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 and state 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 Examination Overview and Procedures for Assessing the BSA/AML Compliance Program.
- Core Examination Overview and Procedures for Regulatory Requirements and Related Topics.
- Expanded Examination Overview and Procedures for Consolidated and Other Types of BSA/AML Compliance Program Structures.
- Expanded Examination Overview and Procedures for Products and Services.

[1] The FFIEC was established in March 1979 to prescribe uniform principles, standards, and report forms and to promote uniformity in the supervision of financial institutions. The Council has six voting members: the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the State Liaison Committee. The Council's activities are supported by interagency task forces and by an advisory State Liaison Committee, comprised of five representatives of state agencies that supervise financial institutions.

- Expanded Examination Overview and Procedures for Persons and Entities.
- Appendices.

The core and expanded overview sections provide narrative guidance and background information on each topic; each overview is followed by examination procedures. The "Core Examination Overview and Procedures for Assessing the BSA/AML Compliance Program" and the "Core Examination Overview and Procedures for Regulatory Requirements and Related Topics" (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" and the "BSA/AML Risk Assessment" sections help the examiner develop an appropriate examination plan based on the risk profile of the bank. 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 and examination procedures address the BSA requirements while the expanded overview and examination procedures address the AML risks of the specific activity.

At a minimum, examiners should use the following examination procedures included within the "Core Examination Overview and Procedures for Assessing the BSA/AML Compliance Program" section 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 19 to 21).
- BSA/AML Risk Assessment (refer to page 31).
- BSA/AML Compliance Program (refer to pages 38 to 43).
- Developing Conclusions and Finalizing the Examination (refer to pages 48 to 51).

While OFAC regulations are not part of the BSA, the core sections include overview and examination procedures for examining a bank's policies, procedures, and processes for ensuring compliance with OFAC sanctions. As part of the scoping and planning procedures, examiners must review the bank's OFAC risk assessment and independent testing to determine the extent to which a review of the bank's OFAC compliance program should be conducted during the examination. Refer to core examination procedures, "Office of Foreign Assets Control," pages 157 to 159, for further guidance.

The expanded sections address specific lines of business, products, customers, 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, customers, or entities could elevate BSA/AML risks. In addition, the expanded section provides guidance on BSA/AML compliance program structures and management.

Not all of the core and expanded examination procedures will likely be applicable to every banking organization. The specific examination 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 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 adding the interrelated sections 8(s) and 21 to the Federal Deposit Insurance Act (FDIA) and section 206(q) of the Federal Credit Union Act (FCUA), 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

[2] 31 USC 5311 *et seq.*, 12 USC 1829b, and 1951 – 1959. Also refer to 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. The term "bank" is used throughout the manual generically to refer to the financial institution being examined.

[4] 12 USC 1818(s), 1829(b), and 1786(q), respectively.

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 (USA PATRIOT Act). Title III of the USA PATRIOT Act is the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001. The USA PATRIOT Act is arguably the single most significant AML law that Congress has enacted since the BSA itself. Among other things, the USA 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 (EDD) procedures for foreign correspondent and private banking accounts; and improving information sharing between financial institutions and the U.S. government. The USA PATRIOT Act and its implementing regulations also:

- 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

[5] The USA 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 USA PATRIOT Act. Those financial institutions that are not currently subject to a final AML program rule are temporarily exempted from the USA PATRIOT Act requirements to establish an AML program, as set forth in 31 CFR 103.170.

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 nonbank financial institutions, such as money services businesses, casinos, brokers/dealers in securities, futures commission merchants, mutual funds, insurance companies, and operators of credit card systems.

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 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 (National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision), insuring (Federal Deposit Insurance Corporation and National Credit Union Administration), regulating, and supervising banks.[6] 12 USC 1818(s)(2) and 1786(q) require 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.

[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.

The federal banking agencies require each bank under their supervision to establish and maintain a BSA compliance program.[7] In accordance with the USA 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 USA 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 USA 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 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

[7] Refer to 12 CFR 208.63, 12 CFR 211.5(m) and 12 CFR 211.24(j) (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.

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.

On July 19, 2007, the federal banking agencies issued a statement setting forth the agencies' policy for enforcing specific anti-money laundering requirements of the BSA. The purpose of the *Interagency Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements* (Interagency Enforcement Statement) is to provide greater consistency among the agencies in enforcement decisions in BSA matters and to offer insight into the considerations that form the basis of those decisions.[9]

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 and examination procedures, "Office of Foreign Assets Control," pages 147 to 156 and 157 to 159, respectively, for guidance.

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 and other weaknesses in the legitimate financial system to launder criminal proceeds, finance terrorism, or conduct other illegal activities, and, ultimately, hide the actual purpose of their activity.

[9] Refer to Appendix R for additional information.

Banking organizations must develop, implement, and maintain effective AML programs that address the ever-changing strategies of money launderers and terrorists who 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,[10] 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 prepaid cards; and funds transfers. There is also evidence that some forms of informal banking (e.g., "hawala"[11]) 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 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.[12] Any property involved in a transaction or traceable to the proceeds of the criminal activity,

[10] Conflict diamonds originate from areas controlled by forces or factions opposed to legitimate and internationally recognized governments and 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).

[11] "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 USA PATRIOT Act, refer to FinCEN's Web site: www.fincen.gov.

[12] 18 USC 1956.

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 U.S. Department of Justice may bring criminal actions for money laundering that may include criminal fines, imprisonment, and forfeiture actions.[13] 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.[14] 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.[15] 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.[16]

Civil Penalties for Violations of the BSA

Pursuant to 12 USC 1818(i) and 1786(k), 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.

---

[13] 18 USC 981 and 982.

[14] 31 USC 5322(a).

[15] *Id.*

[16] *Id.*

CORE EXAMINATION OVERVIEW AND PROCEDURES FOR ASSESSING THE BSA/AML COMPLIANCE PROGRAM

Scoping and Planning — Overview

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

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.

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 (Core and Expanded)") for additional information.
- The bank's BSA/AML risk assessment.
- BSA-reporting database (Web Currency and Banking Retrieval System (Web CBRS)).
- Independent reviews or audits.

Review of the Bank's BSA/AML Risk Assessment

The scoping and planning process should be guided by the examiner's review of the bank's BSA/AML risk assessment. Information gained from the examiner's review of the risk assessment will assist the scoping and planning process as well as the evaluation of the adequacy of the BSA/AML compliance program. 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. Refer to the core overview section, "BSA/AML Risk Assessment," pages 22 to 30, for guidance on

developing a BSA/AML risk assessment. Evaluating the BSA/AML risk assessment is part of scoping and planning the examination, and the inclusion of a section on risk assessment in the manual does not mean the two processes are separate. Rather, risk assessment has been given its own section to emphasize its importance in the examination process and in the bank's design of effective risk-based controls.

Independent Testing

As part of the scoping and planning process, examiners should obtain and evaluate the supporting documents of the independent testing (audit)[17] 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 examination 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 19 to 21).
- BSA/AML Risk Assessment (refer to page 31).
- BSA/AML Compliance Program (refer to pages 38 to 43).
- Developing Conclusions and Finalizing the Examination (refer to pages 48 to 51).

The "Core Examination Overview and Procedures for Regulatory Requirements and Related Topics" section includes an overview and examination procedures for examining a bank's policies, procedures, and processes to ensure compliance with OFAC sanctions. As part of the scoping and planning procedures, examiners must review the bank's OFAC risk assessment and independent testing to determine the extent to which a review of the bank's OFAC compliance program should be conducted during the examination. Refer to core overview and examination procedures, "Office of Foreign Assets Control," pages 147 to 159, for further guidance.

[17] 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.

The examiner should develop and document 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, and any changes to the plan should likewise be documented. The examiner should prepare a request letter to the bank. Suggested request letter items are detailed in Appendix H ("Request Letter Items (Core and Expanded)"). On the basis of the risk profile, quality of audit, previous examination findings, and initial examination work, examiners should complete additional core and expanded examination procedures, as appropriate. The examiner must include an evaluation of the BSA/AML compliance program within the supervisory plan or cycle. At larger, more complex banking organizations, examiners may complete various types of examinations throughout the supervisory plan or cycle to assess BSA/AML compliance. These reviews may focus on one or more business lines (e.g., private banking, trade financing, or foreign correspondent banking relationships), based upon the banking organization's risk assessment and recent audit and examination findings.

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 and should be risk-based. Transaction testing can be performed either through conducting the transaction testing procedures within the independent testing (audit) section (refer to the core examination procedures, "BSA/AML Compliance Program," pages 38 to 43, for further guidance) or completing the transaction testing procedures contained elsewhere within the core or expanded sections.

The extent of transaction testing and activities conducted 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. Examiners should document their decision regarding the extent of transaction testing to conduct, the activities for which it is to be performed, and the rationale for any changes to the scope of transaction testing that occur during the examination.

Information Available From BSA-Reporting Database

Examination planning should also include an analysis of the SARs, Currency Transaction Reports (CTR), 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 database (Web CBRS). 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.

Examination Procedures

Scoping and Planning

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

To facilitate the examiner's understanding of the bank's risk profile and to adequately establish the scope of the BSA/AML examination, the examiner should complete the following steps, in conjunction with the review of the bank's BSA/AML risk assessment:

1. Review prior examination or inspection reports, related workpapers, and management's responses to any previously identified BSA issues; identify completed examination procedures; obtain BSA contact information; identify reports and processes the bank uses to detect unusual activity; identify previously noted higher-risk banking operations; review recommendations for the next examination. In addition, contact bank management as appropriate to discuss the following:

   - BSA/AML compliance program.
   - BSA/AML risk assessment.
   - Suspicious activity monitoring and reporting systems.
   - Level and extent of automated BSA/AML systems.

   For the above topics, refer to the appropriate overview and examination procedures sections in the manual for guidance.

2. Develop list of BSA items to be incorporated into the integrated examination request letter. If the BSA portion of the examination is a stand-alone examination, send the request letter to the bank. Review the request letter documents provided by the bank. Refer to Appendix H (Request Letter Items (Core and Expanded)).

3. Review correspondence between the bank and its primary regulator, if not already completed by the examiner in charge or other dedicated examination personnel. In addition, review correspondence that the bank or the primary regulators have received from, or sent to, outside regulatory and law enforcement agencies relating to BSA/AML compliance. Communications, particularly those received from FinCEN, and the IRS Enterprise Computing Center – Detroit (formerly the Detroit Computing Center) may document matters relevant to the examination, such as the following:

   - Filing errors for SARs, CTRs, and CTR exemptions.
   - Civil money penalties issued by or in process from FinCEN.
   - Law enforcement subpoenas or seizures.

- Notification of mandatory account closures of noncooperative foreign customers holding correspondent accounts as directed by the Secretary of the Treasury or the U.S. Attorney General.

4. Review SARs, CTRs, and CTR exemption information obtained from downloads from the BSA-reporting database. The number of SARs, CTRs, and CTR exemptions filed should be obtained for a defined time period, as determined by the examiner. Consider the following information, and analyze the data for unusual patterns, such as:

   - Volume of activity, and whether it is commensurate with the customer's occupation or type of business.
   - Number and dollar volume of transactions involving higher-risk customers.
   - Volume of CTRs in relation to the volume of exemptions (i.e., whether additional exemptions resulted in significant decreases in CTR filings).
   - Volume of SARs and CTRs in relation to the bank's size, asset or deposit growth, and geographic location.

   The federal banking agencies do not have targeted volumes or "quotas" for SAR and CTR filings for a given bank size or geographic location. Examiners should not criticize a bank solely because the number of SARs or CTRs filed is lower than SARs or CTRs filed by "peer" banks. However, as part of the examination, examiners must review significant changes in the volume or nature of SARs and CTRs filed and assess potential reasons for these changes.

5. Review internal and external audit reports and workpapers for BSA/AML compliance, as necessary, to determine the comprehensiveness and quality of audits, findings, and management responses and corrective action. A review of the independent audit's scope, procedures, and qualifications will provide valuable information on the adequacy of the BSA/AML compliance program.

6. While OFAC regulations are not part of the BSA, evaluation of OFAC compliance is frequently included in BSA/AML examinations. It is not the federal banking agencies' primary role to identify OFAC violations, but rather to evaluate the sufficiency of a bank's implementation of policies, procedures, and processes to ensure compliance with OFAC laws and regulations. To facilitate the examiner's understanding of the bank's risk profile and to adequately establish the scope of the OFAC examination, the examiner should complete the following steps:

   - Review the bank's OFAC risk assessment. The risk assessment, which may be incorporated into the bank's overall BSA/AML risk assessment, should consider the various types of products, services, customers, entities, transactions, and geographic locations in which the bank is engaged, including those that are processed by, through, or to the bank to identify potential OFAC exposure.
   - Review the bank's independent testing of its OFAC compliance program.

- Review correspondence received from OFAC and, as needed, the civil penalties area on OFAC's Web site to determine whether the bank had any warning letters, fines, or penalties imposed by OFAC since the most recent examination.
- Review correspondence between the bank and OFAC (e.g., periodic reporting of prohibited transactions and, if applicable, annual OFAC reports on blocked property).

In addition to the above, at larger, more complex banking organizations, examiners may complete various types of examinations throughout the supervisory plan or cycle to assess OFAC compliance. These reviews may focus on one or more business lines.

7. On the basis of the above examination procedures, in conjunction with the review of the bank's BSA/AML risk assessment, develop an initial examination plan. The examiner should adequately document the plan, as well as any changes to the plan that occur during the examination. The scoping and planning process should ensure that the examiner is aware of the bank's BSA/AML compliance program, OFAC compliance program, compliance history, and risk profile (i.e., products, services, customers, entities, transactions, and geographic locations).

As necessary, additional core and expanded examination procedures may be completed. While the examination plan may change at any time as a result of on-site findings, the initial risk assessment will enable the examiner to establish a reasonable scope for the BSA/AML review. In order for the examination process to be successful, examiners must maintain open communication with the bank's management and discuss relevant concerns as they arise.

