential tool in managing the BSA/AML risks associated with failure to comply with BSA laws and regulations. A sound practice for complex organizations is to establish effective programs through the holding company or lead financial institution that view BSA/AML risks across legal entities, and allow

[100] The lead financial institution is the largest financial institution in the holding company structure in terms of assets unless otherwise designated by the holding company.

[101] Refer to the expanded overview section for additional guidelines on "Foreign Branches and Offices of U.S. Banks," page 107, and the Basel Committee on Bank Supervision's guidance on "Consolidated Know Your Customer (KYC) Risk Management."

management to demonstrate to their boards of directors that they have effective compliance programs in place across the consolidated organization. The program should reflect the organization's structure and be tailored to its size, complexity, and legal requirements that may vary due to the specific business line or host jurisdiction.[102]

The enterprise-wide program should include a central point where BSA/AML risks throughout the organization are aggregated. Structurally, the role could be established at either the level of the holding company or the lead financial institution. Therefore, banking organizations that implement such a program assess risk on a consolidated basis across all activities, business lines, and legal entities. Such consolidations may occur on a nationwide basis or may cross international boundaries depending on the locations of the operations. Enterprise-wide systems that operate on a global basis need to consider the various jurisdictions in which they operate as well as the AML laws and requirements they are subject to, and then incorporate these into their overall program. Internal audit should assess the level of compliance with the enterprise-wide BSA/AML compliance program.

SUBSIDIARIES, AFFILIATES, AND BUSINESS LINES

A holding company or a lead financial institution may decide to implement an enterprise-wide BSA/AML compliance program, either comprehensively or for specific business functions (e.g., audit or suspicious activity monitoring systems). Where business specific functions are so managed, in an examination or inspection, examiners must identify which portions of the BSA/AML compliance program are part of the enterprise-wide program. This information is critical when scoping and planning a BSA/AML examination.

When evaluating the enterprise-wide BSA/AML compliance program for adequacy, the examiner should determine reporting lines and how each subsidiary fits into the overall enterprise-wide compliance structure. The examiner should assess how effectively the holding company or lead financial institution monitors the compliance throughout the organization with the enterprise-wide BSA/AML compliance program, including how well the enterprise-wide system captures relevant data from the subsidiaries.

The evaluation of the enterprise-wide BSA/AML compliance program should reflect an assessment of the individual subsidiaries' BSA/AML compliance program adequacy. Regardless of the decision to implement an enterprise-wide BSA/AML compliance program in whole, or in part, the program must ensure that all affiliates meet their applicable regulatory requirements. For example, an audit program implemented solely on an enterprise-wide basis that does not conduct transaction testing at all bank subsidiaries would not be sufficient to meet regulatory requirements for independent testing for those bank subsidiaries.

[102] Policies and procedures at the branch or subsidiary level should be consistent with, although not necessarily identical to, group or holding company standards.

HOLDING COMPANY

Holding companies that centrally manage the operations and functions of their subsidiary banks and other subsidiaries should have comprehensive risk management policies, procedures, and processes in place to address the entire spectrum of risks. An adequate holding company enterprise-wide BSA/AML compliance program would provide the framework for all subsidiaries and foreign branches to meet their specific regulatory requirements (e.g., country or industry requirements). Accordingly, organizations that centrally manage an enterprise-wide BSA/AML compliance program should provide appropriate structure, develop guidelines, and set risk limits consistent with their domestic and international activities. Refer to the expanded overview section for additional guidelines on "Foreign Branches and Offices of U.S. Banks," page 107.

Organizations that implement an enterprise-wide BSA/AML compliance program should assess risk on a consolidated basis across all activities, business lines, and entities. Organizations often use software or programming solutions to assist in the implementation of the BSA/AML compliance program; these solutions typically include, but are not limited to, monitoring, identifying, and reporting suspicious activity. Some holding companies structure their enterprise-wide programs to centrally manage only specific functions of the BSA/AML compliance program (e.g., risk management information about high risk customers, account closures, audit and suspicious activity monitoring systems).

A bank holding company (BHC) or any non-bank subsidiary thereof, or a foreign financial institution that is subject to the BHC Act or any non-bank subsidiary of such a foreign financial institution operating in the United States is required to file a Suspicious Activity Report (SAR) with the appropriate federal law enforcement agencies, the Federal Reserve, and the U.S. Treasury, as required by 12 CFR 225.4(f). Certain savings and loan holding companies, and their non-depository subsidiaries, are required to file SARs pursuant to Treasury regulations. In addition, savings and loan holding companies, if not required, are strongly encouraged to file SARs in appropriate circumstances.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Correspondent Accounts (Domestic)

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with offering domestic correspondent account relationships, and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

Banks maintain correspondent relationships at other banks to provide certain services that can be performed more economically or efficiently because of the other bank's size, expertise in a specific line of business, or geographic location. Such services may include:

- Deposit accounts. Assets known as "due from bank deposits" or "correspondent bank balances" may represent the bank's primary operating account.
- Funds transfers. A transfer of funds between banks may result from the collection of cash items and cash letters, transfer and settlement of securities transactions, transfer of participating loan funds, purchase or sale of federal funds, or processing of customer transactions.
- Other services. Services include processing loan participations, facilitating secondary market loan sales, performing data processing and payroll services, and exchanging foreign currency.

Bankers' Banks

A bankers' bank, which is organized and chartered to do business with other banks, is generally owned by the banks it services. Bankers' banks, which do not conduct business directly with the public, offer correspondent banking services to independent community banks, thrifts, credit unions, and real estate investment trusts. Bankers' banks provide services directly, through outsourcing arrangements, or by sponsoring or endorsing third parties. The products bankers' banks offer normally consist of traditional correspondent banking services.

RISK FACTORS

Because domestic banks must follow the same regulatory requirements, BSA/AML risks in domestic correspondent banking are minimal in comparison to other types of financial services. Each bank, however, has its own approach for conducting its BSA/AML compliance program, including customer due diligence, management information systems, account monitoring, and reporting suspicious activities. Furthermore, while a

domestic correspondent account may not be considered high risk, transactions through the account, which may be conducted on behalf of the respondent's customer, may be high risk.

RISK MITIGATION

Banks that offer correspondent bank services to other domestic banks (the latter being known as respondent banks) should have policies, procedures, and processes to manage the BSA/AML risks involved in these correspondent relationships and to detect and report suspicious activities. The level of risk varies depending on the respondent bank's BSA/AML compliance program, products, services, customers, and geographic locations. Each bank should monitor transactions related to domestic correspondent accounts.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Correspondent Accounts (Foreign)

OBJECTIVE

Assess the adequacy of the U.S. bank's systems to manage the risks associated with foreign correspondent banking, and management's ability to implement effective due diligence, monitoring, and reporting systems. This section expands the earlier core review of statutory and regulatory requirements of foreign correspondent financial institution account relationships in order to provide a broader assessment of the AML risks associated with this activity.

OVERVIEW

Foreign financial institutions maintain accounts at U.S. banks to gain access to the U.S. financial system and to take advantage of services and products that may not be available in the foreign financial institution's jurisdiction. These services may be performed more economically or efficiently by the U.S. bank or may be necessary for other reasons, such as the facilitation of international trade. Services may include:

- Cash management services, including deposit accounts.
- International funds transfers.
- Check clearing.
- Payable through accounts.
- Pouch activities.
- Foreign exchange services.
- Overnight investment accounts (sweep accounts).
- Loans and letters of credit.

Contractual Agreements

Each relationship that a U.S. bank has with a foreign correspondent financial institution should be governed by an agreement or a contract describing each party's responsibilities and other relationship details (e.g., products and services provided, acceptance of deposits, clearing of items, forms of payment, and acceptable forms of endorsement). The agreement or contract should also consider the foreign correspondent's AML responsibilities, customer base, due diligence procedures, and customer referrals from the correspondent to the U.S. bank, clearly defining all referral terms (e.g., customer type and business profile, customer's geographic location, and any special terms).

RISK FACTORS

Some foreign financial institutions are not subject to the same or similar regulatory guidelines as U.S. banks; therefore, these foreign institutions may pose a higher money laundering risk to the correspondent U.S. bank. Investigations have disclosed that, in the past, foreign correspondent accounts have been used by drug traffickers and other criminal elements to launder funds. Shell companies are sometimes used in the layering process to hide the true ownership of accounts at foreign correspondent financial institutions. Because of the large amount of funds, multiple transactions, and the U.S. bank's potential lack of familiarity with the foreign correspondent financial institution's customer, criminals and terrorists can more easily conceal the source and use of illicit funds. Consequently, each U.S. bank should closely monitor transactions related to foreign correspondent accounts.

Without adequate controls, a U.S. bank may also set up a traditional correspondent account with a foreign financial institution and not be aware that the foreign financial institution is permitting some customers to conduct transactions anonymously through the U.S. bank account (e.g., payable through accounts[103] and nested accounts).

Nested Accounts

Nested accounts occur when a foreign financial institution gains access to the U.S. financial system by operating through a U.S. correspondent account belonging to another foreign financial institution. If the U.S. bank is unaware that its foreign correspondent financial institution customer is providing such access to third-party foreign financial institutions, these third-party financial institutions can effectively gain anonymous access to the U.S. financial system. Behavior indicative of nested accounts and other accounts of concern includes transactions to jurisdictions in which the foreign financial institution has no known business activities or interests and transactions in which the total volume significantly exceeds expected activity for the foreign financial institution, considering its customer base or asset size.

RISK MITIGATION

U.S. banks that offer foreign correspondent financial institution services should have policies, procedures, and processes to manage the BSA/AML risks inherent with these relationships and closely monitor transactions related to these accounts to detect and report suspicious activities. The level of risk varies depending on the foreign financial institution's products, services, customers, and geographic locations. Additional information relating to risk assessments and due diligence is contained in the core overview section "Foreign Correspondent Account Recordkeeping and Due Diligence" on page 68. The U.S. bank's policies, procedures, and processes should:

[103] Refer to expanded overview section "Payable Through Accounts" page 102 for additional information.

- Understand the intended use of the accounts and expected account activity (e.g., determine whether the relationship will serve as a payable through account).
- Understand the foreign correspondent financial institution's other correspondent relationships (e.g., determine whether nested accounts will be utilized).
- Assess the risks posed by the foreign correspondent financial institution relationships.
- Conduct adequate and ongoing due diligence on the foreign correspondent financial institution relationships, which may include periodic visits.
- Ensure foreign correspondent financial institution relationships are appropriately included within the U.S. bank's suspicious activity monitoring and reporting systems.
- Establish criteria for closing the foreign correspondent financial institution account.

As a sound practice, U.S. banks are encouraged to communicate their AML-related expectations to their foreign correspondent financial institution customers. Moreover, the U.S. bank should generally understand the AML controls at the foreign correspondent financial institution, including customer due diligence practices and recordkeeping documentation.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – U.S. Dollar Drafts

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with U.S. dollar drafts, and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

A U.S. dollar draft is a bank draft or check denominated in U.S. dollars and made available at foreign financial institutions. These drafts are drawn on a U.S. correspondent account by a foreign financial institution. Drafts are frequently purchased to pay for commercial or personal transactions and to settle overseas obligations.

RISK FACTORS

The majority of U.S dollar drafts are legitimate; however, drafts have proven, to be vulnerable to money laundering abuse. Such schemes involving U.S. dollar drafts could involve the smuggling of U.S. currency to a foreign financial institution for the purchase of a check or draft denominated in U.S. dollars. The foreign financial institution accepts the U.S. currency and issues a U.S. dollar draft drawn against its U.S. correspondent bank account. Once the currency is in bank draft form, the money launderer can more easily conceal the source of funds. The ability to convert illicit proceeds to a bank draft at a foreign financial institution makes it easier for a money launderer to transport the instrument either back into the United States or to endorse it to a third party in a jurisdiction where money laundering laws or compliance are lax. In any case, the individual has laundered illicit proceeds; ultimately, the draft or check will be returned for processing at the U.S. correspondent bank.

RISK MITIGATION

A U.S. bank's policies, procedures, and processes should include the following:

- Outline criteria for opening a U.S. dollar draft relationship with a foreign financial institution or entity (e.g., jurisdiction; products, services, target market; purpose of account and anticipated activity; or customer history).
- Detail acceptable and unacceptable transactions (e.g., structuring transactions or the purchase of multiple sequentially numbered drafts for the same payee).
- Detail the monitoring and reporting of suspicious activity associated with U.S. dollar drafts.
- Discuss criteria for closing U.S. dollar draft relationships.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Payable Through Accounts

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with payable through accounts (PTAs), and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

Foreign financial institutions use PTAs, also known as "pass-through" or "pass-by" accounts, to provide their customers with access to the U.S. banking system. Some U.S. banks, Edge Act and agreement corporations, and U.S. branches and agencies of foreign financial institutions (collectively referred to as U.S. banks) offer these accounts as a service to foreign financial institutions. Law enforcement authorities have stated that the risk of money laundering and other illicit activities is high in PTA accounts that are not adequately controlled.

Generally, a foreign financial institution requests a PTA for its customers that want to conduct banking transactions in the United States through the foreign financial institution's account at a U.S. bank. The foreign financial institution provides its customers, commonly referred to as "sub-accountholders," with checks that allow them to draw funds from the foreign financial institution's account at the U.S. bank.[104] The sub-accountholders, which may number several hundred or in the thousands for one PTA, all become signatories on the foreign financial institution's account at the U.S. bank. While payable through customers are able to write checks and make deposits at a bank in the United States like any other accountholder, they might not be directly subject to the bank's account opening requirements in the United States.

PTA activities should not be confused with traditional international correspondent banking relationships, in which a foreign financial institution enters into an agreement with a U.S. bank to process and complete transactions on behalf of the foreign financial institution and its customers. Under the latter correspondent arrangement, the foreign financial institution's customers do not have direct access to the correspondent account at the U.S. bank, but they do transact business through the U.S. bank. This arrangement differs significantly from a PTA with sub-accountholders who have direct access to the U.S. bank by virtue of their independent ability to conduct transactions with the U.S. bank through the PTA.