BSA/AML Risk Assessment — Overview

Objective. *Assess the BSA/AML risk profile of the bank and evaluate the adequacy of the bank's BSA/AML risk assessment process.*

Evaluating the BSA/AML risk assessment should be part of scoping and planning the examination, and the inclusion of a section on risk assessment in the manual does not mean the two processes are separate. Rather, risk assessment has been given its own section to emphasize its importance in the examination process and in the bank's design of effective risk-based controls.

The same risk management principles that the bank uses in traditional operational areas should be applied to assessing and managing BSA/AML risk. A well-developed risk assessment will assist in identifying the bank's BSA/AML risk profile. Understanding the risk profile enables the bank to apply appropriate risk management processes to the BSA/AML compliance program to mitigate risk. This risk assessment process enables management to better identify and mitigate gaps in the bank's controls. The risk assessment should provide a comprehensive analysis of the BSA/AML risks in a concise and organized presentation, and should be shared and communicated with all business lines across the bank, board of directors, management, and appropriate staff; as such, it is a sound practice that the risk assessment be reduced to writing.

There are many effective methods and formats used in completing a BSA/AML risk assessment; therefore, examiners should not advocate a particular method or format. Bank management should decide the appropriate method or format, based on the bank's particular risk profile. Whatever format management chooses to use for its risk assessment, it should be easily understood by all appropriate parties.

The development of the BSA/AML risk assessment generally involves two steps: first, identify the specific risk categories (i.e., products, services, customers, entities, transactions, and geographic locations) unique to the bank; and second, conduct a more detailed analysis of the data identified to better assess the risk within these categories. In reviewing the risk assessment during the scoping and planning process, the examiner should determine whether management has considered all products, services, customers, entities, transactions, and geographic locations, and whether management's detailed analysis within these specific risk categories was adequate. 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 based on available information.[18]

[18] Refer to "Examiner Development of a BSA/AML Risk Assessment," pages 29 to 30, for guidance.

Evaluating the Bank's BSA/AML Risk Assessment

An examiner must review the bank's BSA/AML compliance program with sufficient knowledge of the bank's BSA/AML risks in order to determine whether the BSA/AML compliance program is adequate and provides the controls necessary to mitigate risks. For example, during the examination scoping and planning process, the examiner may initially determine that the bank has a high-risk profile, but during the examination, the examiner may determine that the bank's BSA/AML compliance program adequately mitigates these risks. Alternatively, the examiner may initially determine that the bank has a low- or moderate-risk profile; however, during the examination, the examiner may determine that the bank's BSA/AML compliance program does not adequately mitigate these risks.

In evaluating the risk assessment, an examiner should not necessarily take any single indicator as determinative of the existence of a lower or higher BSA/AML risk. The assessment of risk factors is bank-specific, and a conclusion regarding the risk profile should be based on a consideration of all pertinent information. Banks may determine that some factors should be weighed more heavily than others. For example, the number of funds transfers is certainly one factor to be considered in assessing risk; however, in order to effectively identify and weigh the risks, the examiner should look at other factors associated with those funds transfers, such as whether they are international or domestic, the dollar amounts involved, and the nature of the customer relationships.

Identification of Specific Risk Categories

The first step of the risk assessment process is to identify the specific products, services, customers, entities, and geographic locations unique to the bank. 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, entities, and geographic locations may be more vulnerable or 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 the number and volume of transactions, geographic locations, and nature of the customer relationships, should be considered when the bank prepares its risk assessment. The differences in the way a bank interacts with the customer (face-to-face contact versus electronic banking) also should be considered. Because of these factors, risks will vary from one bank to another. In reviewing the bank's risk assessment, examiners should determine whether management has developed an accurate risk assessment that identifies the significant risks to the bank.

The expanded sections in this manual provide guidance and discussions on specific lines of business, products, and customers that may present unique challenges and exposures for which banks may need to institute appropriate policies, procedures, and processes. Absent appropriate controls, these lines of business, products, or customers could elevate aggregate BSA/AML risks. The examiner should expect the bank's ongoing risk assessment process to address the varying degrees of risk associated with its products, services, customers, entities, and geographic locations, as applicable.

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. 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., prepaid and payroll cards), funds transfers (domestic and international), payable upon proper identification (PUPID) transactions, third-party payment processors, remittance activity, automated clearing house (ACH) transactions, and automated teller machines (ATM).
- Electronic banking.
- Private banking (domestic and international).
- Trust and asset management services.
- Monetary instruments.[19]
- Foreign correspondent accounts (e.g., bulk shipments of currency, pouch activity, payable through accounts (PTA), and U.S. dollar drafts).
- Trade finance.
- Services provided to third party payment processors or senders.
- Foreign exchange.
- Special use or concentration accounts.
- Lending activities, particularly loans secured by cash collateral and marketable securities.
- Nondeposit account services (e.g., nondeposit investment products and insurance).

The expanded sections of the manual provide guidance and discussion on specific products and services detailed above.

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 risks. At this stage of the risk assessment process, it is essential that banks exercise judgment and neither define nor

[19] 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," pages 243 to 245, for further discussion on risk factors and risk mitigation regarding monetary instruments.

treat all members of a specific category of customer as posing the same level of risk. In assessing customer risk, banks should consider other variables, such as services sought and geographic locations. The expanded sections of the manual provide guidance and discussion on specific customers and entities that are detailed below:

- Foreign financial institutions, including banks and foreign money services providers (e.g., casas de cambio, currency exchanges, and money transmitters).
- Nonbank 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 (PEP)).[20]
- Nonresident alien (NRA)[21] and accounts of foreign individuals.
- Foreign corporations and domestic business entities, particularly offshore corporations (such as domestic shell companies and Private Investment Companies (PIC) and international business corporations (IBC))[22] located in higher-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).
- Nongovernmental organizations and charities (foreign and domestic).
- Professional service providers (e.g., attorneys, accountants, doctors, or real estate brokers).

Geographic Locations

Identifying geographic locations that may 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 necessarily determine a customer's or transaction's risk level, either positively or negatively.

---

[20] Refer to core overview, "Private Banking Due Diligence Program (Non-U.S. Persons)," pages 130 to 134, and expanded overview, "Politically Exposed Persons," pages 297 to 300, for additional guidance.

[21] 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.

[22] For explanations of PICs and IBCs and additional guidance, refer to expanded overview, "Business Entities (Domestic and Foreign)," pages 323 to 328.

Higher-risk geographic locations can be either international or domestic. International higher-risk geographic locations generally include:

- Countries subject to OFAC sanctions, including state sponsors of terrorism.[23]
- Countries identified as supporting international terrorism under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State.[24]
- 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 USA PATRIOT Act.[25]
- Jurisdictions or countries monitored for deficiencies in their regimes to combat money laundering and terrorist financing by international entities such as the Financial Action Task Force (FATF).
- 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.[26]
- Offshore financial centers (OFC).[27]
- Other countries identified by the bank as higher-risk because of its prior experiences or other factors (e.g., legal considerations, or allegations of official corruption).
- Domestic higher-risk geographic locations may include, but are not limited to, banking offices doing business within, or having customers located within, a U.S. government-designated higher-risk geographic location. Domestic higher-risk geographic locations include:
    - High Intensity Drug Trafficking Areas (HIDTA).[28]

---

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

[24] A list of the countries supporting international terrorism appears in the U.S. Department of State's annual *Country Reports on Terrorism*. This report is available on the U.S. Department of State's Web site for its Counterterrorism Office: www.state.gov/s/ct/.

[25] 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 USA PATRIOT Act are available on the FinCEN Web site: www.fincen.gov/reg_section311.html.

[26] The INCSR, including the lists of high-risk money laundering countries and jurisdictions, may be accessed on the U.S. Department of State's Bureau of International Narcotics and Law Enforcement Affairs Web page www.state.gov/p/inl/rls/nrcrpt.

[27] OFCs offer a variety of financial products and services. For additional information, including assessments of OFCs, refer to www.imf.org/external/ns/cs.aspx?id=55.

- High Intensity Financial Crime Areas (HIFCA).[29]

Analysis of Specific Risk Categories

The second step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage in order to more accurately assess BSA/AML risk. This step involves evaluating data pertaining to the bank's activities (e.g., number of: domestic and international funds transfers; private banking customers; foreign correspondent accounts; PTAs; and domestic and international geographic locations of the bank's business area and customer transactions) in relation to Customer Identification Program (CIP) and customer due diligence (CDD) information. The level and sophistication of analysis may vary by bank. The detailed analysis is important because within any type of product or category of customer there will be accountholders that pose varying levels of risk.

This step in the risk assessment process gives management a better understanding of the bank's risk profile in order to develop the appropriate policies, procedures, and processes to mitigate the overall risk. Specifically, the analysis of the data pertaining to the bank's activities should consider, as appropriate, the following factors:

- Purpose of the account.
- Actual or anticipated activity in the account.
- Nature of the customer's business/occupation.
- Customer's location.
- Types of products and services used by the customer.

The value of a two-step risk assessment process is illustrated in the following example. The data collected in the first step of the risk assessment process reflects that a bank sends out 100 international funds transfers per day. Further analysis may show that approximately 90 percent of the funds transfers are recurring well-documented transactions for long-term customers. On the other hand, the analysis may show that 90 percent of these transfers are nonrecurring or are for noncustomers. While the numbers are the same for these two examples, the overall risks are different.

---

[28] The Anti-Drug Abuse Act of 1988 and The Office of National Drug Control Policy (ONDCP) Reauthorization Act of 1998 authorized the Director of ONDCP to designate areas within the United States that exhibit serious drug trafficking problems and harmfully impact other areas of the country as HIDTAs. The HIDTA Program provides additional federal resources to those areas to help eliminate or reduce drug trafficking and its harmful consequences. A listing of these areas can be found at www.whitehousedrugpolicy.gov/hidta/index.html.

[29] HIFCAs were first announced in the 1999 National Money Laundering Strategy and were conceived in the Money Laundering and Financial Crimes Strategy Act of 1998 as a means of concentrating law enforcement efforts at the federal, state, and local levels in high intensity money laundering zones. A listing of these areas can be found at www.fincen.gov/hifcaregions.html.

As illustrated above, the bank's CIP and CDD information take on important roles in this process. Refer to the core overview sections, "Customer Identification Program" and "Customer Due Diligence," found on pages 52 to 58 and 63 to 65, respectively, for additional guidance.

Developing the Bank's BSA/AML Compliance Program Based Upon Its Risk Assessment

Management should structure the bank's BSA/AML compliance program to adequately address its risk profile, as identified by the risk assessment. Management should understand the bank's BSA/AML risk exposure and develop the appropriate policies, procedures, and processes to monitor and control BSA/AML risks. For example, the bank's monitoring systems to identify, research, and report suspicious activity should be risk-based, with particular emphasis on higher-risk products, services, customers, entities, and geographic locations as identified by the bank's BSA/AML risk assessment.

Independent testing (audit) should review the bank's risk assessment for reasonableness. Additionally, management should consider the staffing resources and the level of training necessary to promote adherence with these policies, procedures, and processes. For those banks that assume a higher-risk BSA/AML profile, management should provide a more robust BSA/AML compliance program that specifically monitors and controls the higher risks that management and the board have accepted. Refer to Appendix I ("Risk Assessment Link to the BSA/AML Compliance Program") for a chart depicting the risk assessment's link to the BSA/AML compliance program.

Consolidated BSA/AML Compliance Risk Assessment

Banks that implement a consolidated or partially consolidated BSA/AML compliance program should assess risk both individually within business lines and across all activities and legal entities. Aggregating BSA/AML risks on a consolidated basis for larger or more complex organizations may enable an organization to better identify risks and risk exposures within and across specific lines of business or product categories. Consolidated information also assists senior management and the board of directors in understanding and appropriately mitigating risks across the organization. To avoid having an outdated understanding of the BSA/AML risk exposures, the banking organization should continually reassess its BSA/AML risks and communicate with business units, functions, and legal entities. The identification of a BSA/AML risk or deficiency in one area of business may indicate concerns elsewhere in the organization, which management should identify and control. Refer to the expanded overview section, "BSA/AML Compliance Program Structures," pages 160 to 165, for additional guidance.

Bank's Updating of the Risk Assessment

An effective BSA/AML compliance program controls risks associated with the bank's products, services, customers, entities, and geographic locations; therefore, an effective risk assessment should be an ongoing process, not a one-time exercise. Management should update its risk assessment to identify changes in the bank's risk profile, as

necessary (e.g., when new products and services are introduced, existing products and services change, higher-risk customers open and close accounts, or the bank expands through mergers and acquisitions). Even in the absence of such changes, it is a sound practice for banks to periodically reassess their BSA/AML risks at least every 12 to 18 months.

Examiner Development of a BSA/AML Risk Assessment

In some situations, banks may not have performed or completed an adequate BSA/AML risk assessment and examiners must complete one based on available information. When doing so, examiners do not have to use any particular format. In such instances, documented workpapers should include the bank's risk assessment, the deficiencies noted in the bank's risk assessment, and the examiner-prepared risk assessment.

Examiners should ensure that they have a general understanding of the bank's BSA/AML risks and, at a minimum, document these risks within the examination scoping process. This section provides some general guidance that examiners can use when they are required to complete a BSA/AML risk assessment. In addition, examiners may share this information with bankers to develop or improve their own BSA/AML risk assessment.

The risk assessment developed by examiners generally will not be as comprehensive as one developed by a bank. However, similar to what is expected in a bank's risk assessment, examiners should obtain information on the bank's products, services, customers, entities, and geographic locations to determine the volume and trend for potentially higher-risk areas. This process can begin with an analysis of:

- BSA-reporting database information (Web Currency and Banking Retrieval System (Web CBRS)).
- Prior examination or inspection reports and workpapers.
- Response to request letter items.
- Discussions with bank management and appropriate regulatory agency personnel.
- Reports of Condition and Income (Call Report) and Uniform Bank Performance Report (UBPR).

Examiners should complete this analysis by reviewing the level and trend of information pertaining to banking activities identified, for example:

- Funds transfers.
- Private banking.
- Monetary instrument sales.
- Foreign correspondent accounts and PTAs.

- Branch locations.
- Domestic and international geographic locations of the bank's business area.