[104] In this type of relationship, the foreign financial institution is commonly referred to as the "master accountholder."

RISK FACTORS

PTAs may be prone to higher risk because U.S. banks do not typically implement the same due diligence requirements for PTAs that they require of domestic customers who want to open checking and other accounts. For example, some U.S. banks merely request a copy of signature cards completed by the payable through customers (the customer of the foreign financial institution). These U.S. banks then process thousands of sub-accountholder checks and other transactions, including currency deposits, through the foreign financial institution's PTA. In most cases, little or no independent effort is expended to obtain or confirm information about the individual and business sub-accountholders that use the PTAs.

Foreign financial institutions' use of PTAs, coupled with inadequate oversight by U.S. banks, may facilitate unsound banking practices, including money laundering and related criminal activities. The potential for facilitating money laundering or terrorist financing, OFAC violations, and other serious crimes increases when a U.S. bank is unable to identify and adequately understand the transactions of the ultimate users (all or most of whom are outside of the United States) of its account with a foreign correspondent. PTAs used for illegal purposes can cause banks serious financial losses in criminal and civil fines and penalties, seizure or forfeiture of collateral, and reputation damage.

RISK MITIGATION

U.S. banks offering PTA services should develop and maintain adequate policies, procedures, and processes to guard against possible illicit use of these accounts. At a minimum, policies, procedures, and processes should enable each U.S. bank to identify the ultimate users of its foreign financial institution PTA and should include the bank's obtaining (or having the ability to obtain through a trusted third-party arrangement) substantially the same information on the ultimate PTA users as it obtains on its direct customers.

Policies, procedures, and processes should include a review of the foreign financial institution's processes for identifying and monitoring the transactions of sub-accountholders and for complying with any AML statutory and regulatory requirements existing in the host country and the foreign financial institution's master agreement with the U.S. bank. In addition, U.S. banks should have procedures for monitoring transactions conducted in foreign financial institutions' PTAs.

In an effort to address the risk inherent in PTAs, U.S. banks should have a signed contract (i.e., master agreement) that includes:

- 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 sub-accountholders (e.g., casas de cambio, finance companies, funds remitters, or other non-bank financial institutions).

- Prohibitions or restrictions on multi-tier sub-accountholders.[105]
- Access to the foreign financial institution's internal documents and audits that pertain to its PTA activity.

U.S. banks should consider closing the PTA in the following circumstances:

- Insufficient information on the ultimate PTA users.
- Evidence of substantive or ongoing suspicious activity.
- Inability to ensure that the PTAs are not being used for money laundering or other illicit purposes.

[105] It is possible for a sub-account to be sub-split into further sub-accounts for separate persons.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Pouch Activities

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with pouch activities, and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

Pouch activity entails the use of a carrier, courier (either independent or common), or a referral agent employed by the courier,[106] to transport currency, monetary instruments, and other documents from outside the United States to a bank in the United States.[107] Pouches can be sent by another bank or individuals. Pouch services are commonly offered in conjunction with foreign correspondent banking services. Pouches can contain loan payments, transactions for demand deposit accounts, or other types of transactions.

RISK FACTORS

Banks should be aware that bulk amounts of monetary instruments purchased in the United States that appear to have been structured to avoid the BSA-reporting requirements often have been found in pouches or cash letters received from foreign financial institutions. This is especially true in the case of pouches and cash letters received from jurisdictions with lax or deficient AML structures. The monetary instruments involved are frequently money orders, traveler's checks, and bank checks that usually have one or more of the following characteristics in common:

- The instruments were purchased on the same or consecutive days at different locations.
- They are numbered consecutively in amounts just under $3,000 or $10,000.
- The payee lines are left blank or made out to the same person (or to only a few people).
- They contain little or no purchaser information.
- They bear the same stamp, symbol, or initials.

[106] Referral agents are foreign individuals or corporations, contractually obligated to the U.S. bank. They provide representative-type services to the bank's clients abroad for a fee. Services can range from referring new customers to the bank, to special mail handling, obtaining and pouching documents, distributing the bank's brochures and applications or forms, notarizing documents for customers, and mailing customers' funds to the bank in the United States for deposit.

[107] For additional guidance, refer to core overview section "International Transportation of Currency or Monetary Instruments Reporting" on page 83.

- They are purchased in round denominations or repetitive amounts.
- The depositing of the instruments is followed soon after by a funds transfer out in the same dollar amount.

RISK MITIGATION

Banks should have policies, procedures, and processes related to pouch activity that should:

- Outline criteria for opening a pouch relationship with an individual or a foreign financial institution (e.g., customer due diligence requirements, type of institution or person, acceptable purpose of the relationship).
- Detail acceptable and unacceptable transactions (e.g., monetary instruments with blank payees, unsigned monetary instruments, and a large number of consecutively numbered monetary instruments).
- Detail procedures for processing the pouch, including employee responsibilities, dual control, reconciliation and documentation requirements, and employee sign off.
- Detail procedures for reviewing for unusual or suspicious activity, including elevating concerns to management. (Contents of pouches may be subject to Currency Transaction Report (CTR), Report of International Transportation of Currency or Monetary Instruments (CMIR), and Suspicious Activity Report (SAR) reporting requirements.)
- Discuss criteria for closing pouch relationships.

The above factors should be included within an agreement or contract between the bank and the courier that details the services to be provided and the responsibilities of both parties.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Foreign Branches and Offices of U.S. Banks

OBJECTIVE

Assess the adequacy of the U.S. bank's systems to manage the risks associated with its foreign branches and offices, and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

U.S. banks open foreign branches and offices[108] to meet specific customer demands, to help the bank grow, or to expand products or services offered. Foreign branches and offices vary significantly in size, complexity of operations, and scope of products and services offered. Examiners must take these factors into consideration when reviewing whether the foreign branches and offices adhere to the bank's BSA/AML compliance program. AML policies, procedures, and processes at the foreign office or branch should comply with local requirements and be consistent with the U.S. bank's standards; however, they may need to be tailored for local or business practices.[109]

RISK FACTORS

Examiners should understand the type of products and services offered at foreign branches and offices, as well as the customers and geographic locations served at the foreign branches and offices. Any service offered by the U.S. bank may be offered by the foreign branches and offices if not prohibited by the host country. Such products and services offered at the foreign branches and offices may have a different risk profile from that of the same product or service offered in the U.S. bank (e.g., money services businesses are regulated in the United States; however, similar entities in another country may not be regulated). Therefore, the examiner should be aware that risks associated with foreign branches and offices may differ (e.g., wholesale versus retail operations).

The examiner should understand the foreign jurisdictions' various AML requirements. Secrecy laws or their equivalent may affect the ability of the foreign branch or office to share information with the U.S. parent bank, or the ability of the examiner to examine on-site. Although specific BSA requirements are not applicable at foreign branches and offices, banks are expected to have policies, procedures, and processes in place at all their

[108] This includes affiliates and subsidiaries.

[109] For additional information refer to "Consolidated Know Your Customer (KYC) Risk Management," Basel Committee on Banking Supervision, 2004, at www.bis.org/publ.

branches and offices to protect against risks of money laundering and terrorist financing. In this regard, foreign branches and offices should be guided by the U.S. bank's BSA/AML policies, procedures, and processes. The foreign branches and offices must comply with OFAC requirements and all local AML-related laws, rules, and regulations.

RISK MITIGATION

Branches and offices of U.S. banks located in high-risk geographic locations may be vulnerable to abuse by money launderers. To address this concern, the U.S. bank's policies, procedures, and processes for the foreign operation should be consistent with the following recommendations:

- The U.S. bank's head office and management at the foreign operation should understand the effectiveness and quality of bank supervision in the host country and understand the legal and regulatory requirements of the host country. The U.S. bank's head office should be aware of and understand any concerns that the host country supervisors' may have with respect to the foreign branch or office.
- The U.S. bank's head office should understand the foreign branches' or offices' risk profile (e.g., products, services, customers, and geographic locations).
- The U.S. bank's head office and management should have access to sufficient information in order to periodically monitor the activity of their foreign branches and offices, including the offices' and branches' level of compliance with head office policies, procedures and processes. Some of this may be achieved through management information systems reports.
- The U.S. bank's head office should develop a system for testing and verifying the integrity and effectiveness of internal controls at the foreign branches or offices by conducting in-country audits. Senior management at the head office should obtain and review copies, written in English, of audit reports and any other reports related to AML and internal control evaluations.
- The U.S. bank's head office should establish robust information sharing practices between branches and offices, particularly regarding high-risk account relationships.
- The U.S. bank's head office should be able to provide examiners with any information deemed necessary to assess compliance with U.S. banking laws.

Foreign branch and office compliance and audit structures can vary substantially based on the scope of operations (e.g., geographic locations) and the type of products, services, and customers. Foreign branches and offices with multiple locations within a geographic region (e.g., Europe, Asia, and South America) are frequently overseen by regional compliance and audit staff. Regardless of the size or scope of operations, the compliance and audit staff and audit programs should be sufficient to oversee the AML risks.

SCOPING AML EXAMINATIONS

Examinations may be completed in the host country or in the United States. The factors that will be considered in deciding whether the examination work should occur in the host jurisdiction or the United States include:

- The risk profile of the foreign branch or office and whether the profile is stable or changing as a result of a reorganization, the introduction of new products or services, or other factors, including the risk profile of the jurisdiction itself.
- The effectiveness and quality of bank supervision in the host country.
- Existence of information sharing agreement between the host country and the U.S. supervisor.
- The history of examination or audit concerns at the foreign branch or office.
- The size and complexity of the foreign branch's or office's operations.
- Effectiveness of internal controls, including systems for managing AML risks on a consolidated basis and internal audit.
- The capability of management at the foreign branch or office to protect the entity from money laundering or terrorist financing.
- The availability of the foreign branch or office records in the United States.

In some jurisdictions, financial secrecy and other laws may prevent or severely limit U.S. examiners or U.S. head office staff from directly evaluating customer activity or records. In cases where an on-site examination cannot be conducted effectively, examiners should consult with appropriate agency personnel. In such cases, agency personnel may contact foreign supervisors to make appropriate information sharing or examination arrangements. In low-risk situations where information is restricted, examiners may conduct U.S.-based examinations (see discussion below). In high-risk situations when adequate examinations (on-site or otherwise) cannot be effected, the agency may require the head office to take action to address the situation, which may include closing the foreign office.

U.S.-Based Examinations

U.S.-based, or off-site examinations, generally require greater confidence in the AML program at the foreign branch or office, as well as the ability to access sufficient records. Such off-site examinations should include discussions with senior bank management at the head and foreign offices which are crucial to the understanding of the foreign branches or offices' operations, AML risks, and AML programs. Also, the examination of the foreign branch or office should include a review of the U.S. bank's involvement in managing or monitoring the foreign branch's operations, internal control systems (e.g., policies, procedures, and monitoring reports), and, where available, the host country supervisors' examination findings, audit findings, and workpapers. As with all BSA/AML examinations, the extent of transaction testing and activities where it is performed is based on various factors including the examiner's judgment of risks, controls, and the adequacy of the independent testing.

Host Jurisdiction-Based Examinations

The standard scoping and planning process will determine the focus of the examination and the resource needs. There may be some differences in the examination process conducted abroad. The host supervisory authority may send an examiner to join the U.S.

team or request attendance at meetings at the beginning and at the conclusion of the examination.

AML reporting requirements also are likely to be different, as they will be adjusted to local regulatory requirements. In addition, on-site work in the host jurisdiction will enable examiners to better understand the role of the U.S. bank in relation to its foreign branch or office.

For both U.S.-based and host-based examinations of foreign branches and offices, the procedures used for specific products, services, and customers are those found in this manual. For example, if an examiner is looking at pouch activities at foreign branches and offices, he or she should use applicable expanded examination procedures.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Parallel Banking

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with parallel banking relationships, and management's ability to implement effective due diligence, monitoring, and reporting systems.

OVERVIEW

A parallel banking organization exists when at least one U.S. bank and one foreign financial institution are controlled either directly or indirectly by the same person or group of persons who are closely associated in their business dealings or otherwise acting together, but are not subject to consolidated supervision by a single home country supervisor. The foreign financial institution will be subject to different money laundering rules and regulations and a different supervisory oversight structure, both of which may be less stringent than in the United States. The regulatory and supervisory differences heighten the BSA/AML risk associated with parallel banking organizations.

RISK FACTORS

Parallel banking organizations may have common management, share policies and procedures, cross-sell products, or generally be linked to a foreign parallel financial institution in a number of ways. The key money laundering concern regarding parallel banking organizations is that the U.S. bank may be exposed to greater risk through transactions with the foreign parallel financial institution. Transactions may be facilitated and risks heightened because of the lack of arm's-length dealing or reduced controls on transactions between banks that are linked or closely associated. For example, officers or directors may be common to both entities or may be different but nonetheless work together.

RISK MITIGATION

The U.S. bank's policies, procedures, and processes for parallel banking relationships should be consistent with those for other foreign correspondent bank relationships. In addition, parallel banks should:

- Provide for independent lines of decision-making authority.
- Guard against conflicts of interest.
- Ensure independent and arm's-length dealings between the related entities.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Electronic Banking

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with electronic banking (e-banking) customers, and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

E-banking systems, which provide electronic delivery of banking products to customers, include automated teller machine (ATM) transactions; online account opening; Internet banking transactions; and telephone banking. For example, credit cards, deposit accounts, mortgage loans, and funds transfers can all be initiated online, without face-to-face contact. Management needs to recognize this as a potentially high-risk area and develop adequate policies, procedures, and processes for customer identification and monitoring for specific areas of banking. Refer to the core procedures section "Customer Identification Programs" (CIP) page 179 for additional information. Additional information on e-banking is available in the FFIEC *Information Technology Examination Handbook.*[110]

RISK FACTORS

Banks should ensure that their monitoring systems adequately capture transactions conducted electronically. As with any account, they should be alert to anomalies in account behavior. Red flags may include the velocity of funds in the account or, in the case of ATMs, the number of debit cards associated with the account.