This information should be evaluated relative to such factors as the bank's total asset size, customer base, entities, products, services, and geographic locations. Examiners should exercise caution if comparing information between banks and use their experience and insight when performing this analysis. Specifically, examiners should avoid comparing the number of SARs filed by a bank to those filed by another bank in the same geographic location. Examiners can and should use their knowledge of the risks associated with products, services, customers, entities, and geographic locations to help them determine the bank's BSA/AML risk profile. Examiners may refer to Appendix J ("Quantity of Risk Matrix") when completing this evaluation.

After identifying potential higher-risk operations, examiners should form a preliminary BSA/AML risk profile of the bank. The preliminary risk profile will provide the examiner with the basis for the initial BSA/AML examination scope and the ability to determine the adequacy of the bank's BSA/AML compliance program. Banks may have an appetite for higher-risk activities, but these risks should be appropriately mitigated by an effective BSA/AML compliance program tailored to those specific risks.

The examiner should develop an initial examination scoping and planning document commensurate with the preliminary BSA/AML risk profile. As necessary, the examiner should identify additional examination procedures beyond the minimum procedures that must be completed during the examination. While the initial scope may change during the examination, the preliminary risk profile will enable the examiner to establish a reasonable scope for the BSA/AML review.

Examiner Determination of the Bank's BSA/AML Aggregate Risk Profile

The examiner, during the "Developing Conclusions and Finalizing the Examination" phase of the BSA/AML examination, should assess whether the controls of the bank's BSA/AML compliance program are appropriate to manage and mitigate its BSA/AML risks. Through this process the examiner should determine an aggregate risk profile for the bank. This aggregate risk profile should take into consideration the risk assessment developed either by the bank or by the examiner and should factor in the adequacy of the BSA/AML compliance program. Examiners should determine whether the bank's BSA/AML compliance program is adequate to appropriately mitigate the BSA/AML risks, based on the risk assessment. The existence of BSA/AML risk within the aggregate risk profile should not be criticized as long as the bank's BSA/AML compliance program adequately identifies, measures, monitors, and controls this risk as part of a deliberate risk strategy. When the risks are not appropriately controlled, examiners must communicate to management and the board of directors the need to mitigate BSA/AML risk. Examiners should document deficiencies as directed in the core examination procedures, "Developing Conclusions and Finalizing the Examination," pages 48 to 51.

Examination Procedures

BSA/AML Risk Assessment

Objective. *Assess the BSA/AML risk profile of the bank and evaluate the adequacy of the bank's BSA/AML risk assessment process.*

1. Review the bank's BSA/AML risk assessment. Determine whether the bank has included all risk areas, including any new products, services, or targeted customers, entities, and geographic locations. Determine whether the bank's process for periodically reviewing and updating its BSA/AML risk assessment is adequate.

2. If the bank has not developed a risk assessment, or if the risk assessment is inadequate, the examiner must complete a risk assessment.

3. Examiners should document and discuss the bank's BSA/AML risk profile and any identified deficiencies in the bank's BSA/AML risk assessment process with bank management.

BSA/AML Compliance Program — Overview

Objective. *Assess the adequacy of the bank's 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.*

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 the bank's management, and significant findings must be included in the report of examination or supervisory correspondence.

The BSA/AML compliance program[30] must be written, approved by the board of directors,[31] 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 the core overview section, "BSA/AML Risk Assessment," pages 22 to 30, for additional guidance on developing a BSA/AML risk assessment. Refer to Appendix I ("Risk Assessment Link to the BSA/AML Compliance Program") for a chart depicting the risk assessment's link to the BSA/AML compliance program. Furthermore, the BSA/AML compliance program must be fully implemented and reasonably designed to meet the BSA requirements.[32] 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.

---

[30] The Board of Governors of the Federal Reserve System requires Edge and agreement corporations and U.S. branches, agencies, and other offices of foreign banks supervised by the Federal Reserve to establish and maintain procedures reasonably designed to ensure and monitor compliance with the BSA and related regulations (refer to Regulation K, 12 CFR 211.5(m)(1) and 12 CFR 211.24(j)(1)). In addition, because the BSA does not apply extraterritorially, foreign offices of domestic banks are expected to have policies, procedures, and processes in place to protect against risks of money laundering and terrorist financing (12 CFR 208.63 and 12 CFR 326.8).

[31] The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, each require the U.S. branches, agencies, and representative offices of the foreign banks they supervise operating in the United States to develop written BSA compliance programs that are approved by their respective bank's board of directors and noted in the minutes, or that are approved by delegatees acting under the express authority of their respective bank's board of directors to approve the BSA compliance programs. "Express authority" means the head office must be aware of its U.S. AML program requirements and there must be some indication of purposeful delegation. For those U.S. branches, agencies, and representative office of foreign banks that were already in compliance with existing obligations under the BSA (and usual and customary business practices), the BSA compliance program requirement should not impose additional burden. Refer to 71 Fed. Reg. 13936 (March 20, 2006). Refer to expanded overview section, "Foreign Branches and Offices of U.S. Banks," pages 169 to 172, for further guidance.

[32] Refer to Appendix R, ("Enforcement Guidance") for additional information.

- 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 CIP must be included as part of the BSA/AML compliance program. Refer to the core overview section, "Customer Identification Program," pages 52 to 58, 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 (i.e., products, services, customers, entities, 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 SARs filed.
- 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.[33]

[33] Refer to Appendix P ("BSA Record Retention Requirements") for guidance.

- Implement risk-based CDD policies, procedures, and processes.
- Identify reportable transactions and accurately file all required reports including SARs, CTRs, and CTR exemptions. (Banks should consider centralizing the review and report-filing functions within the banking organization.)
- Provide for dual controls and the segregation of duties to the extent possible. For example, employees that complete the reporting forms (such as SARs, CTRs, and CTR exemptions) generally should not also be responsible for the decision to file the reports or grant the exemptions.
- Provide sufficient controls and systems for filing CTRs and CTR 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 bank personnel, as appropriate.
- Train employees to be aware of their responsibilities under the BSA regulations and internal policy guidelines.

The above list is not designed to be all-inclusive and should be tailored to reflect the bank's BSA/AML 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 generally every 12 to 18 months, commensurate with the BSA/AML risk profile of the bank. 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 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 adequacy and effectiveness of the BSA/AML compliance program, including policies, procedures, and processes. Typically, this evaluation will include an explicit statement about the BSA/AML compliance program's overall adequacy and effectiveness and compliance with applicable regulatory requirements. At the very least, the audit should contain sufficient information for the reviewer (e.g., an examiner, review auditor, or BSA officer) to reach a conclusion about the overall quality of the BSA/AML compliance program.
- A review of the bank's risk assessment for reasonableness given the bank's risk profile (products, services, customers, entities, and geographic locations).
- Appropriate risk-based transaction testing to verify the bank's adherence to the BSA recordkeeping and reporting requirements (e.g., CIP, SARs, CTRs and CTR exemptions, and 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.
- 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.

- An assessment of the integrity and accuracy of MIS used in the BSA/AML compliance program. MIS includes reports used to identify large currency transactions, aggregate daily currency transactions, funds transfer transactions, monetary instrument sales transactions, and analytical and trend reports.

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 individual to serve as the BSA compliance officer.[34] 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.

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, entities, 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.

---

[34] 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, 12 CFR 211.5(m), and 12 CFR 211.24(j) (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 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 typically should be given to new staff during employee orientation. Training should encompass information related to applicable business lines, such as trust services, international, and private banking. The BSA compliance officer should receive periodic training that is relevant and appropriate given changes to regulatory requirements as well as the activities and overall BSA/AML risk profile of the bank.

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 training 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.

Examination Procedures

BSA/AML Compliance Program

Objective. *Assess the adequacy of the bank's 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.*

1. Review the bank's board approved[35] written BSA/AML compliance program[36] to ensure it contains the following required elements:

   - A system of internal controls to ensure ongoing compliance.
   - Independent testing of BSA compliance.
   - A specifically designated person or persons responsible for managing BSA compliance (BSA compliance officer).
   - Training for appropriate personnel.

   A bank must have a BSA/AML compliance program commensurate with its respective BSA/AML risk profile. In addition, a CIP must be included as part of the BSA/AML compliance program.

2. Assess whether the board of directors and senior management receive adequate reports on BSA/AML compliance.

---

[35] The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency each require the U.S. branches, agencies, and representative offices of the foreign banks they supervise operating in the United States to develop written BSA compliance programs that are approved by their respective bank's board of directors and noted in the minutes, or that are approved by delegatees acting under the express authority of their respective bank's board of directors to approve the BSA compliance programs. "Express authority" means the head office must be aware of its U.S. AML program requirements and there must be some indication of purposeful delegation. For those U.S. branches, agencies, and representative office of foreign banks that were already in compliance with existing obligations under the BSA (and usual and customary business practices), the BSA compliance program requirement should not impose additional burden. Refer to 71 Fed. Reg. 13936 (March 20, 2006). Refer to expanded overview section, "Foreign Branches and Offices of U.S. Banks," pages 169 to 172, for further guidance.

[36] The Board of Governors of the Federal Reserve System requires Edge and agreement corporations and U.S. branches, agencies, and other offices of foreign banks supervised by the Federal Reserve to establish and maintain procedures reasonably designed to ensure and monitor compliance with the BSA and related regulations (refer to Regulation K, 12 CFR 211.5(m)(1) and 12 CFR 211.24(j)(1)). In addition, because the BSA does not apply extraterritorially, foreign offices of domestic banks are expected to have policies, procedures, and processes in place to protect against risks of money laundering and terrorist financing (12 CFR 211.24(j)(1) and 12 CFR 326.8).

Risk Assessment Link to the BSA/AML Compliance Program

3. On the basis of examination procedures completed in the scoping and planning process, including the review of the risk assessment, determine whether the bank has adequately identified the risk within its banking operations (products, services, customers, entities, and geographic locations) and incorporated the risk into the BSA/AML compliance program. Refer to Appendix I ("Risk Assessment Link to the BSA/AML Compliance Program") when performing this analysis.

Internal Controls

4. Determine whether the BSA/AML compliance program includes policies, procedures, and processes that:

   - Identify higher-risk banking operations (products, services, customers, entities, and geographic locations); 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, SARs filed, and corrective action taken.
   - 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 requirements, meet recommendations for BSA/AML compliance, and provide for timely updates to implement changes in regulations.
   - Implement risk-based CDD policies, procedures, and processes.
   - Identify reportable transactions and accurately file all required reports, including SARs, CTRs, and CTR exemptions. (Banks should consider centralizing the review and report-filing functions within the banking organization.)
   - Provide for dual controls and the segregation of duties to the extent possible. For example, employees that complete the reporting forms (such as SARs, CTRs, and CTR exemptions) generally should not also be responsible for the decision to file the reports or grant the exemptions.
   - Provide sufficient controls and monitoring systems for the 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.

- Train employees to be aware of their responsibilities under the BSA regulations and internal policy guidelines.
- Incorporate BSA compliance into job descriptions and performance evaluations of appropriate personnel.

Independent Testing

5. Determine whether the BSA/AML testing (audit) is independent (i.e., performed by a person (or persons) not involved with the bank's BSA/AML compliance staff) and whether persons conducting the testing report directly to the board of directors or to a designated board committee comprised primarily or completely of outside directors.

6. Evaluate the qualifications of the person (or persons) performing the independent testing to assess whether the bank can rely upon the findings and conclusions.

7. Validate the auditor's reports and workpapers to determine whether the bank's independent testing is comprehensive, accurate, adequate, and timely. The independent test should address the following:

   - The overall adequacy and effectiveness of the BSA/AML compliance program, including policies, procedures, and processes. Typically, this evaluation will include an explicit statement about the BSA/AML compliance program's overall adequacy and effectiveness and compliance with applicable regulatory requirements. At the very least, the audit should contain sufficient information for the reviewer (e.g., an examiner, review auditor, or BSA officer) to reach a conclusion about the overall quality of the BSA/AML compliance program.
   - BSA/AML risk assessment.
   - BSA reporting and recordkeeping requirements.
   - CIP implementation.
   - CDD policies, procedures, and processes and whether they comply with internal requirements.
   - Personnel adherence to the bank's BSA/AML policies, procedures, and processes.
   - Appropriate transaction testing, with particular emphasis on higher-risk operations (products, services, customers, and geographic locations).
   - Training, including its comprehensiveness, accuracy of materials, the training schedule, and attendance tracking.
   - The integrity and accuracy of MIS used in the BSA/AML compliance program. MIS includes reports used to identify large currency transactions, aggregate daily currency transactions, funds transfer transactions, monetary instrument sales transactions, and analytical and trend reports.

- Tracking of previously identified issues and deficiencies and verification that they have been corrected by management.
- If an automated system is not used to identify or aggregate large transactions, determine whether the audit or independent review includes a sample test check of tellers' cash proof sheets, tapes, or other documentation to determine whether large currency transactions are accurately identified and reported.

8. Determine whether the audit's review of suspicious activity monitoring systems includes an evaluation of the system's ability to identify unusual activity. Ensure through a validation of the auditor's reports and workpapers that the bank's independent testing:
   - Reviews policies, procedures, and processes for suspicious activity monitoring.
   - Evaluates the system's methodology for establishing and applying expected activity or filtering criteria.
   - Evaluates the system's ability to generate monitoring reports.
   - Determines whether the system filtering criteria are reasonable and include, at a minimum, cash, monetary instruments, funds transfers, and other higher-risk products, services, customers, or geographies, as appropriate.
9. Determine whether the audit's review of suspicious activity reporting systems includes an evaluation of the research and referral of unusual activity. Ensure through a validation of the auditor's reports and workpapers that the bank's independent testing includes a review of policies, procedures, and processes for referring unusual activity from all business lines (e.g., legal, private banking, foreign correspondent banking) to the personnel or department responsible for evaluating unusual activity.
10. Review the audit scope, procedures, and workpapers to determine adequacy of the audit based on the following:
    - Overall audit coverage and frequency in relation to the risk profile of the bank.
    - Board reporting and supervision of, and its responsiveness to, audit findings.
    - Adequacy of transaction testing, particularly for higher-risk banking operations and suspicious activity monitoring systems.
    - Competency of the auditors or independent reviewers regarding BSA/AML requirements.

BSA Compliance Officer

11. Determine whether the board of directors has designated a person or persons responsible for the overall BSA/AML compliance program. Determine whether the

BSA compliance officer has the necessary authority and resources to effectively execute all duties.

12. Assess the competency of the BSA compliance officer and his or her staff, as necessary. Determine whether the BSA compliance area is sufficiently staffed for the bank's overall risk level (based on products, services, customers, entities, and geographic locations), size, and BSA/AML compliance needs. In addition, ensure that no conflict of interest exists and that staff is given adequate time to execute all duties.

Training

13. Determine whether the following elements are adequately addressed in the training program and materials:

    - The importance the board of directors and senior management place on ongoing education, training, and compliance.
    - Employee accountability for ensuring BSA compliance.
    - Comprehensiveness of training, considering specific risks of individual business lines.
    - Training of personnel from all applicable areas of the bank.[37]
    - Frequency of training.
    - Documentation of attendance records and training materials.
    - Coverage of bank policies, procedures, processes, and new rules and regulations.
    - Coverage of different forms of money laundering and terrorist financing as it relates to identification and examples of suspicious activity.
    - Penalties for noncompliance with internal policies and regulatory requirements.

Transaction Testing

Transaction testing must include, at a minimum, either examination procedures detailed below (independent testing) or transaction testing procedures selected from within the core or expanded sections. While some transaction testing is required, examiners have the discretion to decide what testing to conduct. Examiners should document their decision regarding the extent of transaction testing to conduct and the activities where it is to be performed, as well as the rationale for any changes to the scope of transaction

[37] As part of this element, determine whether the bank conducts adequate training for any agents who are responsible for conducting CIP or other BSA-related functions on behalf of the bank.

testing that occur during the examination. Examiners should consider the following when determining how to proceed with transaction testing:

- Accounts or customers identified in the review of information obtained from downloads from the BSA-reporting database.
- Higher-risk products and services, customer and entities, and geographic locations for which it appears from the scoping and planning process that the bank may not have appropriate internal controls.
- New products and services, customers and entities, and geographies introduced into the bank's portfolio since the previous BSA/AML examination.

Independent Testing

14. Select a judgmental sample that includes transactions other than those tested by the independent auditor and determine whether independent testing:
    - Is comprehensive, adequate, and timely.
    - Has reviewed the accuracy of MIS used in the BSA/AML compliance program.
    - Has reviewed suspicious activity monitoring systems to include the identification of unusual activity.
    - Has reviewed whether suspicious activity reporting systems include the research and referral of unusual activity.

Preliminary Evaluation

After the examiner has completed the review of all four required elements of the bank's BSA/AML compliance program, the examiner should document a preliminary evaluation of the bank's program. At this point, the examiner should revisit the initial examination plan, in order to determine whether any strengths or weaknesses identified during the review of the institution's BSA/AML compliance program warrant adjustments to the initial planned scope. The examiner may complete the core examination procedures, "Office of Foreign Assets Control," pages 157 to 159. The examiner should document and support any changes to the examination scope, then proceed to the applicable core and, if warranted, expanded examination procedures. If there are no changes to the examination scope, the examiner should proceed to the core examination procedures, "Developing Conclusions and Finalizing the Examination," pages 48 to 51.

Developing Conclusions and Finalizing the Examination — Overview

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

In the final phase of the BSA/AML examination, the examiner should assemble all findings from the examination procedures completed. From those findings, the examiner should develop and document 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 (ROE), and determine and document what regulatory response, if any, is appropriate.

In some cases, the appropriate regulatory response will include the citation of a regulatory violation. The citation of violations of law and regulation is typically done in the context of supervisory activities. The extent to which violations affect the evaluation of a bank's BSA/AML compliance program is based on the nature, duration, and severity of noncompliance. In some cases, an agency may allow the bank to remedy the violation as part of the supervisory process. In appropriate circumstances, however, an agency may take either informal or formal enforcement actions to address violations of the BSA requirements.[38]

Systemic or Recurring Violations

Systemic or recurring violations of the BSA and its implementing regulations involve either a substantial number of deficiencies or a repeated failure to effectively and accurately record and report information required under the BSA, if the errors or incompleteness impair the integrity of the record or report, fail to adequately represent the transactions required to be reported, or impact the effectiveness of the bank's suspicious activity monitoring and reporting processes. Systemic violations are the result of ineffective systems or controls to obtain, analyze, and maintain required information, or to report customers, accounts, or transactions, as required under various provisions of the BSA. Recurring violations are repetitive occurrences of the same or similar issues. Unlike isolated or inadvertent issues, systemic or recurring issues demonstrate a pattern or practice of noncompliance with the BSA and its implementing regulations.

When evaluating whether violations represent a pattern or practice, examiners must analyze the pertinent facts and circumstances. Repeated, regular, usual, or institutionalized practices will typically constitute a pattern or practice. The totality of the circumstances must be considered when assessing whether a pattern or practice exists.

---

[38] The Interagency Enforcement Statement (refer to Appendix R) explains the basis for the federal banking agencies' enforcement of specific AML requirements of the BSA.

Considerations in determining whether a pattern or practice exists include, but are not limited to:

- Whether the number of violations is high when compared to the bank's total activity. This evaluation usually is determined through a sampling of transactions or records. Based on this process, determinations are made concerning the overall level of noncompliance. However, even if the violations are few in number they could reflect systemic noncompliance, depending on the severity (e.g., significant or egregious).

- Whether there is evidence of similar violations by the bank in a series of transactions or in different divisions or departments. This is not an exact calculation and examiners should balance the number, significance, and frequency of violations identified throughout the organization. Violations identified within various divisions or departments may or may not indicate a systemic violation. These violations should be evaluated in a broader context to determine if training or other compliance system weaknesses are also present.

- The relationship of the violations to one another (e.g., whether they all occurred in the same area of the bank, in the same product line, in the same branch or department, or with one employee).

- The impact the violation or violations have on the bank's suspicious activity monitoring and reporting capabilities.

- Whether the violations appear to be grounded in a written or unwritten policy or established procedure, or result from a lack of an established procedure.

- Whether there is a common source or cause of the violations.

- Whether the violations were the result of an isolated software problem in a BSA/AML reporting software product and whether the bank has taken appropriate steps to address the issue.

Systemic or recurring violations of the BSA could have a significant impact on the adequacy of the bank's BSA/AML compliance program. When systemic instances of noncompliance are identified, the examiner should consider the noncompliance in the context of the overall program (internal controls, training, independent testing, responsible person) and refer to the Interagency Enforcement Statement (refer to Appendix R) to determine whether the bank's BSA/AML compliance program is deficient as a result of the systemic noncompliance. All systemic violations should be brought to the attention of the bank's board of directors and management and documented in the report of examination or supervisory correspondence.

Types of systemic or recurring violations may include, but are not limited to:

- Failure to establish a due diligence program that includes a risk-based approach, and when necessary, enhanced policies, procedures, and controls concerning foreign correspondent accounts.

- Failure to maintain a reasonably designed due diligence program for private banking accounts for non-U.S. persons (as defined in 31 CFR 103.175).
- Frequent, consistent, or recurring late CTR or SAR filings.
- A significant number of CTRs or SARs with errors or omissions of data elements.
- Consistently failing to obtain or verify required customer identification information at account opening.
- Consistently failing to complete searches on 314(a) information requests.
- Failure to consistently maintain or retain records required by the BSA.

Also, the Interagency Enforcement Statement provides that "[t]he Agencies will cite a violation of the SAR regulations, and will take appropriate supervisory actions, if the organization's failure to file a SAR (or SARs) evidences a systemic breakdown in its policies, procedures, or processes to identify and research suspicious activity, involves a pattern or practice of noncompliance with the filing requirement, or represents a significant or egregious situation."[39]

Isolated or Technical Violations

Isolated or technical violations are limited instances of noncompliance with the BSA that occur within an otherwise adequate system of policies, procedures, and processes. These violations generally do not prompt serious regulatory concern or reflect negatively on management's supervision or commitment to BSA compliance, unless the isolated violation represents a significant or egregious situation or is accompanied by evidence of bad faith. Multiple isolated violations throughout bank departments or divisions can be indicative of systemic or recurring system weaknesses or violations.

Corrective action for isolated violations is usually undertaken by the bank's management within the normal course of business. All violations, regardless of type or significance, should be brought to the attention of the bank's management and documented appropriately.

Types of isolated or technical violations may include, but are not limited to:

- Failure to file or late filing of CTRs that is infrequent, not consistent, or nonrecurring.
- Failure to obtain complete customer identification information for a monetary instrument sales transaction that is isolated and infrequent.
- Infrequent, not consistent, or nonrecurring incomplete or inaccurate information in SAR data fields.

[39] Interagency Enforcement Statement, page 6.

- Failure to obtain or verify required customer identification information that is infrequent, not consistent, or nonrecurring.

- Failure to complete a 314(a) information request that is inadvertent or nonrecurring.

In formulating a written conclusion, the examiner does not need to discuss every procedure performed during the examination. During discussions with management about examination conclusions, examiners should include discussions of both strengths and weaknesses of the bank's BSA/AML compliance. Examiners should document all relevant determinations and conclusions.

Examination Procedures

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.*

Formulating Conclusions

1. Accumulate all pertinent findings from the BSA/AML examination procedures performed. Evaluate the thoroughness and reliability of any risk assessment conducted by the bank. Reach a preliminary conclusion as to whether the following requirements are met:

   - The BSA/AML compliance program is effectively monitored and supervised in relation to the bank's risk profile as determined by the risk assessment. The examiner should ascertain if the BSA/AML compliance program is effective in mitigating the bank's overall risk.
   - The board of directors and senior management are aware of BSA/AML regulatory requirements; effectively oversee BSA/AML compliance, and commit, as necessary, to corrective actions (e.g., audit and regulatory examinations).
   - BSA/AML policies, procedures, and processes are adequate to ensure compliance with applicable laws and regulations and appropriately address higher-risk operations (products, services, customers, entities, and geographic locations).
   - Internal controls ensure compliance with the BSA and provide sufficient risk management, especially for higher-risk operations (products, services, customers, entities, and geographic locations).
   - Independent testing (audit) is appropriate and adequately tests for compliance with required laws, regulations, and policies. Overall audit coverage and frequency are appropriate in relation to the risk profile of the bank. Transaction testing is adequate, particularly for higher-risk banking operations and suspicious activity monitoring systems.
   - The designated person responsible for coordinating and monitoring day-to-day compliance is competent and has the necessary resources.
   - Personnel are sufficiently trained to adhere to legal, regulatory, and policy requirements.
   - Information and communication policies, procedures, and processes are adequate and accurate.

   All relevant determinations should be documented and explained.

Determine the Underlying Cause

2. Determine the underlying cause of policy, procedure, or process deficiencies, if identified. These deficiencies can be the result of a number of factors, including, but not limited to, the following:

   - Management has not assessed, or has not accurately assessed, the bank's BSA/AML risks.
   - Management is unaware of relevant issues.
   - Management is unwilling to create or enhance policies, procedures, and processes.
   - Management or employees disregard established policies, procedures, and processes.
   - Management or employees are unaware of or misunderstand regulatory requirements, policies, procedures, or processes.
   - Higher-risk operations (products, services, customers, entities, and geographic locations) have grown faster than the capabilities of the BSA/AML compliance program.
   - Changes in internal policies, procedures, and processes are poorly communicated.

3. Determine whether deficiencies or violations were previously identified by management or audit or were only identified as a result of this examination.

Discuss Findings With Examiner in Charge and Identify Necessary Action

4. Discuss preliminary findings with the examiner in charge (EIC) or examiner responsible for reviewing the bank's overall BSA/AML compliance. Document workpapers appropriately with the following information:

   - A conclusion regarding the adequacy of the BSA/AML compliance program and whether it meets all the regulatory requirements by providing the following:
     - A system of internal controls.
     - Independent testing for compliance.
     - A specific person to coordinate and monitor the BSA/AML compliance program.
     - Training of appropriate personnel.

- A conclusion as to whether the written CIP is appropriate for the bank's size, location, and type of business.
- Any identified violations and an assessment of the severity of those violations.
- Identification of actions needed to correct deficiencies or violations and, as appropriate, the possibility of, among other things, requiring the bank to conduct more detailed risk assessments or take formal enforcement action.
- If necessary, recommendations for supervisory actions. In addition, as necessary, confer with agency supervisory management, and agency legal staff.
- An appropriate rating based on overall findings and conclusions.
- Findings that have been or will be discussed with bank management and, if applicable, any bank commitment for improvements or corrective action.

Preparing the BSA/AML Comments for the Report of Examination

5. Document your conclusion regarding the adequacy of the bank's BSA/AML compliance program. Discuss the effectiveness of each of these elements of the bank's BSA/AML compliance program. Indicate whether the BSA/AML compliance program meets all the regulatory requirements by providing the following:
   - A system of internal controls.
   - Independent testing for compliance.
   - A specific person to coordinate and monitor the BSA/AML compliance program.
   - Training of appropriate personnel.

   The BSA/AML compliance program must also include a written Customer Identification Program (CIP) appropriate for the bank's size, location, and type of business.

   The examiner does not need to provide a written comment on every one of the following items 6 through 13. Written comments should cover only areas or subjects pertinent to the examiner's findings and conclusions. All significant findings must be included in the ROE. The examiner should ensure that workpapers are prepared in sufficient detail to support issues discussed in the ROE. To the extent that the following items are discussed in the workpapers, but not the ROE, the examiner should ensure that the workpapers thoroughly and adequately document each review, as well as any other aspect of the bank's BSA/AML compliance program that merits attention, but may not rise to the level of being included in the ROE. The examiner should organize and reference workpapers and document conclusions and supporting information within internal databases, as appropriate. As applicable, the examiner should prepare a discussion of the following items.

6. Describe whether the bank's policies and procedures for law enforcement requests for information under section 314(a) of the USA PATRIOT Act (31 CFR 103.100) meet regulatory requirements.