Accounts that are opened without face-to-face contact may be a higher risk for money laundering and terrorist financing for the following reasons:

- More difficult to positively verify the individual's identity.
- Customer may be out of the bank's targeted geographic area or country.
- Customer may perceive the transactions as less transparent.
- Transactions are instantaneous.
- May be used by a "front" company or unknown third party.

[110] The FFIEC *Information Technology Examination Handbook* is available at www.ffiec.gov/ffiecinfobase/html_pages/it_01.html

RISK MITIGATION

Banks should establish BSA/AML monitoring, identification, and reporting for unusual and suspicious activities occurring through e-banking systems. Useful management information systems for detecting unusual activity in high-risk accounts include ATM activity reports, funds transfer reports, new account activity reports, change of Internet address reports, Internet Protocol (IP) address reports, and reports to identify related or linked accounts (e.g., common addresses, phone numbers, e-mail addresses, and tax identification numbers). In determining the level of monitoring required for an account, banks should include how the account was opened as a factor. Banks should consider whether customers seeking certain financial services, such as electronic banking, should be required to open accounts on a face-to-face basis. Other controls, such as establishing transaction dollar limits for large items that require manual intervention to exceed the preset limit, may also be instituted by the bank.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Funds Transfers

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with funds transfers, and management's ability to implement effective monitoring and reporting systems. This section expands the core review of the statutory and regulatory requirements of funds transfers to provide a broader assessment of AML risks associated with this activity.

OVERVIEW

Payment systems in the United States consist of numerous financial intermediaries, financial services firms, and non-bank businesses that create, process, and distribute payments. The domestic and international expansion of the banking industry and non-bank financial services has increased the importance of electronic funds transfers, including funds transfers made through the wholesale payment systems. Additional information on the types of wholesale payment systems is available in the FFIEC *Information Technology Examination Handbook*.[111]

FUNDS TRANSFER SERVICES

A vast majority of the value of U.S. dollar payments in the United States are ultimately processed through wholesale payment systems, which generally handle large-value transactions between banks and either large financial services providers or non-bank financial institutions. For comparison, retail transfer systems include automated clearing houses (ACHs), automated teller machines (ATMs), point-of-sale (POS) systems, telephone bill paying, home banking systems, debit cards, and "smart cards," which are gaining widespread customer use. Most of these retail transactions are initiated by customers rather than by banks or corporate users. These individual transactions may then be combined into larger wholesale transfers, which are the focus of this section. In addition, banks conduct numerous wholesale transfers on their own behalf as well as for the benefit of other financial service providers and bank customers (corporate and consumer).

The two primary wholesale payment systems for interbank, or large-value, domestic funds transfer payment orders are Fedwire®[112] and the Clearing House Interbank

[111] The FFIEC *Information Technology Examination Handbook* is available at www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

[112] Fedwire® is a registered service mark of the Federal Reserve Banks. See www.frbservices.org/Wholesale/fedwirefunds.html for further information.

Payments System (CHIPS).[113] The bulk of the dollar value of these payments is processed electronically and is used to purchase, sell, or finance securities transactions; disburse or repay loans; settle real estate transactions; and make large-value, time-critical payments, such as payments for the settlement of interbank purchases and sales of federal funds, settlement of foreign exchange transactions, or other financial market transactions. Fedwire and CHIPS participants facilitate these transactions for non-bank financial institutions and commercial businesses, as well as for banks that do not have direct access.

Structurally there are two components to funds transfers: The instruction, which contains the information on the ultimate sender and receiver of the funds, and the actual movement or transfer of funds. The instructions are sent in a variety of ways, including by e-mail, facsimile (fax), telephone, or telex; by electronic access to the networks of the Fedwire or CHIPS payment systems; and by access to financial telecommunications systems, such as Society for Worldwide Interbank Financial Telecommunication (SWIFT). Fedwire is used for U.S. dollar transfers that are wholly domestic transactions and to facilitate the US dollar leg of international transactions. CHIPS can also be used for U.S. dollar transfers that are wholly domestic and to facilitate the U.S. dollar leg of international transactions, but CHIPS has been predominantly used to facilitate international transactions. SWIFT is an international messaging service that is used to transmit payment instructions for the vast majority of international interbank transactions, which are denominated in numerous currencies.

Fedwire

Fedwire, operated by the Federal Reserve Banks, allows any bank with a Federal Reserve account to transfer funds from that account to the Federal Reserve account of any other bank. Payment to the receiving participant (payee) over Fedwire is final and irrevocable when the Federal Reserve Bank either credits the amount of the payment order to the receiving participant's Federal Reserve Bank reserve account or sends notice to the receiving participant, whichever is earlier. Participants[114] may access Fedwire by four methods:

[113] CHIPS is a private multilateral settlement system owned and operated by The Clearing House Payments Company.

[114] Fedwire participants are any entities that maintain an account with a Federal Reserve Bank in the entity's name. Subject to the Federal Reserve Banks' and the Board of Governors of the Federal Reserve System's risk reduction policies, when applicable, entities authorized by law, regulation, policy, or agreement to be participants include:

- Depository institutions.
- Agencies and branches of foreign banks.
- Member banks of the Federal Reserve System.
- The U.S. Treasury and any entity specifically authorized by federal statute to use the Federal Reserve Banks as fiscal agents or depositories.
- Entities designated by the Secretary of the Treasury.
- Foreign central banks, foreign monetary authorities, foreign governments, and certain international organizations.

- Direct computer interface.
- Offline via telephone with a Federal Reserve Bank.
- Web-based access via virtual private network that can be accessed through the Internet or dial-up connection.
- Dial-up access via a computer-based system.[115]

Although there is no settlement risk to Fedwire participants, they may be exposed to risk caused by errors and omissions and fraud.

CHIPS

CHIPS is a privately operated, real-time, multilateral payments system typically used for large-dollar payments. CHIPS is owned by banks, and any banking organization with a regulated U.S. presence may become an owner and participate in the network. The payments transferred over CHIPS are often related to international interbank transactions, including the dollar payments resulting from foreign currency transactions (such as currency swap contracts) and euro placements and returns. Payment orders are also sent over CHIPS to adjust correspondent balances and make payments associated with commercial transactions, bank loans, and securities transactions.

SWIFT

The SWIFT network is a messaging infrastructure that provides users with a private international communications link among themselves. The actual U.S. dollar funds movements (payments) are completed through correspondent bank relationships, Fedwire, or CHIPS. In addition to customer and bank funds transfers, SWIFT is used to transmit foreign exchange confirmations, debit and credit entry confirmations, statements, collections, and documentary credits.

Informal Value Transfer Systems

Informal value transfer systems (IVTS) (e.g., hawalas) is a term used to describe currency or value transfer systems that operate informally to transfer money as a business.[116] In

- Any other entities authorized by a Federal Reserve Bank to use the Fedwire Securities Service.

[115] Fedwire participants will be gradually phased off of the dial-up computer based system to the web-based access method.

[116] Sources of information on IVTS include:

- FinCEN Advisory 33, "Informal Value Transfer Systems," March 2003.
- U.S. Treasury "Informal Value Transfer Systems Report to the Congress in Accordance with Section 359 of the Patriot Act," November 2002.
- FATF, "Interpretative Note to Special Recommendation VI: Alternative Remittance," June 2003.
- FATF, "Combating the Abuse of Alternative Remittance Systems, International Best Practices," October 2002.

countries lacking a stable financial sector or with large areas not served by formal banks, IVTS may be the only method for conducting financial transactions. Persons living in the United States may also use IVTS to transfer funds to their home countries.

Payable Upon Proper Identification

One type of funds transfer transaction that carries particular risk is the payable upon proper identification (PUPID) service. PUPID transactions are funds transfers for which there is no specific account to deposit the funds into and the beneficiary of the funds is not a bank customer. For example, an individual that has an account at a bank may transfer funds to a relative or an individual who does not have an account relationship with a bank at another location (e.g., city, state, or jurisdiction). In this case, the beneficiary bank may place the incoming funds into a suspense account and ultimately release the funds when the individual provides proof of identity.

RISK FACTORS

The size and complexity of a bank's operation and the origin and destination of the funds being transferred will determine which type of funds transfer system the bank uses. The vast majority of funds transfer instructions are conducted electronically; however, examiners need to be mindful that physical instructions may be transmitted by other informal methods, as described earlier.

IVTS pose a heightened concern because they are able to circumvent the formal system. The lack of recordkeeping requirements coupled with the lack of identification of the IVTS participants may attract money launderers and terrorists. IVTS also pose heightened BSA/AML concerns because they can evade internal controls and monitoring oversight established in the formal banking environment. Principals that operate IVTS frequently use banks to settle accounts.

The risks of PUPID transactions to the beneficiary bank are similar to other activities in which the bank does business with noncustomers. However, the risks are heightened in PUPID transactions, because the bank allows a noncustomer to access the funds transfer system by providing minimal or no identifying information. Some banks that allow noncustomers to transfer funds using the PUPID service pose significant risk to both the originating and beneficiary banks. In these situations, both banks have minimal or no identifying information on the originator or the beneficiary.

RISK MITIGATION

Funds transfers can be used in the placement, layering, and integration stages of money laundering. Funds transfers purchased with currency are an example of the placement stage. Detecting unusual activity in the layering and integration stages is more difficult for a bank; such transactions may appear legitimate. In many cases, a bank may not be involved in the placement of the funds or in the final integration, only the layering of

transactions. Banks should consider all three stages of money laundering when evaluating or assessing funds transfer risks.

Banks need to have sound policies, procedures, and processes to manage the BSA/AML risks of its funds transfer activities. Such policies may encompass more than regulatory recordkeeping minimums and be expanded to cover OFAC.

Obtaining customer due diligence (CDD) information is an important mitigant of risk in providing funds transfer services. Because of the nature of funds transfers, adequate and effective CDD policies, procedures, and processes are critical in detecting unusual and suspicious activities. Equally important is an effective risk-based suspicious activity monitoring and reporting system.

Originating and beneficiary banks should establish effective and appropriate policies, procedures, and processes for PUPID activity including:

- Specifying the type of identification that is acceptable.
- Maintaining documentation of individuals consistent with the bank's recordkeeping policies.
- Defining which bank employees may conduct PUPID transactions.
- Establishing limits on the amount of funds that may be transferred to or from the bank for noncustomers (including type of funds accepted (i.e., currency or official check) by originating bank).
- Monitoring and reporting suspicious activities.
- Providing enhanced scrutiny for transfers to or from certain jurisdictions.
- Identifying disbursement method (i.e., by currency or official check) for proceeds from beneficiary bank.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Electronic Cash

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with electronic cash (e-cash), and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

E-cash is a digital representation of money. E-cash (or e-money) comes in two basic forms: stored value card e-cash and computer e-cash. Stored value card e-cash is most often downloaded through special terminals (e.g., specially equipped automated teller machines (ATMs), computers, or cellular phones) onto electronic cards. Computer e-cash is downloaded to personal computer hard disks via a modem or stored in an online repository.

Consumers use e-cash to access, store, and redeem funds that are maintained electronically. The transfer of funds to the card is a form of prepayment (e.g., telephone calling cards). In addition, e-cash, in the form of payroll cards, is now offered by employers to their employees in place of a check to distribute wages. The value of the funds stored on these cards can be transferred between vendors and individuals using compatible electronic systems, often without using banks.

Using special readers, stored monetary value is subtracted from the card. When the monetary value is depleted, the card is either discarded or, in some instances, value is replenished. In the case of computer e-cash, monetary value is electronically deducted from the bank account when a purchase is made. Additional information on types of e-cash products is available in the FFIEC *Information Technology Examination Handbook*.[117]

RISK FACTORS

Transactions using e-cash may pose the following unique risks to the bank:

- Funds may be transferred to or from an unknown third party.
- As e-cash is accepted worldwide, customers can avoid border restrictions as the transactions can become mobile and may not be subject to jurisdictional restrictions.

[117] The FFIEC *Information Technology Examination Handbook* is available at www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

- Transactions are instantaneous.
- The customer may perceive the transactions as less transparent.

RISK MITIGATION

Banks should establish BSA/AML monitoring, identification, and reporting for unusual and suspicious activities occurring through e-cash facilities. Useful management information systems for detecting unusual activity on high-risk accounts include, ATM activity reports (focusing on foreign transactions), funds transfer reports, new account activity reports, change of Internet address reports, Internet Protocol (IP) address reports, and reports to identify related or linked accounts (e.g., common addresses, phone numbers, e-mail addresses, and tax identification numbers). Other controls, such as establishing transaction and account dollar limits that require manual intervention to exceed the preset limit, may also be instituted by the bank.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Third-Party Payment Processors

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with its relationships with third-party payment processors, and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

Non-bank, or third-party, payment processors (processors) are bank customers that provide payment-processing services to merchants and other business entities.

Traditionally, processors contracted primarily with retailers that had physical locations in order to process the retailers' transactions. These merchant transactions primarily included credit card payments but also covered automated clearing house demand drafts[118] (also known as e-checks), and debit and stored value cards transactions. With the expansion of the Internet, retail borders have been eliminated. Processors may now service a variety of merchant accounts, including conventional retail and Internet-based establishments, prepaid travel, and Internet gaming enterprises.

RISK FACTORS

Processors generally are not subject to BSA/AML regulatory requirements. As a result, some processors may be vulnerable to money laundering, identity theft, and fraud schemes.

The bank's BSA/AML risks when dealing with a processor account are similar to risks from other activities in which the bank's customer conducts transactions through the bank on behalf of the customer's clients. When the bank is unable to identify and understand the nature and source of the transactions processed through an account, the risks to the bank and the likelihood of suspicious activity can increase. If a bank has not implemented an adequate processor-approval program that goes beyond credit risk management, it could be vulnerable to processing illicit or sanctioned transactions.

[118] A demand draft is a substitute for a preprinted paper check. The draft is produced without a consumer signature but presumably with the consumer's authorization.