7. If the bank maintains any foreign correspondent or private banking accounts for non-U.S. persons, describe whether the bank's due diligence policies, procedures, and processes meet regulatory requirements under section 312 of the USA PATRIOT Act (31 CFR 103.176 and 103.178).

8. Describe the board of directors' and senior management's commitment to BSA/AML compliance. Consider whether management has the following:

   - A strong BSA/AML compliance program fully supported by the board of directors.

   - A requirement that the board of directors and senior management are kept informed of BSA/AML compliance efforts, audit reports, any compliance failures, and the status of corrective actions.

9. Describe whether the bank's policies, procedures, and processes for SAR filings meet the regulatory requirements and are effective.

10. Describe whether the bank's policies, procedures, and processes for large currency transactions meet the requirements of 31 CFR 103.22 and are effective.

11. If applicable, describe whether the bank's policies, procedures, and processes for CTR exemptions meet regulatory reporting requirements, appropriately grant exemptions, and use the correct forms.

12. Describe whether the bank's funds transfer policies, procedures, and processes meet the requirements of 31 CFR 103.33(e) and (g). Briefly discuss whether the policies, procedures, and processes include effective internal controls (e.g., separation of duties, proper authorization for sending and receiving, and posting to accounts), and provide a means to monitor transfers for CTR reporting purposes.

13. Describe the bank's recordkeeping policies, procedures, and processes. Indicate whether they meet the requirements of 31 CFR 103.

    .

CORE EXAMINATION OVERVIEW AND PROCEDURES FOR REGULATORY REQUIREMENTS AND RELATED TOPICS

Customer Identification Program — Overview

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

All banks must have a written CIP.[40] The CIP rule implements section 326 of the USA 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.[41] The implementation of a CIP by subsidiaries of banks is appropriate as a matter of safety and soundness and protection from reputational risks. Domestic subsidiaries (other than functionally regulated subsidiaries subject to separate CIP rules) of banks should comply with the CIP rule that applies to the parent bank when opening an account within the meaning of 31 CFR 103.121.[42]

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.

---

[40] Refer to 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).

[41] 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.

[42] *Frequently Asked Questions Related to Customer Identification Program Rules* issued by FinCEN, 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, April 28, 2005.

- The bank's methods of opening accounts.
- The types of identifying information available.
- The bank's size, location, and customer base, including types of products and services used by customers in different geographic locations.

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.

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.[43] 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.[44] 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)).

---

[43] 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.

[44] The bank may demonstrate that it knows an existing customer's true identity by 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 about the person's accounts without issue, loans made and repaid, or other services performed for the person over a period of time. However, the comparable procedures used to verify the identity detailed above might not suffice for persons that the bank has deemed to be higher risk.

Customer Information Required

The CIP must contain account-opening procedures detailing the identifying information that must be obtained from each customer.[45] At a minimum, the bank must obtain the following identifying information from each customer before opening the account:[46]

- Name.
- Date of birth for individuals.
- Address.[47]
- Identification number.[48]

Based on its risk assessment, 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.

---

[45] 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.

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

[47] 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.

[48] An identification number for a U.S. person is a taxpayer identification number (TIN) (or evidence of an application for one), and an identification number 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 (SSN), individual taxpayer identification number (ITIN), or employer identification number).

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 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 and Retention Requirements

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.[49] 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.

---

[49] A bank may keep photocopies of identifying documents that it uses to verify a customer's identity; however, the CIP regulation does not require it. A bank's verification procedures should be risk-based and, in certain situations, keeping copies of identifying documents may be warranted. In addition, a bank may have procedures to keep copies of the documents for other purposes, for example, to facilitate investigating potential fraud. However, if a bank does choose to retain photocopies of identifying documents, it should ensure that these photocopies are physically secured to adequately protect against possible identity theft. (These documents should be retained in accordance with the general recordkeeping requirements in 31 CFR 103.38.) Nonetheless, a bank should be mindful that it must not improperly use any documents containing a picture of an individual, such as a driver's license, in connection with any aspect of a credit transaction. Refer to *Frequently Asked Questions Related to Customer Identification Program Rules* issued by FinCEN, 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, April 28, 2005.

- 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.[50] 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.

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 rule implementing the AML program requirements of 31 USC 5318(h) and is regulated by a federal functional regulator.[51]

---

[50] 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 31 CFR 103.100 requests remain separate and distinct requirements.

[51] 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;

- 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 CIP 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 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. Refer to "Reliance on Another Financial Institution," pages 57 to 58.

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 (FAQ), 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.

Office of Thrift Supervision; Securities and Exchange Commission; or Commodity Futures Trading Commission.

Examination Procedures

Customer Identification Program

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

1. Verify that the bank's policies, procedures, and processes include a comprehensive program for identifying customers who open an account after October 1, 2003. The written program must be included within the bank's BSA/AML compliance program and must include, at a minimum, policies, procedures, and processes for the following:

   - Identification of information required to be obtained (including name, address, taxpayer identification number (TIN), and date of birth, for individuals), and risk-based identity verification procedures (including procedures that address situations in which verification cannot be performed).
   - Procedures for complying with recordkeeping requirements.
   - Procedures for checking new accounts against prescribed government lists, if applicable.
   - Procedures for providing adequate customer notice.
   - Procedures covering the bank's reliance on another financial institution or a third party, if applicable.
   - Procedures for determining whether and when a SAR should be filed.

2. Determine whether the bank's CIP considers the types of accounts offered; methods of account opening; and the bank's size, location, and customer base.

3. Determine whether the bank's policy for opening new accounts for existing customers appears reasonable.

4. Review board minutes and verify that the board of directors approved the CIP, either separately or as part of the BSA/AML compliance program (31 CFR 103.121(b)(1)).

5. Evaluate the bank's audit and training programs to ensure that the CIP is adequately incorporated (31 CFR 103.121(b)(1)).

6. Evaluate the bank's policies, procedures, and processes for verifying that all new accounts are checked against prescribed government lists for suspected terrorists or terrorist organizations on a timely basis, if such lists are issued (31 CFR 103.121(b)(4)).

Transaction Testing

7. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of new accounts opened since the most recent examination to review for compliance with the bank's CIP. The sample should include a cross-section of accounts (e.g., consumers and businesses, loans and deposits, credit card relationships, and Internet accounts). The sample should also include the following:

   - Accounts opened for a customer that provides an application for a TIN or accounts opened with incomplete verification procedures.
   - New accounts opened using documentary methods and new accounts opened using nondocumentary methods.
   - Accounts identified as higher risk.[52]
   - Accounts opened by existing higher-risk customers.
   - Accounts opened with exceptions.
   - Accounts opened by a third party (e.g., indirect loans).

8. From the previous sample of new accounts, determine whether the bank has performed the following procedures:

   - Opened the account in accordance with the requirements of the CIP (31 CFR 103.121(b)(1)).
   - Formed a reasonable belief as to the true identity of a customer, including a higher-risk customer. (The bank should already have a reasonable belief as to the identity of an existing customer (31 CFR 103.121(b)(2)).)
   - Obtained from each customer, before opening the account, the identity information required by the CIP (31 CFR 103.121(b)(2)(i)) (e.g., name, date of birth, address, and identification number).
   - Within a reasonable time after account opening, verified enough of the customer's identity information to form a reasonable belief as to the customer's true identity (31 CFR 103.121(b)(2)(ii)).
   - Appropriately resolved situations in which customer identity could not be reasonably established (31 CFR 103.121(b)(2)(iii)).

[52] Higher-risk accounts, for CIP purposes, may include accounts in which identification verification is typically more difficult (e.g., foreign private banking and trust accounts, accounts of senior foreign political figures, offshore accounts, and out-of-area and non-face-to-face accounts).

- Maintained a record of the identity information required by the CIP, the method used to verify identity, and verification results (including results of discrepancies) (31 CFR 103.121(b)(3)).
- Compared the customer's name against the list of known or suspected terrorists or terrorist organizations, if applicable (31 CFR 103.121(b)(4)).
- Filed SARs, as appropriate.

9. Evaluate the level of CIP exceptions to determine whether the bank is effectively implementing its CIP. A bank's policy may not allow staff to make or approve CIP exceptions. However, a bank may exclude isolated, nonsystemic errors (such as an insignificant number of data entry errors) from CIP requirements without compromising the effectiveness of its CIP (31 CFR 103.121(b)(1)).
10. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit, select a sample of relationships with third parties the bank relies on to perform its CIP (or portions of its CIP), if applicable. If the bank is using the "reliance provision":
    - Determine whether the third party is a federally regulated institution subject to a final rule implementing the AML program requirements of 31 USC 5318(h).
    - Review the contract between the parties, annual certifications, and other information, such as the third party's CIP (31 CFR 103.121(b)(6)).
    - Determine whether reliance is reasonable. The contract and certification will provide a standard means for a bank to demonstrate that it has satisfied the "reliance provision," unless the examiner has reason to believe that the bank's reliance is not reasonable (e.g., the third party has been subject to an enforcement action for AML or BSA deficiencies or violations).
11. If the bank is using an agent or service provider to perform elements of its CIP, determine whether the bank has established appropriate internal controls and review procedures to ensure that its CIP is being implemented for third-party agent or service-provider relationships (e.g., car dealerships).
12. Review the adequacy of the bank's customer notice and the timing of the notice's delivery (31 CFR 103.121(b)(5)).
13. Evaluate the bank's CIP record retention policy and ensure that it corresponds to the regulatory requirements to maintain certain records. The bank must retain the identity information obtained at account opening for five years after the account closes. The bank must also maintain a description of documents relied on, methods used to verify identity, and resolution of discrepancies for five years after the record is made (31 CFR 103.121(b)(3)(ii)).

14. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with CIP.

Customer Due Diligence — Overview

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.*

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 higher risk for money laundering and terrorist financing. The objective of CDD should be to enable the bank to predict with relative certainty the types of transactions in which a customer is likely to engage. These processes 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. Processes should also include enhanced CDD for higher-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 higher-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 should obtain information at account opening sufficient to develop an understanding of normal and expected activity for the customer's occupation or business operations. This understanding may be based on account type or customer classification. For additional guidance, refer to Appendix K ("Customer Risk versus Due Diligence and Suspicious Activity Monitoring").

This information should allow the bank to differentiate between lower-risk customers and higher-risk customers at account opening. Banks should monitor their lower-risk customers through regular suspicious activity monitoring and customer due diligence processes. If there is indication of a potential change in the customer's risk profile (e.g., expected account activity, change in employment or business operations), management should reassess the customer risk rating and follow established bank policies and procedures for maintaining or changing customer risk ratings.

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 processes should include periodic risk-based 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 Higher-Risk Customers

Customers that pose higher money laundering or terrorist financing risks present increased exposure to banks; due diligence policies, procedures, and processes should be enhanced as a result. Enhanced due diligence (EDD) for higher-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. Higher-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 for identifying higher-risk customers may be found in the core overview section, "BSA/AML Risk Assessment," pages 22 to 30.

The bank may determine that a customer poses a higher risk because of the customer's business activity, ownership structure, anticipated or actual volume and types of

transactions, including those transactions involving higher-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.
- Individuals with ownership or control over the account, such as beneficial owners, signatories, or guarantors.
- Occupation or type of business (of customer or other individuals with ownership or control over the account).
- Financial statements.
- Banking references.
- Domicile (where the business is organized).
- 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.

As due diligence is an ongoing process, a bank should take measures to ensure account profiles are current and monitoring should be risk-based. Banks should consider whether risk profiles should be adjusted or suspicious activity reported when the activity is inconsistent with the profile.

Examination Procedures

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.*

1. Determine whether the bank's CDD policies, procedures, and processes are commensurate with the bank's risk profile. Determine whether the bank has processes in place for obtaining information at account opening, in addition to ensuring current customer information is maintained.

2. Determine whether policies, procedures, and processes allow for changes to a customer's risk rating or profile. Determine who is responsible for reviewing or approving such changes.

3. Review the enhanced due diligence procedures and processes the bank uses to identify customers that may pose higher risk for money laundering or terrorist financing.

4. Determine whether the bank provides guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient information or inaccurate information is obtained.

Transaction Testing

5. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, sample CDD information for higher-risk customers. Determine whether the bank collects appropriate information and effectively incorporates this information into the suspicious activity monitoring process. This sample can be performed when testing the bank's compliance with its policies, procedures, and processes as well as when reviewing transactions or accounts for possible suspicious activity.

6. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with CDD.

Suspicious Activity Reporting — Overview

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

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. Examiners and banks should recognize that the quality of SAR content is critical to the adequacy and effectiveness of the suspicious activity reporting system.

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, evaluate, and report suspicious activity. However, as part of the examination process, examiners should review individual SAR filing decisions to determine the effectiveness of the bank's suspicious activity identification, evaluation, and reporting process. Banks, bank holding companies, and their subsidiaries are required by federal regulations[53] 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.[54]
  - 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.

[53] Refer to 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) and 31 CFR 103.18 (FinCEN).

[54] Refer to Appendix G ("Structuring") for additional guidance.

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

Suspicious activity monitoring and reporting are critical internal controls. Proper monitoring and reporting processes are essential to ensuring that the bank has an adequate and effective BSA compliance program. Appropriate policies, procedures, and processes should be in place to monitor and identify unusual activity. The sophistication of monitoring systems should be dictated by the bank's risk profile, with particular emphasis on the composition of higher-risk products, services, customers, entities, and geographies. 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. Monitoring systems typically include employee identification or referrals, transaction-based (manual) systems, surveillance (automated) systems, or any combination of these.

Generally, effective suspicious activity monitoring and reporting systems include four key components (refer to Appendix S "Key Suspicious Activity Monitoring Components"). The components, listed below, are interdependent, and an effective suspicious activity monitoring and reporting process should include successful implementation of each component. Breakdowns in any one or more of these components may adversely affect SAR reporting and BSA compliance. The four key components to an effective monitoring and reporting system are:

- Identification or alert of unusual activity (which may include: employee identification, law enforcement inquiries, other referrals, and transaction and surveillance monitoring system output).
- Managing alerts.
- SAR decision making.
- SAR completion and filing.

These four components are present in banks of all sizes. However, the structure and formality of the components may vary. Larger banks will typically have greater differentiation and distinction between functions, and may devote entire departments to the completion of each component. Smaller banks may use one or more employees to complete several tasks (e.g., review of monitoring reports, research activity, and completion of the actual SAR). Policies, procedures, and processes should describe the steps the bank takes to address each component and indicate the person(s) or departments responsible for identifying or producing an alert of unusual activity, managing the alert, deciding whether to file, and SAR completion and filing.

Identification of Unusual Activity

Banks use a number of methods to identify potentially suspicious activity, including but not limited to activity identified by employees during day-to-day operations, law enforcement inquiries, or requests, such as those typically seen in 314(a) and 314(b) requests, transaction and surveillance monitoring system output, or any combination of these.

Employee Identification

During the course of day-to-day operations, employees may observe unusual or potentially suspicious transaction activity. Banks should implement appropriate training, policies, and procedures to ensure that personnel adhere to the internal processes for identification and referral of potentially suspicious activity. Banks should be aware of all methods of identification and should ensure that their suspicious activity monitoring system includes processes to facilitate the transfer of internal referrals to appropriate personnel for further research.

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 when appropriate, identifying unusual or potentially suspicious activity related to those subjects, and filing, as appropriate, SARs related to those subjects. Law enforcement

inquiries and requests can include grand jury subpoenas, National Security Letters (NSL), and section 314(a) requests.[55]

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. For example, the receipt of a grand jury subpoena should cause a bank to review account activity for the relevant customer.[56] A bank should 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. Due to the confidentiality of grand jury proceedings, if a bank files a SAR after receiving a grand jury subpoena, law enforcement discourages banks from including any reference to the receipt or existence of the grand jury subpoena in the SAR. Rather, the SAR should reference only those facts and activities that support a finding of suspicious transactions identified by the bank.

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.[57]
- Information from credit bureaus.[58]
- Financial records from financial institutions.[59]

NSLs are highly confidential documents; for that reason, examiners will not review or sample specific NSLs.[60] 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

[55] Refer to core overview section, "Information Sharing," pages 97 to 102, for a discussion on section 314(a) requests.

[56] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance" *The SAR Activity Review – Trends, Tips & Issues*, Issue 10, May 2006, pages 42 – 44, at www.fincen.gov.

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

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

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

[60] Refer to the Bank Secrecy Act Advisory Group, *The SAR Activity Review — Trends, Tips & Issues*, Issue 8, April 2005 for further information on NSLs which is available at www.fincen.gov..

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.

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.

Transaction Monitoring (Manual Transaction Monitoring)

A transaction monitoring system, sometimes referred to as a manual transaction monitoring system, typically targets specific types of transactions (e.g., those involving large amounts of cash, those to or from foreign geographies) and includes a manual review of various reports generated by the bank's MIS or vendor systems in order to identify 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. Many MIS or vendor systems include filtering models for identification of potentially unusual activity. 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 higher-risk products, services, customers, entities, 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. The programming of the bank's monitoring systems should be independently reviewed for reasonable filtering criteria. Typical transaction monitoring reports are as follows.

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 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).

- Currency transactions aggregated by customer name, tax identification number, or customer information file number.

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 higher-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 be reviewed for unusual activity. Activities identified during these reviews should be subjected to additional research to ensure that identified activity is consistent with the stated account purpose and expected activity. When inconsistencies are identified, banks may need to conduct a global relationship review to determine if a SAR is warranted.

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. Reviews for suspicious activity should encompass activity for an extended period of time (30, 60, 90 days) and should focus on, among other things, identification of commonalities, such as common payees and purchasers, or consecutively numbered purchased monetary instruments.

Surveillance Monitoring (Automated Account Monitoring)

A surveillance monitoring system, sometimes referred to as an automated account monitoring system, can cover multiple types of transactions and use various rules to identify potentially suspicious activity. In addition, many can adapt over time based on historical activity, trends, or internal peer comparison. These 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 higher-risk customers typically use surveillance monitoring systems.

Surveillance monitoring 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 systems are more sophisticated than the basic manual system, which only filters on one rule (e.g., transaction greater than $10,000). Rule-based systems can apply multiple rules, overlapping rules, and filters that are more complex. For example, rule-based systems can initially apply a rule, or set of criteria to all accounts within a bank (e.g., all retail customers), and then apply a more refined set of criteria to a subset of accounts or risk category of accounts (e.g., all retail customers with direct deposits). Rule-based systems can also filter against individual customer-account profiles.

Intelligent systems are adaptive and can filter transactions, based on historical account activity or compare customer activity against a pre-established peer group or 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.

Relative to surveillance monitoring, system capabilities and thresholds refer to the parameters or filters used by banks in their monitoring processes. Parameters and filters should be reasonable and tailored to the activity that the bank is trying to identify or control. After parameters and filters have been developed, they should be reviewed before implementation to identify any gaps (common money laundering techniques or frauds) that may not have been addressed. For example, a bank may discover that its filter for cash structuring is triggered only by a daily cash transaction in excess of $10,000. The bank may need to refine this filter in order to avoid missing potentially suspicious activity because common cash structuring techniques often involve transactions that are slightly under the CTR threshold. Once established, the bank should review and test system capabilities and thresholds on a periodic basis. This review should focus on specific parameters or filters in order to ensure that intended information is accurately captured and that the parameter or filter is appropriate for the bank's particular risk profile.

Understanding the filtering criteria of a surveillance monitoring system is critical to assessing the effectiveness of the system. System filtering criteria should be developed through a review of specific higher-risk products and services, customers and entities, and geographies. System filtering criteria, including specific profiles and rules, should be based on what is reasonable and expected for each type of account. Monitoring accounts purely based on historical activity can be misleading if the activity is not actually consistent with similar types of accounts. For example, an account may have a historical transaction activity that is substantially different from what would normally be expected from that type of account (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 monitoring system's programming methodology and effectiveness should be independently validated to ensure that the models are detecting potentially suspicious activity.

Managing Alerts

Alert management focuses on processes used to investigate and evaluate identified unusual activity. Banks should be aware of all methods of identification and should ensure that their suspicious activity monitoring program includes processes to evaluate any unusual activity identified, regardless of the method of identification. Banks should have policies, procedures, and processes in place for referring unusual activity from all areas of the bank or business lines to the personnel or department responsible for evaluating unusual activity. Within those procedures, management should establish a clear and defined escalation process from the point of initial detection to disposition of the investigation.

The bank should assign adequate staff to the identification, evaluation, and reporting of potentially suspicious activities, taking into account the bank's overall risk profile and the volume of transactions. Additionally, a bank should ensure that the assigned staff possess the requisite experience levels and are provided with comprehensive and ongoing training to maintain their expertise. Staff should also be provided with sufficient internal and external tools to allow them to properly research activities and formulate conclusions.

Internal research tools include, but are not limited to, access to account systems and account information, including CDD and EDD information. CDD and EDD information will assist banks in evaluating if the unusual activity is considered suspicious. For additional information, refer to the core overview section, "Customer Due Diligence," pages 63 to 65. External research tools may include widely available Internet media search tools, as well those accessible by subscription. After thorough research and analysis, investigators should document conclusions including any recommendation regarding whether or not to file a SAR.

When multiple departments are responsible for researching unusual activities (i.e., the BSA department researches BSA-related activity and the Fraud department researches fraud-related activity), the lines of communication between the departments must remain open. This allows banks with bifurcated processes to gain efficiencies by sharing information, reducing redundancies, and ensuring all suspicious activity is identified, evaluated, and reported.

If applicable, reviewing and understanding suspicious activity monitoring across the organizations' affiliates, subsidiaries, and business lines may enhance a banking

organization's ability to detect suspicious activity, and thus minimize the potential for financial losses, increased legal or compliance expenses, and reputational risk to the organization. Refer to the expanded overview section, "BSA/AML Compliance Program Structures," pages 160 to 165, for further guidance.

Identifying Underlying Crime

Banks are required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing,[61] and certain other crimes above prescribed dollar thresholds. However, banks are not obligated to investigate or confirm the underlying 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.

SAR Decision Making

After thorough research and analysis has been completed, findings are typically forwarded to a final decision maker (individual or committee). 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. Within those procedures, management should establish a clear and defined escalation process from the point of initial detection to disposition of the investigation.

The decision maker, whether an individual or committee, should have the authority to make the final SAR filing decision. When the bank uses a committee, there should be a clearly defined process to resolve differences of opinion on filing decisions. Banks should document SAR decisions, including the specific reason for filing or not filing a SAR. Thorough documentation provides a record of the SAR decision-making process, including final decisions not to file a SAR. However, due to the variety of systems used to identify, track, and report suspicious activity, as well as the fact that each suspicious activity reporting decision will be based on unique facts and circumstances, no single form of documentation is required when a bank decides not to file.[62]

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

[61] 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: 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.

[62] Bank Secrecy Act Advisory Group, "Section 4 — Tips on SAR Form Preparation & Filing," *The SAR Activity Review — Trends, Tips & Issues*, Issue 10, May 2006, page 38, at www.fincen.gov.

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.[63]

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.[64] This practice will notify law enforcement of the continuing nature of the activity in aggregate. In addition, this practice will 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.

Banks should be aware that law enforcement may have an interest in ensuring that certain accounts remain open notwithstanding suspicious or potential criminal activity in connection with those accounts. If a law enforcement agency requests that a bank maintain a particular account, the bank should ask for a written request. The written request should indicate that the agency has requested that the bank maintain the account and the purpose and duration of the request. Ultimately, the decision to maintain or close an account should be made by a bank in accordance with its own standards and guidelines.[65]

The bank should develop policies, procedures, and processes indicating when to escalate issues or problems identified as the 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 whether and, if so, when to close the account.

---

[63] Refer to Interagency Enforcement Statement (Appendix R) for additional information.

[64] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance," *The SAR Activity Review — Trends, Tips & Issues*, Issue 1, October 2000, page 27 at www.fincen.gov.

[65] Refer to *Requests by Law Enforcement for Financial Institutions to Maintain Accounts,* June 13, 2007, at www.fincen.gov.

- Criteria for when to notify law enforcement, if appropriate.

SAR Completion and Filing

SAR completion and filing are a critical part of the SAR monitoring and reporting process. Appropriate policies, procedures, and processes should be in place to ensure SAR forms are filed in a timely manner, are complete and accurate, and that the narrative provides a sufficient description of the activity reported as well as the basis for filing. Beginning on September 12, 2009, banks that file SARs electronically can receive from FinCEN a Document Control Number as an acknowledgement of receipt for a submitted SAR.[66]

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 facts that may constitute a basis for filing a SAR. If no suspect can be identified, 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.[67]

The phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review. There are a variety of legitimate transactions that could raise a red flag simply because they are inconsistent with an accountholder's normal account activity. For example, a real estate investment (purchase or sale), the receipt of an inheritance, or a gift, may cause an account to have a significant credit or debit that would be inconsistent with typical account activity. The bank's automated account monitoring system or initial discovery of information, such as system-generated reports, may flag the transaction; however, this should not be considered initial detection of potential suspicious activity. The 30-day (or 60-day) period does not begin until an appropriate review is conducted and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR regulation.[68]

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

---

[66] Refer to http://fincen.gov/whatsnew/html/20090826.html for additional information.

[67] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance," *The SAR Activity Review — Trends, Tips & Issues*, Issue 1, October 2000, page 27, at www.fincen.gov.

[68] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance," *The SAR Activity Review — Trends, Tips & Issues*, Issue 10, May 2006, page 44, at www.fincen.gov. For examples of when the date of initial detection occurs, refer to *SAR Activity Review — Trends, Tips, and Issues,* Issue 14, October 2008, page 38 at www.fincen.gov.

review should be completed in a reasonable period of time. What constitutes a "reasonable period of time" will vary according to the facts and circumstances of the particular matter being reviewed and the effectiveness of the SAR monitoring, reporting, and decision-making process of each bank. The key factor is that a bank has established adequate procedures for reviewing and assessing facts and circumstances identified as potentially suspicious, and that those procedures are documented and followed.[69]

For situations requiring immediate attention, in addition to filing a timely SAR, a bank must immediately notify, by telephone, an "appropriate law enforcement authority" and, as necessary, the bank's primary regulator. For this initial notification, an "appropriate law enforcement authority" would generally be the local office of the IRS 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.[70]

SAR Quality

Banks are required to file SAR forms that are complete, thorough, and timely. Banks should include all known subject information on the SAR form. 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 determining 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 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 are included within the SAR form (no attachments to the narrative section can be stored in 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 (e.g., "Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative," November 2003, and "Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting," October 2007) at www.fincen.gov/news_room/rp/sar_guidance.html.

---

[69] *Id*.

[70] For suspicious activity related to terrorist activity, institutions may also call FinCEN's Financial Institution's terrorist hotline at the toll-free number 866-556-3974 (7 days a week, 24 hours a day) to further facilitate the immediate transmittal of relevant information to the appropriate authorities.

Notifying Board of Directors of SAR Filings

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. 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.[71]

SAR Record Retention and Supporting Documentation

Banks must retain copies of SARs and supporting documentation for five years from the date of filing the SAR. Additionally, banks must provide all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or federal banking agency. "Supporting documentation" refers to all documents or records that assisted a bank in making the determination that certain activity required a SAR filing. No legal process is required for disclosure of supporting documentation to FinCEN or an appropriate law enforcement or federal banking agency.[72]

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[73] or federal banking agency, shall decline to produce

---

[71] As noted in the Bank Secrecy Act Advisory Group's *The SAR Activity Review — Trends, Tips & Issues*, 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." Refer to www.fincen.gov.

[72] Refer to *Suspicious Activity Report Supporting Documentation,* June 13, 2007, at www.fincen.gov.