RISK MITIGATION

Banks offering account services to processors should develop and maintain adequate policies, procedures, and processes to address risks related to these relationships. At a minimum, these policies should authenticate the processor's business operations and assess their risk level. Verification and assessment of a processor can be completed by performing the following procedures:

- Reviewing the processor's promotional materials, including its web site, to determine the target clientele. (Businesses with elevated risk may include: offshore companies, online gambling-related operations, and online payday lenders). For example, a processor whose customers are primarily offshore would be inherently riskier than a processor whose customers are primarily restaurants.
- Determining whether the processor re-sells its services to a third party who may be referred to as an "agent or provider of Independent Sales Organization (ISO) opportunities" or "gateway" arrangements.[119]
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of its due diligence standards for new merchants.
- Identifying the processor's major customers.
- Reviewing corporate documentation including independent reporting services and, if applicable, documentation on principal owners.
- Visiting the processor's business operations center.

Banks that provide account services should monitor their processor relationships for any significant changes in the processors' business strategies that may affect their risk profile. Banks should periodically re-verify and update the businesses' profiles to ensure the risk assessment is appropriate.

In addition to adequate and effective account opening and due diligence procedures for processor accounts, management should monitor these relationships for unusual and suspicious activities. To effectively monitor these accounts, the bank should have an understanding of the following processor information:

- Merchant base.
- Merchant activities.
- Average number of dollar volume and number of transactions.
- "Swiping" versus "keying" volume for credit card transactions.
- Charge-back history.

[119] Gateway arrangements are similar to an Internet service provider with excess computer storage capacity who sells its capacity to a third party, who would then distribute computer service to various other individuals unknown to the provider. The third party would be making decisions about who would be receiving the service, although the provider would be providing the ultimate storage capacity. Thus, the provider bears all of the risks while receiving a smaller profit.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Purchase and Sale of Monetary Instruments

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with monetary instruments, and management's ability to implement effective monitoring and reporting systems. This section expands the core review of statutory and regulatory requirements for purchase and sale of monetary instruments in order to provide a broader assessment of the money laundering risks associated with this activity.

OVERVIEW

Monetary instruments are products provided by banks and include cashier's checks, traveler's checks, and money orders. Monetary instruments are typically purchased to pay for commercial or personal transactions and, in the case of traveler's checks, as a form of stored value for future purchases.

RISK FACTORS

The purchase or exchange of monetary instruments at the placement and layering stages of money laundering can conceal the source of illicit proceeds. As a result, banks have been major targets in laundering operations because they provide and process monetary instruments through deposits. For example, customers or noncustomers have been known to purchase monetary instruments in amounts below the $3,000 threshold to avoid having to provide adequate identification. Subsequently, monetary instruments are then placed into deposit accounts to circumvent the Currency Transaction Report (CTR) filing threshold.

RISK MITIGATION

Banks selling monetary instruments should have appropriate policies, procedures, and processes in place to mitigate risk. Policies should define:

- Acceptable and unacceptable monetary instrument transactions (e.g., noncustomer transactions, monetary instruments with blank payees, unsigned monetary instruments, identification requirements for structured transactions or the purchase of multiple sequentially numbered monetary instruments for the same payee).
- Procedures for reviewing for unusual or suspicious activity, including elevating concerns to management.
- Criteria for closing relationships or refusing to do business with noncustomers who have consistently or egregiously been involved in suspicious activity.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Brokered Deposits

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with brokered deposit relationships, and management's ability to implement effective due diligence, monitoring, and reporting systems.

OVERVIEW

The use of brokered deposits is a common funding source for many banks. Recent technology developments allow brokers to provide bankers with increased access to a broad range of potential investors who have no relationship with the bank. Deposits can be raised over the Internet, through certificates of deposit listing services, or through other advertising methods.

Deposit brokers provide intermediary services for banks and investors. This activity is considered higher risk because each deposit broker operates under its own guidelines for obtaining deposits. The level of regulatory oversight over deposit brokers varies, as does the applicability of BSA/AML requirements directly on the deposit broker. However, the deposit broker is subject to OFAC requirements regardless of its regulatory status. Consequently, the deposit broker may not be performing adequate due diligence, OFAC screening (for additional information refer to the core overview section "Office of Foreign Assets Control" on page 84), or Customer Identification Program (CIP) procedures. The bank accepting brokered deposits depends on the deposit broker to sufficiently perform required account opening procedures and to follow applicable BSA/AML compliance program requirements.

RISK FACTORS

Money laundering and terrorist financing risks arise because the bank may not know the ultimate beneficial owners or the source of funds. The deposit broker could represent a range of clients that may be of high risk for money laundering and terrorist financing (e.g., nonresident or offshore customers, politically exposed persons (PEPs), or foreign shell banks).

RISK MITIGATION

Banks that accept deposit broker accounts or funds should develop appropriate policies, procedures, and processes that establish minimum CDD procedures for all deposit brokers providing deposits to the bank. The level of due diligence a bank performs

should be commensurate with its knowledge of the deposit broker and the deposit broker's known business practices and customer base.

In an effort to address the risk inherent in deposit broker relationships, banks should have a signed contract that sets out the roles and responsibilities of each party and restrictions on types of customers (e.g., nonresident or offshore customers, PEPs, or foreign shell banks). Banks should conduct sufficient due diligence on unknown, foreign, independent, or unregulated deposit brokers. To manage the BSA/AML risks associated with brokered deposits, the bank should:

- Determine whether the deposit broker is a legitimate business, in all operating locations where the business is conducted.
- Review the deposit broker's business strategies, including targeted customer markets (e.g., foreign or domestic customers) and methods for soliciting clients.
- Determine whether the deposit broker is subject to regulatory oversight.
- Evaluate whether the deposit broker's BSA/AML/OFAC policies, procedures, and processes are adequate (e.g., ascertain whether the deposit broker performs sufficient CDD including CIP procedures).
- Determine whether the deposit broker screens clients for OFAC matches.
- Evaluate the adequacy of the deposit broker's BSA/AML/OFAC audits and ensure that they address compliance with applicable regulations and requirements.

Banks should take particular care in their oversight of deposit brokers who are not regulated entities and:

- Are unknown to the bank.
- Conduct business or obtain deposits primarily in other jurisdictions.
- Use unknown or hard-to-contact businesses and banks for references.
- Provide other services that may be suspect, such as creating shell corporations for foreign clients.
- Refuse to provide requested audit and due diligence information or insist on placing deposits before providing this information.
- Use technology that provides anonymity to customers.

Banks should also monitor existing deposit broker relationships for any significant changes in business strategies that may influence the broker's risk profile. As such, banks should periodically re-verify and update each deposit broker's profile to ensure an appropriate risk assessment.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Privately-Owned Automated Teller Machines

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with privately-owned automated teller machines (ATMs) and Independent Sales Organization (ISO) relationships, and management's ability to implement effective due diligence, monitoring, and reporting systems.

OVERVIEW

Privately-owned ATMs are particularly susceptible to money laundering and fraud. Operators of these ATMs are often included within the definition of an ISO.[120]

Privately-owned ATMs are typically found in convenience stores, bars, restaurants, grocery stores, or check cashing establishments. Some ISOs are large-scale operators, but many privately-owned ATMs are owned by the proprietors of the establishments in which they are located. Most dispense currency, but some dispense only a paper receipt (scrip) that the customer exchanges for currency or goods. Fees and surcharges for withdrawals, coupled with additional business generated by customer access to an ATM, make the operation of a privately-owned ATM profitable.

ISOs link their ATMs to an ATM transaction network. The ATM network routes transaction data to the customer's bank to debit the customer's account and ultimately credit the ISO's account, which could be located at a bank anywhere in the world. Payments to the ISO's account are typically made through the ACH system. Additional information on types of retail payment systems is available in the FFIEC *Information Technology Examination Handbook*.[121]

Sponsoring Bank

Some electronic funds transfers (EFTs) or point-of-sale (POS) networks require an ISO to be sponsored by a member of the network (sponsoring bank). The sponsoring bank and the ISO are subject to all network rules. The sponsoring bank is also charged with ensuring the ISO abides by all network rules. Therefore, the sponsoring bank should

[120] An ISO typically acts as an agent for merchants, including ATM owners, to process electronic transactions. In some cases, an ATM owner may act as its own ISO processor. Banks may engage the services of an ISO to solicit merchants and privately owned ATMs; however, in many situations, ISOs contract with merchants and ATM owners without the review and approval of the clearing bank.

[121] The FFIEC *Information Technology Examination Handbook* is available at www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

conduct proper due diligence on the ISO and maintain adequate documentation to ensure that the sponsored ISO complies with all network rules.

RISK FACTORS

Most states do not currently register, limit ownership, monitor, or examine privately-owned ATMs or their ISOs. While the provider of the ATM transaction network and the sponsoring bank should be conducting adequate due diligence on the ISO, actual practices may vary. Furthermore, the provider may not be aware of ATM or ISO ownership changes once an ATM contract has been established. As a result, many privately-owned ATMs have been involved in, or are susceptible to, money laundering schemes, identity theft, outright theft of the ATM currency, and fraud. Consequently, privately-owned ATMs and their ISOs pose increased risk and should be treated accordingly by banks doing business with them.

Some privately-owned ATMs are managed by a vault currency servicer that provides armored car currency delivery, replenishes the ATM with currency, and arranges for insurance against theft and damage. Many ISOs, however, manage and maintain their own machines, including the replenishment of currency. Banks may also provide currency to ISOs under a lending agreement, which exposes those banks to various risks, including reputation and credit risk.

Money laundering can occur through privately-owned ATMs when an ATM is replenished with illicit currency that is subsequently withdrawn by legitimate customers. This process results in ACH deposits to the ISO's account that appear as legitimate business transactions. Consequently, all three phases of money laundering (placement, layering, and integration) can occur simultaneously. Money launderers may also collude with merchants and previously legitimate ISOs to provide illicit currency to the ATMs at a discount.

RISK MITIGATION

Banks should implement appropriate polices, procedures, and processes to address risks with ISO relationships. At a minimum, the policies should include:

- Verification of an ISO's legitimacy through a review of corporate documentation, licenses, permits, contracts, or references.
- Review of public databases to determine the existence of issues with the ISO or principal owners.
- Understanding of the currency servicing arrangements for privately-owned ATMs and whether legitimate currency generation is sufficient to service machines.
- Documentation of the locations of privately-owned ATMs and determination of the ISO's target geographic market.
- Expected account activity, including currency withdrawals.

Because of these risks, due diligence on customers that are ISOs, beyond the minimum Customer Identification Program requirements is critical. Banks should also perform due diligence on ATM owners. This due diligence should:

- Verify the ATM owner's legitimacy through a review of corporate documentation, licenses, permits, contracts, or references, including the ATM transaction provider contract.
- Review public databases for information on the ATM owners.
- Obtain the addresses of all ATM locations, ascertain the types of businesses where they are located, and identify targeted demographics.
- Determine expected ATM activity levels, including currency withdrawals.
- Ascertain the sources of currency for the ATMs by reviewing copies of armored car contracts, lending arrangements, or any other documentation, as appropriate.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Nondeposit Investment Products

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with both networking and in-house nondeposit investment products (NDIP), and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

Nondeposit investment products (NDIP) include a wide array of investment products (e.g., securities, bonds, and fixed or variable annuities). Sales programs may also include cash management sweep accounts to retail and commercial clients; these programs are offered by the bank directly. Banks offer these investments to increase fee income and provide customers with additional products and services. The manner in which the NDIP relationship is structured and the methods in which the products are offered substantially affect the bank's BSA/AML risks and responsibilities.

Networking Arrangements

Banks typically enter into networking arrangements with securities broker/dealers to offer NDIP on bank premises. For BSA/AML purposes, under a networking arrangement, the customer is a customer of the broker/dealer, although the customer may also be a bank customer for other financial services. Bank examiners recognize that the U.S. Securities and Exchange Commission (SEC) is the primary regulator for NDIP offerings through broker/dealers, and the agencies will observe functional supervision requirements of the Gramm-Leach-Bliley Act.[122] Federal banking agencies are responsible for supervising NDIP activity conducted directly by the bank.

[122] Functional regulation limits the circumstances in which the federal banking agencies can directly examine or require reports from a bank affiliate or subsidiary whose primary regulator is the SEC, the Commodity Futures Trading Commission, or state issuance authorities. Federal banking agencies are generally limited from examining such an entity unless further information is needed to determine whether the banking affiliate or subsidiary poses a material risk to the bank, to determine compliance with a legal requirement under the federal banking agencies' jurisdiction, or to assess the bank's risk management system covering the functionally regulated activities. These standards require greater reliance on the functional regulator and better cooperation among regulators.

Different types of networking arrangements may include the following:

Co-branded Products – Co-branded products are offered by another company or financial services corporation[123] in co-sponsorship with the bank. For example, a financial services corporation tailors a mutual fund product for sale at a specific bank. The product is sold exclusively at that bank and bears the name of both the bank and the financial services corporation.

Because of this co-branded relationship, responsibility for BSA/AML compliance becomes complex. As these accounts are not under the sole control of the bank or financial entity, responsibilities for completing Customer Identification Program (CIP), customer due diligence (CDD), and suspicious activity monitoring and reporting can vary. The bank should fully understand each party's contractual responsibilities and ensure adequate control by all parties.

Dual-Employee Arrangements – In a dual-employee arrangement, the bank and the financial services corporation such as an insurance agency or a registered broker/dealer have a common (shared) employee. The shared employee may conduct banking business as well as sell NDIP, or sell NDIP full-time. Because of this dual-employee arrangement, the bank retains responsibility over NDIP activities. Even if contractual agreements establish the financial services corporation as being responsible for BSA/AML, the bank remains responsible and needs to ensure proper oversight and compliance with all regulatory requirements.[124]

Under some networking arrangements, registered securities sales representatives are dual employees of the bank and the broker/dealer. When the dual employee is providing investment products and services, the broker/dealer is responsible for monitoring the registered representative's compliance with applicable securities laws and regulations. When the dual employee is providing bank products or services, the bank has the responsibility for monitoring the employee's performance and compliance with BSA/AML.