[73] Examples of agencies to which a SAR or the information contained therein could be provided include: the criminal investigative services of the armed forces; the Bureau of Alcohol, Tobacco, and Firearms; an attorney general, district attorney, or state's attorney at the state or local level; the Drug Enforcement Administration; the Federal Bureau of Investigation; the Internal Revenue Service or tax enforcement agencies at the state level; the Office of Foreign Assets Control; a state or local police department; a United States Attorney's Office; Immigration and Customs Enforcement; the U.S. Postal Inspection Service; and the U.S. Secret Service. For additional information, refer to Bank Secrecy Act Advisory Group, "Section 5—Issues and Guidance," *The SAR Activity Review—Trends, Tips & Issues,* Issue 9, October 2005, page 44 at www.fincen.gov.

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.

Sharing SARs With Head Offices and Controlling Companies

Interagency guidance clarifies that banking organizations may share SARs with head offices and controlling companies, whether located in the United States or abroad.[74] A controlling company as defined in the guidance includes:

- A bank holding company (BHC), as defined in section 2 of the BHC Act.
- A savings and loan holding company, as defined in section 10(a) of the Home Owners' Loan Act.
- A company having the power, directly or indirectly, to direct the management policies of an industrial loan company or a parent company or to vote 25 percent or more of any class of voting shares of an industrial loan company or parent company.

The guidance confirms that:

- A U.S. branch or agency of a foreign bank may share a SAR with its head office outside the United States.
- A U.S. bank may share a SAR with controlling companies whether domestic or foreign.

Banks should maintain appropriate arrangements to protect the confidentiality of SARs. The guidance does not address whether a bank may share a SAR with an affiliate other than a controlling company or head office. However, in order to manage risk across an organization, banks that file a SAR may disclose to entities within its organization the information underlying a SAR filing.

---

[74] *Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies*, issued by Financial Crimes Enforcement Network, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and Office of Thrift Supervision, January 20, 2006.

Examination Procedures

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.*

Initially, examiners may elect to "map out" the process the bank follows to monitor for, identify, research, and report suspicious activities. Once the examiner has an understanding of the process, the examiner should follow an alert through the entire process.

Identification of Unusual Activity

1. Review the bank's policies, procedures, and processes for identifying, researching, and reporting suspicious activity. Determine whether they include the following:

   - Lines of communication for the referral of unusual activity to appropriate personnel.
   - Designation of individual(s) responsible for identifying, researching, and reporting suspicious activities.
   - Monitoring systems used to identify unusual activity.
   - Procedures for reviewing and evaluating the transaction activity of subjects included in law enforcement requests (e.g., grand jury subpoenas, section 314(a) requests, or National Security Letters (NSL)) for suspicious activity. NSLs are highly confidential documents; as such, examiners will not review or sample specific NSLs. Instead, examiners should evaluate the policies, procedures, and processes for:
     - Responding to NSLs.
     - Evaluating the account of the target for suspicious activity.
     - Filing SARs, if necessary.
     - Handling account closures.

2. Review the bank's monitoring systems and how the system(s) fits into the bank's overall suspicious activity monitoring and reporting process. Complete the appropriate examination procedures that follow. When evaluating the effectiveness of the bank's monitoring systems, examiners should consider the bank's overall risk profile (higher-risk products, services, customers, entities, and geographic locations), volume of transactions, and adequacy of staffing.

Transaction (Manual Transaction) Monitoring

3. Review the bank's transaction monitoring reports. Determine whether the reports capture all areas that pose money laundering and terrorist financing risks. Examples of these reports include: currency activity reports, funds transfer reports, monetary instrument sales reports, large item reports, significant balance change reports, nonsufficient funds (NSF) reports, and nonresident alien (NRA) reports.

4. Determine whether the bank's transaction monitoring systems use reasonable filtering criteria whose programming has been independently verified. Determine whether the monitoring systems generate accurate reports at a reasonable frequency.

Surveillance (Automated Account) Monitoring

5. Identify the types of customers, products, and services that are included within the surveillance monitoring system.

6. Identify the system's methodology for establishing and applying expected activity or profile filtering criteria and for generating monitoring reports. Determine whether the system's filtering criteria are reasonable.

7. Determine whether the programming of the methodology has been independently validated.

8. Determine that controls ensure limited access to the monitoring system and sufficient oversight of assumption changes.

Managing Alerts

9. Determine whether the bank has policies, procedures, and processes to ensure the timely generation of, review of, and response to reports used to identify unusual activities.

10. Determine whether policies, procedures, and processes require appropriate research when monitoring reports identify unusual activity.

11. Evaluate the bank's 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, and section 314(a) requests) is effectively evaluated.

12. Verify that staffing levels are sufficient to review reports and alerts and investigate items, and that staff possess the requisite experience level and proper investigatory tools. The volume of system alerts and investigations should not be tailored solely to meet existing staffing levels.

13. Determine whether the bank's SAR decision process appropriately considers all available CDD and EDD information.

SAR Decision Making

14. Determine whether the bank's policies, procedures, and processes include procedures for:

    - Documenting decisions not to file a SAR.
    - Escalating issues identified as the result of repeat SAR filings on accounts.
    - Considering closing accounts as a result of continuous suspicious activity.

SAR Completion and Filing

15. Determine whether the bank's policies, procedures, and processes provide for:

    - Completing, filing, and retaining SARs and their supporting documentation.
    - Reporting SARs to the board of directors, or a committee thereof, and informing senior management.
    - Sharing SARs with head offices and controlling companies, as necessary

Transaction Testing

Transaction testing of suspicious activity monitoring systems and reporting processes is intended to determine whether the bank's policies, procedures, and processes are adequate and effectively implemented. Examiners should document the factors they used to select samples and should maintain a list of the accounts sampled. The size and the sample should be based on the following:

- Weaknesses in the account monitoring systems.
- The bank's overall BSA/AML risk profile (e.g., number and type of higher-risk products, services, customers, entities, and geographies).
- Quality and extent of review by audit or independent parties.
- Prior examination findings.
- Recent mergers, acquisitions, or other significant organizational changes.
- Conclusions or questions from the review of the bank's SARs.

Refer to Appendix O ("Examiner Tools for Transaction Testing") for additional guidance.

16. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, sample specific customer accounts to review the following:

    - Suspicious activity monitoring reports.

- CTR download information.
- Higher-risk banking operations (products, services, customers, entities, and geographies).
- Customer activity.
- Subpoenas received by the bank.
- Decisions not to file a SAR.

17. For the customers selected previously, obtain the following information, if applicable:
    - CIP and account-opening documentation.
    - CDD documentation.
    - Two to three months of account statements covering the total customer relationship and showing all transactions.
    - Sample items posted against the account (e.g., copies of checks deposited and written, debit or credit tickets, and funds transfer beneficiaries and originators).
    - Other relevant information, such as loan files and correspondence.
18. Review the selected accounts for unusual activity. If the examiner identifies unusual activity, review customer information for indications that the activity is typical for the customer (i.e., the sort of activity in which the customer is normally expected to engage). When reviewing for unusual activity, consider the following:
    - For individual customers, whether the activity is consistent with CDD information (e.g., occupation, expected account activity, and sources of funds and wealth).
    - For business customers, whether the activity is consistent with CDD information (e.g., type of business, size, location, and target market).
19. Determine whether the transaction or surveillance suspicious activity monitoring system detected the activity that the examiner identified as unusual.
20. For transactions identified as unusual, discuss the transactions with management. Determine whether the account officer demonstrates knowledge of the customer and the unusual transactions. After examining the available facts, determine whether management knows of a reasonable explanation for the transactions.
21. Determine whether the bank has failed to identify any reportable suspicious activity.
22. From the results of the sample, determine whether the transaction or surveillance suspicious activity monitoring system effectively detects unusual or suspicious activity. Identify the underlying cause of any deficiencies in the monitoring systems (e.g., inappropriate filters, insufficient risk assessment, or inadequate decision making).

23. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of management's research decisions to determine the following:

    - Whether management decisions to file or not file a SAR are supported and reasonable.
    - Whether documentation is adequate.
    - Whether the decision process is completed and SARs are filed in a timely manner.

24. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, sample the SARs downloaded from the BSA reporting database or the bank's internal SAR records. Review the quality of SAR content to assess the following:

    - SARs contain accurate information.
    - SAR narratives are complete and thorough, and clearly explain why the activity is suspicious.
    - If SAR narratives from the BSA reporting database are blank or contain language, such as "see attached," ensure that the bank is not mailing attachments to the IRS Enterprise Computing Center — Detroit (formerly the Detroit Computing Center).[75]

25. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with monitoring, detecting, and reporting suspicious activity.

[75] The IRS Enterprise Computing Center — Detroit's toll-free number is 800-800-2877.

Currency Transaction Reporting — Overview

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

A bank must file a Currency Transaction Report (CTR) (FinCEN Form 104) for each transaction in currency[76] (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," pages 90 to 94, for further guidance.

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 (IRA), 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 electronically). The bank must retain copies of CTRs for five years from the date of the report (31 CFR 103.27(a)(3)).

CTR Backfiling

If a bank has failed to file CTRs on reportable transactions, the bank should begin filing CTRs and should contact the IRS Enterprise Computing Center — Detroit (formerly the

[76] 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.

Detroit Computing Center)[77] to request a determination on whether the backfiling of unreported transactions is necessary.

[77] The IRS Enterprise Computing Center – Detroit's toll-free number is 800-800-2877.

Examination Procedures

Currency Transaction Reporting

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

1. Determine whether the bank's policies, procedures, and processes adequately address the preparation, filing, and retention of CTRs (FinCEN Form 104).

2. Review correspondence that the bank has received from the IRS Enterprise Computing Center – Detroit (formerly the Detroit Computing Center) relating to incorrect or incomplete CTRs (errors). Determine whether management has taken corrective action, when necessary.

3. Review the currency transaction system (e.g., how the bank identifies transactions applicable for the filing of a CTR). Determine whether the bank aggregates all or some currency transactions within the bank. Determine whether the bank aggregates transactions by taxpayer identification number (TIN), individual taxpayer identification number (ITIN), employer identification number (EIN), or customer information file (CIF) number. Also, evaluate how CTRs are filed on customers with missing TINs or EINs.

Transaction Testing

4. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of filed CTRs (hard copy or from computer-generated filings) to determine whether:

   - CTRs are completed in accordance with FinCEN instructions.

   - CTRs are filed for large currency transactions identified by tellers' cash proof sheets, automated large currency transaction systems, or other types of aggregation systems that cover all relevant areas of the bank, unless an exemption exists for the customer.

   - CTRs are filed accurately and completely within 15 calendar days after the date of the transaction (25 days if filed electronically).

   - The bank's independent testing confirms the integrity and accuracy of the MIS used for aggregating currency transactions. If not, the examiner should confirm the integrity and accuracy of the MIS. The examiner's review should confirm that tellers do not have the capability to override currency aggregation systems.

   - Discrepancies exist between the bank's records of CTRs and the CTRs reflected in the download from the BSA reporting database.

- The bank retains copies of CTRs for five years from the date of the report (31 CFR 103.27(a)(3)).

5. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with currency transaction reporting.

Currency Transaction Reporting Exemptions — Overview

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

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 listed public 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.

On December 5, 2008, FinCEN issued amendments to the rules governing CTR exemptions.[78] The amendments, among other things, removed the initial designation and annual review requirements for certain Phase I customers, the biennial filing requirement for Phase II exempt customers, and eliminated the waiting period for exempting otherwise eligible Phase II customers by adopting a risk-based approach to exempting those customers. The following discussion reflects the updated regulatory requirements.

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 or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange or have been designated as a NASDAQ National Market Security listed on the NASDAQ Stock Market (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 or analogous equity interest is owned by the listed entity.

[78] Refer to 73 Fed. Reg. 74010 (December 5, 2008).

Filing Time Frames

Banks must file a one-time Designation of Exempt Person form (FinCEN Form 110) to exempt each eligible listed public company or eligible subsidiary from currency transaction reporting. The form must be filed with the IRS within 30 days after the first transaction in currency that the bank wishes to exempt.

Banks do not need to file a Designation of Exempt Person form for Phase I-eligible customers that are banks, federal, state, or local governments, or entities exercising governmental authority. Nevertheless, a bank should take the same steps to assure itself of a customer's initial eligibility for exemption, and document the basis for the conclusion, that a reasonable and prudent bank would take to protect itself from loan or other fraud or loss based on misidentification of a person's status. Exemption of a Phase I entity covers all transactions in currency with the exempted entity, not only transactions in currency conducted through an account.

Annual Review

The information supporting each designation of a Phase I-exempt listed public company or subsidiary must be reviewed and verified by the bank at least once per year. Annual reports, stock quotes from newspapers, or other information, such as electronic media could be used to document the review. Banks do not need to confirm the continued exemption eligibility of Phase I customers that are banks, government agencies, or entities exercising governmental authority.

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 two months or prior to the passing of two months' time if the bank undertakes a risk-based analysis of that customer that allows it to form and document a reasonable belief that the customer has a legitimate business purpose for conducting frequent large currency transactions; (ii) frequently[79] 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

[79] FinCEN has noted that, for purposes of 31 CFR 103.22(d)(2)(vi)(B): "[Banks] may designate an otherwise eligible customer for Phase II exemption after the customer has within a year conducted five or more reportable cash transactions." Refer to 73 Fed. Reg. 74010, 74014 (December 5, 2008).

States or a state, or is registered as and 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)(5)(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 a 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.
- 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[80] are derived from one or more of the ineligible business activities listed in the rule.

A bank must consider and maintain materials and other supporting information that allow it to substantiate that the decision to exempt the customer from currency transaction

[80] 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. Refer to FinCEN Ruling 2002-1, www.fincen.gov.

reporting was based upon a reasonable determination that the customer derives no more than 50 percent of its annual gross revenues from ineligible business activities. Such a reasonable determination should be based upon its understanding of the nature of the customer's business, the purpose of the customer's accounts, and the actual or anticipated activity in those accounts.[81]

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 two months or prior to the passing of two months' time if the bank undertakes a risk-based analysis of that customer that allows it to form and document a reasonable belief that the customer has a legitimate business purpose for conducting frequent large currency transactions; (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 a Designation of Exempt Person form with the IRS within 30 days after the first transaction in currency that the bank plans 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. The bank should document the annual review. 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.