Third-Party Arrangements – Third-party arrangements may involve leasing the bank's lobby space to a financial services corporation to sell NDIPs. In this case, the third-party must clearly differentiate itself from the bank. If the arrangement is appropriately implemented, third-party arrangements do not affect the BSA/AML compliance requirements of the bank. As a sound practice, the bank is encouraged to ascertain if the financial services provider has an adequate BSA/AML compliance program as part of its due diligence.

---

[123] A financial services corporation includes those entities offering NDIP, which may include investment firms, financial institutions, securities brokers/dealers, and insurance companies.

[124] If the bank uses the reliance provision under the CIP, responsibility for CIP shifts to the third-party provider. Refer to core overview section "Customer Identification Program" on page 30 for additional information.

In-House Sales and Proprietary Products

Unlike networking arrangements, the bank is fully responsible for in-house NDIP transactions completed on behalf of its customers, either with or without the benefit of an internal broker/dealer employee.[125] In addition, the bank may also offer its own proprietary NDIPs, which can be created and offered by the bank, its subsidiary, or an affiliate.

With in-house sales and proprietary products, the entire customer relationship and all BSA/AML risks may need to be managed by the bank, depending on how the products are sold. Unlike a networking arrangement, in which all or some of the responsibilities may be assumed by the third party broker/dealer with in-house sales and proprietary products, the bank should manage all of its in-house and proprietary NDIP sales not only on a department-wide basis, but on an enterprise-wide basis.

RISK FACTORS

BSA/AML risks arise because NDIP can involve complex legal arrangements, large dollar amounts, and the rapid movement of funds. NDIP portfolios managed and controlled directly by clients pose a greater money laundering risk than those managed by the bank or by the financial services provider. Sophisticated clients may create ownership structures to obscure the ultimate control and ownership of these investments. For example, customers can retain a certain level of anonymity by creating Private Investment Companies (PICs), offshore trusts, or other investment entities that hide the customer's ownership or beneficial interest.

RISK MITIGATION

Management should develop risk-based policies, procedures, and processes that enable the bank to identify unusual account relationships and circumstances, questionable assets and sources of funds, and other potential areas of risk (e.g., offshore accounts, agency accounts, and unidentified beneficiaries). Management should be alert to situations that need additional review or research.

---

[125] A bank shall not be considered to be a broker, nor need an employee registered as a broker/dealer, because the bank engages in any one or more of the activities under the conditions described:

- The bank effects customer transactions in municipal securities.
- The bank effects not more than 500 transactions in securities for its customers in any calendar year, and such transactions are not effected by an employee of the bank who is also an employee of a broker or dealer.
- The bank deals in commercial paper, banker's acceptances, commercial bills, or exempted securities.
- The bank effects customer transactions in identified banking products as defined in section 206 of the Gramm-Leach-Bliley Act.
- The bank effects customer transactions in certain stock purchase plans such as employee benefit plans, dividend reinvestment plans, and issuer plans.

Networking Arrangements

Before entering into a networking arrangement, banks should conduct an appropriate review of the broker/dealer. The review should include an assessment of the broker/dealer's financial status, management experience, National Association of Securities Dealers (NASD) status, reputation, and ability to fulfill its BSA/AML compliance responsibilities in regards to the bank's retail customers. Appropriate due diligence would include a determination that the broker/dealer has adequate policies, procedures, and processes in place to enable the broker/dealer to meet its legal obligations.

The bank should maintain documentation on its due diligence of the broker/dealer. Furthermore, detailed written contracts should address all facets of the networking arrangement, including the responsibilities of the broker/dealer and its registered representatives. The contract should specifically cover each party's responsibilities for compliance with BSA/AML regulations and laws and for suspicious activity monitoring and reporting.

A bank may also want to mitigate risk exposure by limiting certain investment products offered to its retail customers. Investment products such as PICs, offshore trusts, or offshore hedge funds may involve international funds transfers or offer customers ways to obscure ownership interests.

Bank management should make reasonable efforts to update due diligence information on the broker/dealer. Such efforts may include a periodic review of information on the broker/dealer's compliance with its BSA/AML responsibilities, verification of the broker/dealer's record in meeting testing requirements, and a review of consumer complaints. Bank management is also encouraged, when possible, to review BSA/AML reports generated by the broker/dealer. This review could include information on account openings, transactions, investment products sold, and suspicious activity monitoring and reporting.

In-House Sales and Proprietary Products

Bank management should assess risk on the basis of a variety of factors such as:

- The type of NDIP purchased and the size of the transactions.
- The types and frequency of transactions.
- The country of residence of the principals or beneficiaries, or the country of incorporation, or the source of funds.
- Accounts and transactions that are not usual and customary for the customer or for the bank.

For customers that management considers high risk for money laundering and terrorist financing, more stringent documentation, verification, and transaction monitoring procedures should be established. Enhanced due diligence may be appropriate in the following situations:

- The bank is entering into a relationship with a new customer.
- Nondiscretionary accounts have a large asset size or frequent transactions.
- The customer resides in a foreign jurisdiction.
- The customer is a PIC or other corporate structure established in a higher risk jurisdiction.
- Assets or transactions are atypical for the customer.
- Investment type, size, assets, or transactions are atypical for the bank.
- International funds transfers are conducted, particularly from offshore funding sources.
- The identities of the principals or beneficiaries in investments or relationships are unknown or cannot be easily determined.
- Politically exposed persons are parties to any investments or transactions.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Insurance

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with insurance sales, and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

Banks engage in insurance sales to increase their profitability, mainly through expanding and diversifying fee-based income. Insurance products are typically sold to bank customers through networking arrangements with an affiliate, an operating subsidiary, or other third party insurance providers. Banks are also interested in providing cross-selling opportunities for customers by expanding the insurance products they offer. The types of insurance products sold may include life, health, property and casualty, and fixed or variable annuities.

RISK FACTORS

Insurance products can be used to facilitate money laundering. For example, currency can be used to buy one or more life insurance policies, which may subsequently be quickly canceled by a policyholder (also known as "early surrender") for a penalty. The insurance company refunds the money to the purchaser in the form of a check. Non-life insurance policies can be used to launder money or finance terrorism through the submission by a policyholder of inflated or false claims to its insurance carrier, which if paid, would enable the insured to recover a part or all of the originally invested payments. Other ways insurance products can be used to launder money include:

- Borrowing against the cash surrender value of permanent life insurance policies.
- Selling units in investment-linked products (such as annuities).
- Using insurance proceeds from an early policy surrender to purchase other financial assets.
- Buying policies that allow the transfer of beneficial interests without the knowledge and consent of the issuer (e.g., secondhand endowment and bearer insurance policies).[126]

[126] Refer to the International Association of Insurance Supervisors' "Guidance Paper on Anti Money Laundering and Combating the Financing of Terrorism," October 2004 available at www.iaisweb.org.

RISK MITIGATION

To mitigate money laundering risks, the bank should adopt policies, procedures, and processes that include:

- The identification of high-risk accounts.
- Customer due diligence, including enhanced due diligence for higher risk accounts.
- Products, services, and target markets.
- Employee compensation and bonus arrangements that are related to sales.
- Monitoring, including the review of early policy terminations and the reporting of unusual and suspicious transactions (e.g., a single, large premium payment, a customer's purchase of a product that appears to fall outside the customer's normal range of financial transactions, early redemptions, multiple transactions, payments to apparently unrelated third parties, and collateralized loans).
- Recordkeeping.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Concentration Accounts

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with concentration accounts, and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

Concentration accounts are internal accounts established to facilitate the processing and settlement of multiple or individual customer transactions within the bank, usually on the same day. These accounts may also be known as special-use, omnibus, suspense, settlement, intraday, sweep, or collection accounts. Concentration accounts are frequently used to facilitate transactions for private banking, trust and custody accounts, funds transfers, and international affiliates.

RISK FACTORS

Money laundering risk can arise in concentration accounts if the customer-identifying information, such as name, transaction amount, and account number, is separated from the financial transaction. If separation occurs, the audit trail is lost, and accounts may be misused or administered improperly. Banks that use concentration accounts should implement adequate policies, procedures, and processes covering the operation and recordkeeping for these accounts. Policies should establish guidelines to identify, measure, monitor, and control the risks.

RISK MITIGATION

Because of the risks involved, management should be familiar with the nature of their customers' business and with the transactions flowing through the bank's concentration accounts. Additionally, the monitoring of concentration account transactions is necessary to identify and report unusual or suspicious transactions.

Internal controls are necessary to ensure that processed transactions include the identifying customer information. Retaining complete information is crucial for compliance with regulatory requirements as well as ensuring adequate transaction monitoring. Adequate internal controls may include:

- Maintaining a comprehensive system that identifies, bank-wide, the general ledger accounts used as concentration accounts, as well as the departments and individuals authorized to use those accounts.

- Requiring dual signatures on general ledger tickets.
- Prohibiting direct customer access to concentration accounts.
- Capturing customer transactions in the customer's account statements.
- Prohibiting customer's knowledge of concentration accounts or their ability to direct employees to conduct transactions through the accounts.
- Retaining appropriate transaction and customer identifying information.
- Frequent reconciling of the accounts by an individual who is independent from the transactions.
- Establishing timely discrepancy resolution process.
- Identifying recurring customer names.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Lending Activities

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with lending activities, and management's ability to implement effective due diligence, monitoring, and reporting systems.

OVERVIEW

Lending activities include, but are not limited to, real estate, trade finance,[127] cash-secured, credit card, consumer, commercial, and agricultural. Lending activities can include multiple parties (e.g., guarantors, signatories, principals, or loan participants).

RISK FACTORS

The involvement of multiple parties may increase the risk of money laundering or terrorist financing when the source and use of the funds are not transparent. This lack of transparency can create opportunities in any of the three stages of money laundering or terrorist financing schemes. These schemes could include the following:

- To secure a loan, an individual purchases a certificate of deposit with illicit funds.
- Loans are made for an ambiguous or illegitimate purpose.
- Loans are made for, or are paid for, a third party.
- The bank or the customer attempts to sever the paper trail between the borrower and the illicit funds.
- Loans are extended to persons located outside the United States, particularly to those in high-risk jurisdictions and geographic locations. Loans may also involve collateral located outside the United States.

RISK MITIGATION

All loans are considered to be accounts for purposes of the Customer Identification Program (CIP) regulations. For loans that may pose a higher risk for money laundering and terrorist financing, including the loans listed above, the bank should complete due diligence on related account parties (i.e., guarantors, signatories, or principals). Due diligence beyond what is required for a particular lending activity will vary according to the BSA/AML risks present but could include performing reference checks, obtaining credit references, verifying the source of collateral, and obtaining tax or financial statements on the borrower and any or all of the various parties involved in the loan.

[127] Refer to the expanded overview section "Trade Finance Activities" on page 140.

The bank should have policies, procedures, and processes to monitor, identify, and report unusual and suspicious activities. The sophistication of the systems used to monitor lending account activity should conform to the size and complexity of the bank's lending business. For example, the bank can review loan reports such as early payoffs, past dues, fraud, or cash-secured.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Trade Finance Activities

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with trade finance activities, and management's ability to implement effective due diligence, monitoring, and reporting systems.

OVERVIEW

Trade finance typically involves short-term financing to facilitate the import and export of goods. These operations can involve the transmission of funds to enable the transaction (e.g., letter of credit), or may instead only involve the payment of funds if the commercial terms of the transactions are not met (e.g., guarantees or standby letters of credit). In both cases, a bank's involvement in trade finance minimizes payment risk to importers and exporters. The nature of trade finance activities requires the active involvement of multiple parties on both sides of the transaction. In addition to the basic exporter/importer relationship at the center of any particular trade activity, relationships may exist between the exporter and the suppliers and between the importer and the customers. Both the exporter and importer may also have other banking relationships. Furthermore, many other intermediary financial and nonfinancial institutions may provide conduits and services to expedite the underlying documents and payment flows associated with trade transactions.

As an example, in a letter of credit arrangement, a bank can serve as the issuing bank, allowing its customer (the buyer) to purchase goods locally or internationally, or the bank can act as an advising bank, enabling their customer (the exporter) to sell their goods locally or internationally. The relationship between the two banks will vary, and in some cases it may be similar to a correspondent relationship.

RISK FACTORS

The involvement of multiple parties can make the process of due diligence more difficult. As such, the bank should conduct a thorough review and fully understand all trade finance documentation and related values. Since the trade finance business can be more document-based than other areas of banking, it can be susceptible to documentary fraud, which can be linked to money laundering, terrorist financing, or the circumvention of OFAC sanctions or other prohibitions. Banks should be alert to transactions involving higher risk goods (e.g., trade in weapons or nuclear equipment).

Furthermore, goods may be over- or undervalued in an effort to evade AML or customs regulations. For example, an importer may pay a large sum of money from the proceeds

of an illegal activity for goods which are essentially worthless and are subsequently discarded. Trade documents, such as invoices, are fraudulently altered to hide the scheme. The illegal proceeds transferred in the trade transaction are then used to buy expensive assets such as gems, fine art, luxury cars, airplanes, or boats which can be exported to any country.

Issuing banks maintain foreign correspondent banking relationships to facilitate international trade. Banks must comply with OFAC sanctions by ensuring that transactions receive appropriate OFAC licensing in advance of funding.

RISK MITIGATION

Banks should obtain sufficient customer due diligence on prospective import/export customers before establishing the account or credit relationship. This due diligence should involve gathering information on principals and beneficiaries, as appropriate, including their identities, nature of the customer's business, and source of wealth and funds. With regard to letters of credit, the advising or confirming bank may have a correspondent banking relationship with the issuing bank to facilitate trade due to the frequency of transactions in which both parties are involved. Alternatively, it could be a one-time transaction, and the bank would not have a formal relationship with the issuing bank.

Policies, procedures, and processes should require a thorough review of all applicable trade finance documentation to enable the bank to monitor and report unusual and suspicious activity. The sophistication of the reporting systems and management information systems should be commensurate with the size and complexity of the bank's trade finance activities. In addition to financial transaction monitoring and OFAC filtering, the bank's review should detect:

- Shipping items that are inconsistent with the nature of the customer's business.
- Customers conducting business with jurisdictions designated as high risk.
- Customers conducting transactions with businesses involved in higher-risk activities (i.e., weapons dealers, nuclear materials, or chemical).
- Goods entering or exiting ports of non-cooperative countries.
- Irregular pricing of goods.
- Excessively amended letters of credit.
- Transactions designed to evade home country legal restrictions.

With regard to monitoring for irregular pricing of goods, the examiner should verify that the bank reviews the documentation related to the transaction to determine whether the prices are generally consistent with market prices. Bank employees engaged in the review of pricing should be aware of market prices on the basis of general knowledge.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Private Banking

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with private banking activities, and management's ability to implement effective due diligence, monitoring, and reporting systems. This section expands the core review of the statutory and regulatory requirements of private banking in order to provide a broader assessment of the AML risks associated with this activity.

OVERVIEW

Private banking activities are generally defined as providing personalized services to high net worth customers (e.g., estate planning, financial advice, lending, investment management, bill paying, mail forwarding, and maintenance of a residence). Private banking has become an increasingly important business line for large and diverse banking organizations and a source of enhanced fee income.

U.S. banks may manage private banking relationships for both domestic and international customers. Typically, thresholds of private banking service are based on the amount of assets under management and on the need for specific products or services (e.g., real estate management, closely held company oversight, money management). The fees charged are ordinarily based on asset thresholds and the use of specific products and services.

Private banking arrangements are typically structured to have a central point of contact (i.e., relationship manager) that acts as a liaison between the client and the bank and facilitates the client's use of the bank's financial services and products. Appendix N ("Private Banking – Common Structure") provides an example of a typical private banking structure and illustrates the relationship between the client and the relationship manager. Typical products and services offered in a private banking relationship include:

- Cash management (e.g., checking accounts, overdraft privileges, cash sweeps, and bill-paying services).
- Funds transfer.
- Asset management (e.g., trust, investment advisory, investment management, and custodial and brokerage services).[128]
- The facilitation of offshore entities (e.g., Private Investment Companies (PICs), international business corporations (IBCs), and trusts).[129]

[128] Refer to the expanded procedures section on "Trust and Asset Management Services" on page 255.

- Lending services (e.g., mortgage loans, credit cards, personal loans, and letters of credit).
- Financial planning services including tax and estate planning.
- Custody services.
- Other services as requested (e.g., mail services).

Privacy and confidentiality are important elements of private banking relationships. Although customers may choose private banking services simply to manage their assets, they may also seek a confidential, safe, and legal haven for their capital. When acting as a fiduciary, banks have statutory, contractual, and ethical obligations to uphold.

RISK FACTORS

Private banking services can be vulnerable to money laundering schemes and past money laundering prosecutions have demonstrated that vulnerability. The 1999 Permanent Subcommittee on Investigations "Private Banking and Money Laundering: A Case Study of Opportunities and Vulnerabilities"[130] outlined, in part, the following vulnerabilities to money laundering:

- Private bankers as client advocates.
- Powerful clients including politically exposed persons, industrialists, and entertainers.
- A culture of confidentiality and the use of secrecy jurisdictions or shell corporations.[131]
- A private banking culture of lax internal controls.
- The competitive nature of the business.
- Significant profit potential for the bank.

Risk of Shell Corporations

A shell corporation exists on paper but transacts either no business or minimal business. They are typically used for legitimate investment purposes and can be incorporated in the United States (e.g., Delaware) or offshore as IBCs. The risks associated with shell corporations include poor or non-existent records (e.g., ownership documentation), inadequate government oversight, the lack of public disclosures, and the large range of permissible activities that may be allowed in the incorporating jurisdiction. Some shell corporations issue bearer shares. Because of the high degree of money laundering and terrorist financing risks associated with bearer shares, banks should maintain control of bearer shares or entrust them with a reliable independent third party. Because many shell

[129] Refer to the expanded procedures section "Corporate Entities (Domestic and Foreign)" on page 269.

[130] Refer to http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_senate_hearings&docid=f:61699.wais.

[131] A shell corporation is defined as a corporation without a physical presence in any country.

corporations allow an individual to be shielded by the shell corporation's legal identity, due diligence may be difficult.

RISK MITIGATION

Effective policies, procedures, and processes can help protect banks from becoming conduits for or victims of money laundering, terrorist financing, and other financial crimes that are perpetrated through private banking relationships. Additional information relating to risk assessments and due diligence is contained in the core overview section "Private Banking Due Diligence Program (Non-U.S. Persons)" on page 75. Ultimately, illicit activities through the private banking unit could result in significant financial costs and reputational risk to the bank if management oversight is lax. Financial impacts could include regulatory sanctions and fines, litigation expenses, the loss of business, reduced liquidity, asset seizures and freezes, loan losses, and remediation expenses.

Customer Risk Assessment

Banks should assess the risks its private banking activities pose on the basis of the scope of operations and the complexity of the bank's customer relationships. Management should establish a risk profile for each customer to be used in prioritizing oversight resources and for ongoing monitoring of relationship activities. The following factors should be considered when identifying risk characteristics of private banking customers:

- Nature of the customer and the customer's business. The source of the customer's wealth, the nature of the customer's business, and the extent to which the customer's business history presents an increased risk for money laundering and terrorist financing. This factor should be considered for private banking accounts opened for PEPs.[132]
- Purpose and activity. The size, purpose, types of accounts, products, and services involved in the relationship, and the anticipated activity of the account.
- Relationship. The nature and duration of the bank's relationship (including relationships with affiliates) with the private banking customer.
- Customer's corporate structure. Type of corporate structure (e.g., IBCs, shell corporations (domestic or foreign), or PICs).
- Location and jurisdiction. The location of the private banking customer's domicile and business (domestic or foreign). The review should consider the extent to which the relevant jurisdiction is internationally recognized as presenting a greater risk for money laundering or, conversely, is considered to have robust AML standards.
- Public information. Information known or reasonably available to the bank about the private banking customer. The scope and depth of this review should depend on the nature of this relationship and the risks involved.

[132] Refer to the core overview section "Private Banking Due Diligence Program (Non-U.S. Persons)" on page 75 and to the expanded overview section "Politically Exposed Persons" on page 153.

Customer Due Diligence

Customer due diligence (CDD) is essential when establishing any customer relationship, and it is critical for private banking clients.[133] Banks should take reasonable steps to establish the identity of their private banking clients and, as appropriate, the beneficial owners of accounts. Adequate due diligence should vary based on the risk factors identified previously. Policies, procedures, and processes should define acceptable CDD for different types of products (e.g., PICs), services, and accountholders.

Under the Customer Identification Program (CIP), banks must verify customer information for private banking accounts; this minimum requirement, however, does not extend to beneficiaries of those accounts. For purposes of the CIP, a bank is not required to look through accounts maintained for non-individuals (e.g., private banking accounts opened for a PIC) to verify the identities of beneficiaries. Instead, the bank is only required to verify the identity of the named accountholder. A bank may, however, need to take additional steps to verify the identity of a customer that is not an individual (e.g., a PIC) by obtaining information about individuals with ownership or control over the account in order to verify the customer's identity[134] and to determine whether the account is maintained for non-U.S. persons.[135]

Before opening accounts, banks should collect the following information from the private banking clients:

- The purpose of the account.
- The type of products and services to be used.
- Anticipated account activity.
- A description and history of the source of the client's wealth.
- The client's estimated net worth, including financial statements.
- The current source of funds for the account.
- The references or other information to confirm the reputation of the client.

Board of Directors and Senior Management Oversight

The board of directors' and senior managements' active oversight of private banking activities and the creation of an appropriate corporate oversight culture are crucial elements of a sound risk management and control environment. The purpose and objectives of the organization's private banking activities should be clearly identified and communicated by the board and senior management. Well-developed goals and objectives should describe the target client base in terms of minimum net worth,

---

[133] Due diligence policies, procedures, and processes are required for private banking accounts for non-U.S. persons by section 312 of the Patriot Act. Refer to the core overview section "Private Banking Due Diligence Program (Non-U.S. Persons)" on page 75.

[134] See 31 CFR 103.121(b)(2)(ii)(C).

[135] See the "Private Banking Due Diligence Program (Non-U.S. Persons)" core procedures on page 202.

investable assets, and types of products and services sought. Goals and objectives should also specifically describe the types of clients the bank will and will not accept and should establish appropriate levels of authorization for new-client acceptance. Board and senior management should also be actively involved in establishing control and risk management goals for private banking activities, including effective audit and compliance reviews. Each bank should ensure that its policies, procedures, and processes for conducting private banking activities are evaluated and updated regularly and ensure that roles, responsibilities, and accountability are clearly delineated.

Employee compensation plans are often based on the number of new accounts established or on an increase in managed assets. Board and senior management should ensure that compensation plans do not create incentives for employees to ignore appropriate due diligence and account opening procedures or possible suspicious activity relating to the account. Procedures that require various levels of approval for accepting new private banking accounts can minimize such opportunities.

Given the sensitive nature of private banking and the potential liability associated with it, banks should thoroughly investigate the background of newly hired private banking relationship managers and should establish ongoing monitoring of their personal financial condition to detect any indications of inappropriate activities. However, when private banking relationship managers change employers, their customers often move with them. Banks bear the same potential liability for the existing customers of newly hired officers as they do for any new private banking relationship. Therefore, those accounts should be promptly reviewed using the bank's procedures for establishing new account relationships.

Management information systems (MIS) and reports are also important in effectively supervising and managing private banking relationships and risks. Board and senior management should review relationship manager compensation reports, budget or target comparison reports, and applicable risk management reports. Private banker MIS reports should enable the relationship manager to view and manage the whole client and any related client relationships.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Trust and Asset Management Services

OBJECTIVE

Assess the adequacy of the bank's policies, procedures, processes, and systems to manage the risks associated with trust and asset management[136] services, and management's ability to implement effective due diligence, monitoring, and reporting systems.

OVERVIEW

Trust[137] accounts are generally defined as a legal arrangement in which one party (the trustor or grantor) transfers ownership of assets to a person or bank (the trustee) to be held or used for the benefit of others. These arrangements include the broad categories of court-supervised accounts (i.e., executorships and guardianships), personal trusts (i.e., living trusts, trusts established under a will, and charitable trusts), and corporate trusts (i.e., bond trusteeships).

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,[138] and safekeeping relationships. Agency products and services may be offered in a traditional trust department or through other bank departments.

CUSTOMER IDENTIFICATION PROGRAM

Customer Identification Program (CIP) rules, which became effective October 1, 2003, apply to substantially all bank accounts opened after that date. The CIP rule defines an "account" to include cash management, safekeeping, custodian, and trust relationships. However, the CIP rule excludes employee benefit accounts established pursuant to the Employee Retirement Income Security Act of 1974 (ERISA).

---

[136] Asset management accounts can be trust or agency accounts managed by the bank.

[137] The OCC and OTS use the broader term "fiduciary capacity" instead of "trust." Fiduciary capacity includes 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 a 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 (12 CFR 9.2(e) and 12 CFR 550.30).

[138] For purposes of national banks and OTS-regulated savings associations, certain investment management activities, such as providing investment advice for a fee, are "fiduciary" in nature.

For purposes of the CIP, the bank is not required to search the trust, escrow, or similar accounts to verify the identities of beneficiaries but instead is only required to verify the identity of the named accountholder (the trust). In the case of a trust account, the customer is the trust whether or not the bank is the trustee for the trust. However, the CIP rule also provides that, based on the bank's risk assessment of a new account opened by a customer that is not an individual, the bank may need "to obtain information about" individuals with authority or control over such an account, including signatories, in order to verify the customer's identity.[139] For example, in certain circumstances involving revocable trusts, the bank may need to gather information about the settlor, grantor, trustee, or other persons with the authority to direct the trustee, and who thus have authority or control over the account, in order to establish the true identity of the customer.

In the case of an escrow account, if a bank establishes an account in the name of a third party, such as a real estate agent, who is acting as escrow agent, then the bank's customer is the escrow agent. If the bank is the escrow agent, then the person who establishes the account is the bank's customer. For example, if the purchaser of real estate directly opens an escrow account and deposits funds to be paid to the seller upon satisfaction of specified conditions, the bank's customer will be the purchaser. Further, if a company in formation establishes an escrow account for investors to deposit their subscriptions pending receipt of a required minimum amount, the bank's customer will be the company in formation (or if not yet a legal entity, the person opening the account on its behalf). However, the CIP rule also provides that, based on the bank's risk assessment of a new account opened by a customer that is not an individual, the bank may need "to obtain information about" individuals with authority or control over such an account, including signatories, in order to verify the customer's identity.[140]

RISK FACTORS

Trust and asset management accounts, including agency relationships, present BSA/AML concerns similar to those of deposit taking, lending, and other traditional banking activities. Concerns are primarily due to the unique relationship structures involved when the bank handles trust and agency activities such as:

- 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.

[139] Refer to 31 CFR 103.121(b)(2)(ii)(C).

[140] Id.

- Transfer agent accounts.
- Other related business lines.[141]

As in any account relationship, money laundering risk may arise from trust and asset management activities. When misused, trust and asset management accounts can conceal the sources and uses of funds, as well as the identity of beneficial and legal owners. Customers and account beneficiaries may try to remain anonymous in order to move illicit funds or avoid scrutiny. For example, customers may seek a certain level of anonymity by creating Private Investment Companies (PICs), offshore trusts, or other investment entities that hide the true ownership or beneficial interest of the trust.

RISK MITIGATION

Management should develop policies, procedures, and processes that enable the bank to identify unusual account relationships and circumstances, questionable assets and sources of assets, and other potential areas of risk (e.g., offshore accounts, PICs, asset protection trusts (APTs),[142] agency accounts, and unidentified beneficiaries). While the majority of traditional trust and asset management accounts will not need enhanced due diligence, management should be alert to those situations that need additional review or research.

Customer Comparison Against Lists

The bank must be capable of maintaining required CIP information and completing the required one-time check of trust account names against section 314(a) search requests. The bank should also be able to identify customers who may be politically exposed persons (PEPs), doing business with or located in jurisdictions designated as "special money laundering concern" under section 311 of the Patriot Act, or match OFAC lists.[143] As a sound practice, the bank should also determine the identity of other parties that may have control over the account, such as grantors or co-trustees.

Refer to the core overview section "Information Sharing" for additional guidance on information sharing procedures, for the 314(a) search request, refer to page 55, and the expanded overview section "Politically Exposed Persons" for additional information, page 153.

---

[141] Refer to the appropriate federal banking agency's manuals for specific definitions of these products.

[142] APTs are a special form of irrevocable trust, usually created (settled) offshore for the principal purposes 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.

[143] Management and examiners should be aware that OFAC list matching is not a BSA requirement. However, since trust systems are typically separate and distinct from bank systems, verification of these checks on the bank system is not sufficient to ensure that these checks are also completed in the trust and asset management department.

Circumstances Warranting Enhanced Due Diligence

Management should assess account risk on the basis of a variety of factors which may include:

- The type of trust or agency account and its size.
- The types and frequency of transactions.
- The country of residence of the principals or beneficiaries, or the country where established, or source of funds.
- Accounts and transactions that are not usual and customary for the customer or for the bank.

Stringent documentation, verification, and transaction monitoring procedures should be established for accounts that management considers as high risk. Typically, employee benefit accounts and court-supervised accounts are among the lowest BSA/AML risks.

The following are examples of situations in which enhanced due diligence may be appropriate:

- The bank is entering into a relationship with a new customer.
- The account principals or beneficiaries reside in a foreign jurisdiction, or the trust or its funding mechanisms are established offshore.
- Assets or transactions are atypical for the type and character of the customer.
- The account type, size, assets, or transactions are atypical for the bank.
- International funds transfers are conducted, particularly through offshore funding sources.
- Accounts are funded with easily transportable assets such as gemstones, precious metals, coins, artwork, rare stamps, or negotiable instruments.
- Accounts or relationships are maintained in which the identities of the principals, or beneficiaries, or sources of funds are unknown or cannot easily be determined.
- Accounts benefit charitable organizations or other non-governmental organizations (NGOs) that may be used as a conduit for illegal activities.[144]
- Interest on lawyers' trust accounts (IOLTA) holding and processing significant dollar amounts.
- Account assets which include PICs.
- PEPs are parties to any accounts or transactions.

[144] Refer to the expanded overview section "Non-Governmental Organizations and Charities," page 162 for further guidance.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Nonresident Aliens and Foreign Individuals

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with transactions involving accounts held by nonresident aliens (NRAs) and foreign individuals, and management's ability to implement effective due diligence, monitoring, and reporting systems.

OVERVIEW

Foreign individuals maintaining relationships with U.S. banks can be divided into two categories: resident aliens and nonresident aliens. For definitional purposes, an NRA is a non-U.S. citizen who: (i) is not a lawful permanent resident of the United States during the calendar year and who does not meet the substantial presence test,[145] or (ii) has not been issued an alien registration receipt card, also known as a green card. The Internal Revenue Service determines the tax liabilities of a foreign person and officially defines the person as a "resident" or "nonresident."

Although NRAs are not permanent residents, they may have a legitimate need to establish an account relationship with a U.S. bank. NRAs use bank products and services for asset preservation (e.g., mitigating losses due to exchange rates), business expansion, and investments. The amount of NRA deposits in the U.S. banking system has been estimated to range from hundreds of billions of dollars to about $1 trillion. Even at the low end of the range, the magnitude is substantial, both in terms of the U.S. banking system and the economy.

RISK FACTORS

Banks may find it more difficult to verify and authenticate an NRA accountholder's identification, source of funds, and source of wealth, which may result in BSA/AML risks. The NRA's home country may also heighten the account risk, depending on the secrecy laws of that country. Since the NRA is expected to reside outside of the United

[145] A foreign national is a resident alien if the individual is physically present in the United States for at least 31 days in the current calendar year and present 183 days or more based on counting: all days present during the current year, plus 1/3 of the days present in the preceding year, plus 1/6 of the days present in the second preceding year. Certain days of presence are disregarded, such as (i) days spent in the United States for a medical condition that developed while the foreign national was present in the United States and unable to leave, (ii) days regular commuters spend traveling to or from Canada or Mexico, (iii) a day of less than 24 hours spent while in transit between two locations outside the United States., and (iv) days when the foreign national was an exempt individual. The individual is considered a resident alien for federal income and employment tax purposes from the first day of physical presence in the United States in the year that the test is satisfied. Refer to the Internal Revenue Service web site: www.irs.gov.

States, funds transfers or the use of foreign automated teller machines (ATMs) may be more frequent. The BSA/AML risk may be further heightened if the NRA is a politically exposed person (PEP). Refer to the expanded procedures section "Politically Exposed Persons," on page 259 for further information.

RISK MITIGATION

Banks should establish policies, procedures, and processes that provide for sound due diligence and verification practices, adequate risk assessment of NRA accounts, and ongoing monitoring and reporting of unusual or suspicious activities. The following factors are to be considered when determining the risk level of an NRA account:

- The accountholder's home country.
- The types of products and services used.
- Forms of identification.
- The source of wealth and funds.
- Unusual account activity.

NRA customers may request W-8 status for U.S. tax withholding. In such cases, the NRA customer completes a W-8 form, which attests to the customer's foreign and U.S. tax-exempt status. While it is an Internal Revenue Service (IRS) form, a W-8 is not sent to the IRS, but is maintained on file at the bank to support the lack of any tax withholding from earnings.[146]

The bank's Customer Identification Program (CIP) should detail the identification requirements for opening an account for an NRA. The program should include the use of documentary and nondocumentary methods to verify a customer. In addition, the Patriot Act amended the BSA to require special due diligence for private banking accounts for non-U.S. persons, including those held for PEPs or senior foreign political figures.

[146] Additional information can be found at www.irs.gov/formspubs.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Politically Exposed Persons

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with transactions involving politically exposed persons (PEPs), and management's ability to implement effective due diligence, monitoring, and reporting systems.

OVERVIEW

For the purposes of this manual, a PEP is a person identified in the course of normal account opening, maintenance or compliance procedures to be a "senior foreign political figure," any member of a senior foreign political figure's "immediate family," and any "close associate" of a senior foreign political figure.

Interagency guidance issued in January 2001, offers banks resources that can help them to determine whether an individual is a senior foreign political figure, an immediate family member, or a close associate.[147] According to this guidance:

- A "senior foreign political figure" is a 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 corporation. In addition, a senior foreign political figure includes any corporation, business or other entity that has been formed by, or for the benefit of, a senior foreign political figure.
- The "immediate family" of a senior foreign political figure typically includes the figure's parents, siblings, spouse, children, and in-laws.
- A "close associate" of a senior foreign political figure is a person who is widely and publicly known to maintain an unusually close relationship with the senior foreign political figure, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the senior foreign political figure. While close associates are more difficult for banks to identify, they include individuals who due to the nature of their relationship with the PEP, are in a position to conduct significant domestic and international financial transactions on behalf of the PEP.

[147] "Guidance on Enhanced Scrutiny for Transactions that may Involve the Proceeds for Foreign Official Corruption" issued 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, January 2001.

RISK FACTORS

In high-profile cases over the past few years, PEPs have used banks as conduits for their illegal activities, including corruption, bribery, and money laundering. Banks that conduct business with dishonest PEPs face substantial reputation risk, enhanced scrutiny, and possible supervisory action.

RISK MITIGATION

Banks should obtain comprehensive due diligence information on PEPs and establish policies, procedures, and processes that provide for greater scrutiny and monitoring of all PEP accounts. Account opening procedures are critical, as this is the prime opportunity for the bank to gather the following information on a PEP:

- The identity of the accountholder and beneficial owner.
- The source of funds.
- The source of wealth.
- Information on immediate family members or close associates having transaction authority over the account.
- The purpose of the account and the expected volume and nature of account activity.

PEP accounts are not limited to large or internationally-focused banks. A PEP can open an account at any bank, regardless of its size or location. Banks should specifically identify PEP accounts and assess the degree of risks involved, which will vary. Senior management should be involved in the decision to accept a PEP account. If management determines after-the-fact that an account is a PEP account, they should evaluate the risks and take appropriate steps. Ongoing monitoring of PEP accounts is critical to ensuring that the accounts are being used as anticipated. The BSA requires due diligence for private banking accounts maintained for certain PEPs.[148]

[148] Refer to the core overview section "Private Banking Due Diligence Program (Non-U.S. Persons)," on page 75.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Embassy and Foreign Consulate Accounts

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with transactions involving embassy and foreign consulate accounts, and management's ability to implement effective due diligence, monitoring, and reporting systems.

OVERVIEW

Embassies contain the offices of the foreign ambassador, the diplomatic representative, and their staff. The embassy, led by the ambassador, is a foreign government's official representation in the United States (or other country). Foreign consulate offices act as branches of the embassy and perform various administrative and governmental functions (e.g., issuing visas and handling immigration matters). Foreign consulate offices are typically located in major metropolitan areas. In addition, foreign ambassadors' diplomatic representatives, their families, and their associates may be considered politically exposed persons (PEPs) in certain circumstances.[149]

Embassies and foreign consulates in the United States require access to the banking system to meet many of their day-to-day financial responsibilities. Such services can range from account relationships for operational expenses (e.g., payroll, rent, and utilities) to inter-and intragovernmental transactions (e.g., commercial and military purchases). In addition to official embassy accounts, some banks provide ancillary services or accounts to embassy staff, families, and current or prior foreign government officials. Each of these relationships poses different levels of risk to the bank.

Embassy accounts, including those accounts for a specific embassy office such as a cultural or education ministry, a defense attaché or ministry, or any other account, should have a specific operating purpose stating the official function of the foreign government office. Consistent with established practices for business relationships, these embassy accounts should have written authorization by the foreign government.

RISK FACTORS

To provide embassy and foreign consulate services, a U.S. bank may need to maintain a foreign correspondent relationship with the embassy's or foreign consulate's bank. Banks conducting business with foreign embassies or consulates should assess and understand the potential risks of these accounts and should develop appropriate policies,

[149] Refer to the expanded overview section "Politically Exposed Persons" for additional information on page 153.

procedures, and processes. Embassy or foreign consulate accounts may pose a higher risk in the following circumstances:

- Accounts are from countries that have been designated as high risk.
- Substantial currency transactions take place in the accounts.
- Account activity is not consistent with the purpose of the account (e.g., pouch activity or payable upon proper identification transactions).
- Accounts directly fund personal expenses of foreign nationals, including but not limited to expenses for college students.
- Official embassy business is conducted through personal accounts.

RISK MITIGATION

Banks should obtain comprehensive due diligence information on embassy and foreign consulate account relationships. For private banking accounts for non-U.S. persons specifically, banks must obtain due diligence information as required by 31 CFR 103.181.[150] The bank's due diligence related to embassy and foreign consulate account relationships should be commensurate with the risk levels presented. In addition, banks are expected to establish policies, procedures, and processes that provide for greater scrutiny and monitoring of all embassy and foreign consulate account relationships. Management should fully understand the purpose of the account and the expected volume and nature of account activity. Ongoing monitoring of embassy and foreign consulate account relationships is critical to ensuring that the account relationships are being used as anticipated.

[150] Refer to core section overview "Private Banking Due Diligence Program (Non-U.S. Persons)," on page 75 for additional guidance.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Non-Bank Financial Institutions

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with accounts of non-bank financial institutions (NBFIs), and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

NBFIs are broadly defined as institutions that offer financial services. The Patriot Act has defined a variety of entities as financial institutions.[151] Common examples of NBFIs include, but are not limited to:

- Casinos and card clubs.
- Securities and commodities firms (e.g., brokers/dealers, investment advisers, mutual funds, hedge funds, or commodity traders).
- Money services businesses (e.g., certain check cashers; currency dealers or exchangers; issuers, sellers, or redeemers of traveler's checks, money orders, or stored value cards; money transmitters).
- Other financial institutions (e.g., dealers in precious metals, stones, or jewels; pawnbrokers; loan or finance companies).

Some NBFIs are currently required to develop an AML program, comply with the reporting and recordkeeping requirements of the BSA, and report suspicious activity, as are required by banks. NBFIs typically require a bank account in order to operate. Although NBFIs maintain operating accounts at banks, the BSA does not require, and neither FinCEN nor the federal banking agencies expect, banks to serve as the *de facto* regulator of any NBFI industry or individual NBFI customer. Furthermore, while banks are expected to manage risk associated with all accounts, including NBFI accounts, banks will not be held responsible for their customers' compliance with the BSA and other applicable federal and state laws and regulations.

Guidance on Providing Banking Services to Money Services Businesses

FinCEN and the federal banking agencies issued interpretive guidance on April 26, 2005, to clarify the BSA requirements and supervisory expectations as applied to accounts opened or maintained for money services businesses.[152] The guidance sets forth the

[151] Refer to Appendix D "Statutory Definition of Financial Institution."

[152] Refer to "Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States," available at www.fincen.gov.

following minimum due diligence expectations for banks when opening or maintaining accounts for money services businesses:

- Confirm FinCEN registration, if required.
- Confirm state licensing, if applicable.
- Confirm agent status, if applicable.
- Conduct a risk assessment to determine the level of risk associated with each account and whether further due diligence is required.

While several specific components of the guidance are unique to money services businesses (such as expectations to confirm registration with FinCEN), the fundamental core of the guidance – that banks should apply the requirements of the BSA on a risk-assessed basis – is applicable to accounts held for all NBFI customers, as described in the risk mitigation section below.

RISK FACTORS

NBFI industries are extremely diverse, ranging from large multi-national corporations to small, independent businesses that offer financial services only as an ancillary component to its primary business (e.g., grocery store that offers check cashing). The range of products and services offered, and the customer bases served by NBFIs, are equally diverse.

Banks that maintain account relationships with NBFIs may be exposed to a higher risk for potential money laundering activities because many NBFIs:

- Lack ongoing customer relationships and require minimal or no identification by customers.
- Maintain limited or inconsistent recordkeeping on customers and transactions.
- Engage in frequent currency transactions.
- Are subject to varying levels of regulatory requirements and oversight.
- Can quickly change their product mix or location and quickly enter or exit an operation.
- Sometimes operate without proper registration or licensing.

RISK MITIGATION

Banks that maintain account relationships with NBFIs should develop policies, procedures, and processes to:

- Identify NBFIs relationships.
- Assess the potential risks posed by the NBFI relationships.
- Conduct adequate and ongoing due diligence on the NBFI relationships when necessary.

- Ensure NBFI relationships are appropriately considered within the bank's suspicious activity monitoring and reporting systems.

Risk Assessment Factors

Banks should assess the risks posed by their NBFI customers and direct their resources most appropriately to those accounts that pose a more significant money laundering risk. The following factors may be used to help identify the relative risks within the NBFI portfolio. Nevertheless, management should weigh and evaluate each risk assessment factor to arrive at a risk determination for each customer and to prioritize oversight resources. Relevant risk factors include:

- Types of products and services offered by the NBFI.
- Locations and markets served by the NBFI.
- Anticipated account activity.
- Purpose of the account.

A bank's due diligence should be commensurate with the level of risk of the NBFI customer identified through its risk assessment. If a bank's risk assessment indicates potential for a heightened risk of money laundering or terrorist financing, it will be expected to conduct further due diligence in a manner commensurate with the heightened risk.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Professional Service Providers

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with professional service provider relationships, and management's ability to implement effective due diligence, monitoring, and reporting systems.

OVERVIEW

A professional service provider acts as an intermediary between its client and the bank. Professional service providers include lawyers, accountants, investment brokers, and other third parties that act as financial liaisons for their clients. These providers may conduct financial dealings for their clients. For example, an attorney may perform services for a client, or arrange for services to be performed on the client's behalf, such as: settlement of real estate transactions, asset transfers, management of client monies, investment services, and trust arrangements.

A typical example is interest on lawyers' trust accounts (IOLTA). These accounts contain funds for a lawyer's various clients, but act as a standard bank account with one unique feature: The interest earned on the account is ceded to the state bar association or another entity for public interest and pro bono purposes.

RISK FACTORS

In contrast to escrow accounts that are set up to serve individual clients, professional service provider accounts allow for ongoing business transactions with multiple clients. Generally, a bank has no direct relationship with or knowledge of the beneficial owners of these accounts, who may be a constantly changing group of individuals and legal entities.

As with any account that presents third-party risk, the bank could be more vulnerable to potential money laundering abuse. Some potential examples of abuse could include:

- Laundering illicit currency.
- Structuring currency deposits and withdrawals.
- Opening any third-party account for the primary purpose of masking the underlying client's identity.

As such, the bank should establish an effective due diligence program for the professional service provider as summarized below.

RISK MITIGATION

When establishing and maintaining relationships with professional service providers, banks should adequately assess account risk and monitor the relationship for suspicious or unusual activity. At account opening, the bank should have an understanding of the intended use of the account, including anticipated transaction volume, products and services used, and geographic locations involved in the relationship. As indicated in the core overview section on "Currency Transaction Reporting Exemptions," page 51, professional service providers cannot be exempted from currency transaction reporting requirements.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Non-Governmental Organizations and Charities

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with accounts of non-governmental organizations (NGOs) and charities, and management's ability to implement effective due diligence, monitoring, and reporting systems.

OVERVIEW

NGOs are private nonprofit organizations that pursue activities intended to serve the public good. NGOs may provide basic social services, work to relieve suffering, promote the interests of the poor, bring citizen concerns to governments, encourage political participation, protect the environment, or undertake community development to serve the needs of citizens, organizations, or groups in one or more of the communities that the NGO operates. An NGO can be any nonprofit organization that is independent from government.

NGOs can range from large regional, national, or international charities to community-based self-help groups. NGOs also include research institutes, churches, professional associations, and lobby groups. NGOs typically depend, in whole or in part, on charitable donations and voluntary service for support.

RISK FACTORS

Since NGOs can be used to obtain funds for charitable organizations, the flow of funds both into and out of the NGO can be complex, making them susceptible to abuse by money launderers and terrorists. Consequently, law enforcement has increased their scrutiny of NGOs.

RISK MITIGATION

To assess the risk of NGO customers, a bank should conduct adequate due diligence on the organization. In addition to required Customer Identification Program (CIP) information, due diligence for NGOs should focus on other aspects of the organization, such as the following:

- Purpose or ideology.
- The geographic areas served (including headquarters and operational areas).
- The organizational structure.
- The donor and volunteer base.
- Funding and disbursement criteria (including basic beneficiary information).

- Recordkeeping requirements.
- Its affiliation with other NGOs, governments, or groups.
- Internal controls and audits.

For accounts that bank management considers to be high risk, stringent documentation, verification, and transaction monitoring procedures should be established. NGO accounts that are at higher risk for BSA/AML concerns include those operating or providing services internationally, conducting unusual or suspicious activities, or lacking proper documentation. Enhanced due diligence for these accounts should include:

- Evaluating the principals.
- Obtaining and reviewing the financial statements and audits.
- Verifying the source and use of funds.
- Evaluating large contributors or grantors of the NGO.
- Conducting reference checks.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Corporate Entities (Domestic and Foreign)

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with transactions involving domestic and foreign corporate entities, and management's ability to implement effective due diligence, monitoring, and reporting systems.

OVERVIEW

The term "corporate entities" refers to a variety of company formations that may be used for many purposes, such as tax and estate planning. Corporate entities are relatively easy to establish. Individuals, partnerships, and existing corporations establish corporate entities for legitimate reasons, but the entities may be abused for money laundering and terrorist financing.

Domestic Corporate Entities

Shell corporations registered in the United States are a type of domestic corporate entity that may pose heightened risks.[153] In some state jurisdictions, only minimal information is required to register articles of incorporation and maintain corporate "good standing," for corporate entities – increasing the potential for their abuse by criminal and terrorist organizations.

Foreign Corporate Entities

Frequently used foreign corporate entities include trusts, investment funds, and insurance companies. Two foreign entities that can pose particular money laundering risk are international business corporations (IBCs) and Private Investment Companies (PICs) opened in offshore financial centers (OFCs).[154] Many OFCs have limited organizational disclosure and recordkeeping requirements for establishing foreign corporate entities, creating an opportune environment for money laundering.

[153] A shell corporation is defined as a corporation without a physical presence in any country.

[154] While some OFCs are well regulated, the primary attraction of the offshore sector remains the frequent existence of legal frameworks designed to obscure the identity of beneficial owners, to promote regulatory and supervisory arbitrage, and to provide mitigation or evasion of home-country tax regimes.

International Business Corporations

IBCs are entities formed outside of a person's country of residence which can be used to maintain confidentially or hide assets. There are a variety of advantages to using an IBC which include, but are not limited to, the following:

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

Through an IBC, an individual is able to conduct the following:

- Open and hold bank accounts.
- Hold and transfer funds.
- Engage in international business and other related transactions.
- Hold and manage offshore investments (e.g., stocks, bonds, mutual funds, and certificates of deposit) many of which may not be available to "individuals" depending on their location of residence.
- Hold corporate debit and credit cards, thereby allowing convenient access to funds.

Private Investment Companies

PICs are separate legal entities. PICs offer confidentiality of ownership, hold assets centrally, and may provide intermediaries between private banking customers and the potential beneficiaries of the PICs. A PIC may also be an investment of a trust account. PICs are incorporated frequently in countries that impose low or no taxes on company assets and operations or that are bank secrecy havens.

RISK FACTORS

Money laundering and terrorist financing risks arise because corporate entities can hide the true owner of assets or property derived from or associated with criminal activity. The privacy and confidentiality surrounding some corporate entities may be exploited by criminals, money launderers, and terrorists. Verifying the grantors and beneficial owner(s) of some corporate entities may be extremely difficult, as the characteristics of these entities shield the legal identity of the owner. Few public records will disclose true ownership. Overall, the lack of ownership transparency; minimal or no recordkeeping requirements, financial disclosures, and supervision; and the range of permissible activities all increase money laundering risk.

While corporate entities can be established in most international jurisdictions, the majority are incorporated in OFCs that provide ownership privacy and impose few or no tax obligations. To maintain anonymity, many corporate entities are formed with nominee directors, nominee officeholders, and nominee shareholders. In certain jurisdictions, corporate entities can also be established using bearer shares; ownership

records are not maintained, rather ownership is based on physical possession of the stock certificates. Revocable trusts are another method used to insulate the grantor and beneficial owner and can be designed to own and manage the corporate entity, presenting significant barriers to law enforcement.

While U.S.-based shell corporations have been used for legitimate purposes, they have also been abused as conduits for money laundering and have hidden overseas transactions or the existence of layered domestic or foreign corporate entity structures. Shell corporations registered in the United States have been identified as conducting suspicious transactions with foreign-based counterparties. These transactions, primarily funds transfers circling in and out of the U.S. banking system, evidenced no apparent business purpose. Domestic corporate entities with bank-like names, but without regulatory authority to conduct banking, should be particularly suspect.

RISK MITIGATION

Management should develop policies, procedures, and processes that enable the bank to identify account relationships, in particular deposit accounts, and monitor the risks associated with these accounts in all the bank's departments. Corporate entity customers may open accounts within the private banking department, within the trust department, or at local branches. Management should establish enhanced due diligence at account opening and during the life of the relationship to manage risk in these accounts. The bank should gather sufficient information on the corporate entities and their beneficial owners to understand and assess the risks of the account relationship. Important information for determining the valid use of these entities includes: the type of business, the purpose of the account, the source of funds, and the source of wealth of the beneficiary.

The bank's Customer Identification Program (CIP) should detail the identification requirements for opening an account for a corporate entity. When opening an account for a customer that is not an individual, banks are permitted by 31 CFR 103.121 to obtain information about the individuals who have authority and control over such accounts in order to verify the customer's identity (the customer being the corporate entity). Required account opening information may include articles of incorporation, a corporate resolution by the directors authorizing the opening of the account, or the appointment of a person to act as a signatory for the entity on the account. Particular attention should be paid to articles of association that allow for nominee shareholders, board members, and bearer shares.

If the bank, through its trust or private banking departments, is facilitating the establishment of a corporate entity for a new or existing customer, the money laundering risk to the bank is typically mitigated. Since the bank is aware of the parties (i.e., grantors, beneficiaries, and shareholders) involved in the corporate entity, initial due diligence and verification is easier to obtain. Furthermore, in such cases, the bank frequently has ongoing relationships with the customers initiating the establishment of a corporate entity.

Risk assessment may include a review of the domestic or international jurisdiction where the corporate entity was established, the type of account (or accounts) and expected versus actual transaction activities, the types of products that will be used, and whether the corporate entity was created in-house or externally. If ownership is held in bearer share form, the bank should maintain the physical control of the bearer shares either in-house or with a trusted third party to ensure that the ownership of the corporate entity does not change without the bank's knowledge. The bank's risk assessment of a corporate entity customer becomes more important in complex corporate formations. For example, a foreign IBC may establish a layered series of corporate entities, with each entity naming its parent as its beneficiary.

Ongoing account monitoring is critical to ensure that the accounts are reviewed for unusual and suspicious activity. The bank should be aware of high-risk transactions in these accounts, such as activity that has no business or apparent lawful purpose, funds transfer activity to and from high-risk jurisdictions, currency intensive transactions, and frequent changes in the ownership or control of the nonpublic corporate entity.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Overview – Cash-Intensive Businesses

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with cash-intensive businesses and entities, and management's ability to implement effective due diligence, monitoring, and reporting systems.

OVERVIEW

Cash-intensive businesses and entities cover various industry sectors. Most of these businesses are conducting legitimate business; however, some aspects of these businesses may be susceptible to money laundering or terrorist financing. Common examples include, but are not limited to, the following:

- Convenience stores.
- Restaurants.
- Retail stores.
- Liquor stores.
- Cigarette distributors.
- Privately-owned automated teller machines (ATMs).
- Vending machine operators.
- Parking garages.

RISK FACTORS

Some businesses and entities may be misused by money launderers to legitimize their illicit proceeds. For example, a criminal may own a cash-intensive business, such as a restaurant, and use it to launder currency from illicit criminal activities. The restaurant's currency deposits with its bank do not, on the surface, appear unusual since the business is legitimately a cash-generating entity. However, the volume of currency in a restaurant used to launder money will most likely be higher in comparison with similar restaurants in the area. The nature of cash-intensive businesses and the difficulty in identifying unusual activity may cause these businesses to be considered high risk.

RISK MITIGATION

When establishing and maintaining relationships with cash-intensive businesses, banks should establish policies, procedures, and processes to identify high-risk relationships; assess AML risks; complete due diligence at account opening and periodically throughout the relationship; and include such relationships in appropriate monitoring for unusual or suspicious activity. At the time of account opening, the bank should have an

understanding of the customer's business operations; the intended use of the account; including anticipated transaction volume, products, and services used; and the geographic locations involved in the relationship.

When conducting a risk assessment of cash-intensive businesses, banks should direct their resources to those accounts that pose the greatest risk of money laundering or terrorist financing. The following factors may be used to identify the risks:

- The purpose of the account.
- The volume, frequency, and nature of currency transactions.
- Customer history (e.g., length of relationship, Currency Transaction Report (CTR) filings,[155] Suspicious Activity Report (SAR) filings).
- The primary business activity, products, and services offered.
- The corporate or business structure.
- Geographic locations and jurisdictions of operations.
- The availability of information and cooperation of the business in providing information.

For those customers deemed to be particularly high risk, bank management may consider implementing sound practices, such as periodic on-site visits, interviews with the business's management, or closer reviews of transactional activity.

[155] As discussed in the core overview section "Currency Transaction Reporting Exemptions," on page 51, certain entities are ineligible for currency transaction reporting exemptions as a non-listed business.