Safe Harbor for Failure to File CTRs

The rules (31 CFR 103.22(d)(7)) 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

[81] For additional details, refer to Guidance on Supporting Information Suitable for Determining the Portion of a Business Customer's Annual Gross Revenues that is Derived from Activities Ineligible for Exemption from Currency Transaction Reporting Requirements (FIN-2009-G001) (April 27, 2009), at www.fincen.gov.

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 have any effect on the requirement that banks file SARs or on other recordkeeping requirements. 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, it may formally revoke the exemption by filing FinCEN Form 110 and checking the "Exemption Revoked" box or informally revoke the exemption by filing CTRs on the customer. In either case, the bank should begin filing CTRs and should contact the IRS Enterprise Computing Center — Detroit (formerly the Detroit Computing Center)[82] to request a determination on whether the backfiling of unreported currency transactions is necessary.

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

[82] The IRS Enterprise Computing Center — Detroit's toll-free number is 800-800-2877.

Examination Procedures

Currency Transaction Reporting Exemptions

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

1. Determine whether the bank uses the Currency Transaction Report (CTR) exemption process. If yes, determine whether the policies, procedures, and processes for CTR exemptions are adequate.

Phase I Exemptions (31 CFR 103.22(d)(2)(i)–(v))

2. Determine whether the bank files the Designation of Exempt Person form (FinCEN Form 110) with the IRS to exempt eligible listed public companies and their subsidiaries from CTR reporting as defined in 31 CFR 103.22. The form should be filed within 30 days of the first reportable transaction that was exempted.

3. Assess whether ongoing and reasonable due diligence is performed, including required annual reviews to determine whether a listed public company or subsidiary remains eligible for designation as an exempt person under the regulatory requirements. Management should properly document exemption determinations (e.g., with stock quotes from newspapers and consolidated returns for the entity).

Phase II Exemptions (31 CFR 103.22(d)(2)(vi)–(vii))

Under the regulation, the definition of exempt persons includes "non-listed businesses" and "payroll customers" as defined in 31 CFR 103.22(d)(2)(vi)–(vii). Nevertheless, several businesses remain ineligible for exemption purposes; refer to 31 CFR 103.22(d)(5)(viii) and the "Currency Transaction Reporting Exemptions — Overview" section of this manual.

4. Determine whether the bank files a Designation of Exempt Person form with the IRS to exempt a customer, as identified by management, from CTR reporting.

5. Determine whether the bank maintains documentation to support that the "non-listed businesses" it has designated as exempt from CTR reporting do not receive more than 50 percent of gross revenue from ineligible business activities.

6. Assess whether ongoing and reasonable due diligence is performed, including required annual reviews, to determine whether a customer is eligible for designation as exempt from CTR reporting. Customers must meet the following requirements to be eligible for exemption under the regulation:

- Have frequent[83] currency transactions in excess of $10,000 (regular withdrawals to pay domestic employees in currency in the case of a payroll customer).
- Be incorporated or organized under the laws of the United States or a state, or registered as and eligible to do business within the United States or a state.
- Maintain a transaction account at the bank for at least two months (or prior to the passing of two months' time if the bank has conducted a risk-based analysis of a customer that allows it to form and document a reasonable belief that the customer has a legitimate business purpose for conducting frequent large currency transactions).

Transaction Testing

7. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of Designation of Exempt Person forms from the bank to test compliance with the regulatory requirements (e.g., only eligible businesses are exempted and adequate supporting documentation is maintained).
8. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with currency transaction reporting exemptions.

---

[83] FinCEN has noted that when interpreting the term "frequently" for purposes of 31 CFR 103.22(d)(2)(vi)(B): "[Banks] may designate an otherwise eligible customer for Phase II exemption after the customer has within a year conducted five or more reportable cash transactions." Refer to 73 Fed. Reg. 74010, 74014 (December 5, 2008).

Information Sharing — Overview

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).*

On September 26, 2002, final regulations (31 CFR 103.100 and 31 CFR 103.110) implementing section 314 of the USA PATRIOT Act became effective. The regulations established procedures for information sharing to deter money laundering and terrorist activity. On February 5, 2010, FinCEN amended the regulations to allow state, local, and certain foreign law enforcement agencies access to the information sharing program.[84]

Information Sharing Between Law Enforcement and Financial Institutions — Section 314(a) of the USA PATRIOT Act (31 CFR 103.100)

A federal, state, local, or foreign[85] 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.

Search Requirements

Upon receiving an information request,[86] 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

[84] Refer to 75 Fed. Reg. 6560 (February 10, 2010).

[85] A foreign law enforcement agency must come from a jurisdiction that is a party to the Agreement on Mutual Legal Assistance between the United States and the European Union. *Id.* at 6560-61.

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

positive matches to FinCEN within 14 days, unless otherwise specified in the information request.

In March 2005, FinCEN began posting section 314(a) subject lists through the Web-based 314(a) Secure Information Sharing System. Every two weeks, or more frequently if an emergency request is transmitted, the financial institution's designated point(s) of contact will receive notification from FinCEN that there are new postings to FinCEN's secure Web site. The point of contact will be able to access the current section 314(a) subject list (and one prior) and download the files in various formats for searching. Financial institutions should report all positive matches via the Secure Information Sharing System (SISS). As of June 2, 2008, FinCEN has suspended the transmission by facsimile of section 314(a) subject lists to financial institutions. Financial institutions to which FinCEN ceased transmitting section 314(a) subject lists by facsimile that obtain Internet access should take steps to begin receiving section 314(a) subject lists through the SISS.

FinCEN has provided financial institutions with General Instructions and Frequently Asked Questions (FAQ) 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.[87] The General Instructions or FAQs are made available to the financial institutions on the SISS.[88]

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 the 314(a) subject lists 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.

According to the FAQs available on the SISS, if a financial institution receiving 314(a) subject lists through the SISS fails to perform or complete searches on one or more information request received during the previous 12 months, it must immediately obtain these prior requests from FinCEN and perform a retroactive search of its records.[89] A

---

[87] For example, regarding funds transfers, the "General Instructions" state that, unless the instructions to a specific 314(a) request state otherwise, banks are required to search funds transfer records maintained pursuant to 31 CFR 103.33, to determine whether the named subject was an originator/transmittor of a funds transfer for which the bank was the originator/transmittor's financial institution, or a beneficiary/recipient of a funds transfer for which the bank was the beneficiary/recipient's financial institution.

[88] The General Instructions and FAQs also can be obtained by contacting FinCEN toll-free at 800-949-2732.

[89] The financial institution should contact FinCEN's 314 Program Office via e-mail at sys314a@fincen.gov to obtain prior information requests. If the financial institution discovers a positive match while performing a retroactive search, it should contact the 314 Program Office toll-free at 800-949-2732 and select option 2. Financial institutions must respond with positive matches within 14 days of receiving a

financial institution is not required to perform retroactive searches in connection with information sharing requests that were transmitted more than 12 months before the date upon which it discovers that it failed to perform or complete searches on prior information requests. Additionally, in performing retroactive searches a financial institution is not required to search records created after the date of the original information request.

Use Restrictions and Confidentiality

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)). 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) subject 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) subject lists are not permanent "watch lists." In fact, section 314(a) subject 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) subject list should not be the sole factor used to determine whether to file a SAR. Financial institutions should establish a process for determining when and if a SAR should be filed. Refer to the core overview section, "Suspicious Activity Reporting," pages 67 to 80, for additional guidance.

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 banking regulator, or the 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 points of contact 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) subject list to respond to requests. However, the section 314(a) subject lists cannot be shared with

---

prior information request; however, if a retroactive search results in no positive matches then no further action is required.

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.

Documentation

Additionally, documentation that all required searches were performed is essential. For those 314(a) subject lists received via facsimile prior to June 2, 2008, a bank may maintain copies of the cover page of the request with a financial institution sign-off that the records were checked, the date of the search, and search results (e.g., positive or negative). For positive matches with subject lists received via facsimile, copies of the form returned to FinCEN and the supporting documentation should be retained. For those institutions utilizing the Web-based 314(a) SISS, banks may print a search self-verification document for each 314(a) subject list transmission. Additionally, a Subject Response List can be printed for documentation purposes. The Subject Response List displays the total number of positive responses submitted to FinCEN for that transmission, the transmission date, the submitted date, and the tracking number and subject name that had the positive hit. 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.

FinCEN regularly updates a list of recent search transmissions, including information on the date of transmission, tracking number, and number of subjects listed in the transmission.[90] Bankers and examiners may review this list to verify that search requests have been received. Each bank should contact its primary federal regulator for guidance to ensure it obtains the section 314(a) subject list and for updating contact information.[91]

---

[90] This list, titled "Law Enforcement Information Sharing with the Financial Industry," is available on the "Section 314(a)" page of FinCEN's Web site. The list contains information on each search request transmitted since January 4, 2005, and is updated after each transmission.

[91] Refer to the FinCEN Web site at www.fincen.gov/statutes_regs/patriot/pdf/poc_change_314a.pdf for section 314(a) contacts for each primary regulator.

Voluntary Information Sharing — Section 314(b) of the USA PATRIOT Act (31 CFR 103.110)

Section 314(b) encourages financial institutions[92] 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.[93] 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 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.[94] 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 (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

---

[92] 31 CFR 103.110 generally defines "financial institution" as any financial institution described in 31 USC 5312(a)(2) that is required to establish and maintain an AML compliance program.

[93] FinCEN has indicated that a financial institution participating in the section 314(b) program may share information relating to transactions that the institution suspects may involve the proceeds of one or more specified unlawful activities ("SUAs") and such an institution will still remain within the protection of the section 314(b) safe harbor from liability. Information related to the SUAs may be shared appropriately within the 314(b) safe harbor to the extent that the financial institution suspects that the transaction may involve the proceeds of one or more SUAs and the purpose of the permitted information sharing under the 314(b) rule is to identify and report activities that the financial institution suspects may involve possible terrorist activity or money laundering. Refer to *Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act,* FIN-2009-G002 (June 16, 2009) at www.fincen.gov.

[94] Instructions on submitting a notification form (initial or renewal) are available on FinCEN's Web site at www.fincen.gov.

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 transaction 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.

Examination Procedures

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).*

Information Sharing Between Law Enforcement and Financial Institutions (Section 314(a))

1. Verify that the financial institution is currently receiving section 314(a) requests from FinCEN or from an affiliated financial institution that serves as the subject financial institution's point of contact. If the financial institution is not receiving information requests[95] or contact information changes, the financial institution should update its contact information with its primary regulator in accordance with the instructions at www.fincen.gov.

2. Verify that the financial institution has sufficient policies, procedures, and processes to document compliance; maintain sufficient internal controls; provide ongoing training; and independently test its compliance with 31 CFR 103.100, which implements section 314(a) of the USA PATRIOT Act. At a minimum, the procedures should accomplish the following:

   - Designate a point of contact for receiving information requests.
   - Ensure that the confidentiality of requested information is safeguarded.
   - Establish a process for responding to FinCEN's requests.
   - Establish a process for determining if and when a SAR should be filed.

3. Determine whether the search policies, procedures, and processes the financial institution uses to respond to section 314(a) requests are comprehensive and cover all records identified in the General Instructions for such requests. The General Instructions include searching accounts maintained by the named subject during the preceding 12 months and transactions conducted within the last six months. Financial institutions have 14 days from the transmission date of the request to respond to a section 314(a) Subject Information Form.

4. If the financial institution uses a third-party vendor to perform or facilitate searches, determine whether an agreement or procedures are in place to ensure confidentiality.

[95] As of June 2, 2008, FinCEN has suspended the transmission by facsimile of section 314(a) subject lists to financial institutions. Financial institutions to which FinCEN ceased transmitting section 314(a) subject lists by facsimile that obtain Internet access should take steps to begin receiving section 314(a) subject lists via the Web-based 314(a) Secure Information Sharing System.

5. Review the financial institution's internal controls and determine whether its documentation to evidence compliance with section 314(a) requests is adequate. This documentation could include, for example, the following:

   - Copies of section 314(a) requests.
   - A log that records the tracking numbers and includes a sign-off column.
   - For 314(a) subject lists received via facsimile prior to June 2, 2008, copies of the cover page of the requests, with a financial institution sign-off, that the records were checked, the date of the search, and search results (e.g., positive or negative).
   - Copies of SISS-generated search self-verification documents.
   - For positive matches, copies of the form returned to FinCEN (e.g., SISS-generated Subject Response Lists) and the supporting documentation should be retained.

Voluntary Information Sharing (Section 314(b))

6. Determine whether the financial institution has decided to share information voluntarily. If so, verify that the financial institution has filed a notification form with FinCEN and provides an effective date for the sharing of information that is within the previous 12 months.

7. Verify that the financial institution has policies, procedures, and processes for sharing information and receiving shared information, as specified under 31 CFR 103.110, (which implements section 314(b) of the USA PATRIOT Act).

8. Financial institutions that choose to share information voluntarily should have policies, procedures, and processes to document compliance; maintain adequate internal controls; provide ongoing training; and independently test its compliance with 31 CFR 103.110. At a minimum, the procedures should:

   - Designate a point of contact for receiving and providing information.
   - Ensure the safeguarding and confidentiality of information received and information requested.
   - Establish a process for sending and responding to requests, including ensuring that other parties with whom the financial institution intends to share information (including affiliates) have filed the proper notice.
   - Establish procedures for determining whether and when a SAR should be filed.

9. If the financial institution is sharing information with other entities and is not following the procedures outlined in 31 CFR 103.110(b), notify the examiners reviewing the privacy rules.

10. Through a review of the financial institution's documentation (including account analysis) on a sample of the information shared and received, evaluate how the financial institution determined whether a SAR was warranted. The financial institution is not required to file SARs solely on the basis of information obtained through the voluntary information sharing process. In fact, the information obtained through the voluntary information sharing process may enable the financial institution to determine that no SAR is required for transactions that may have initially appeared suspicious. The financial institution should have considered account activity in determining whether a SAR was warranted.

Transaction Testing

11. On the basis of a risk assessment, prior examination reports, and a review of the financial institution's audit findings, select a sample of positive matches or recent requests to determine whether the following requirements have been met:

    - The financial institution's policies, procedures, and processes enable it to search all of the records identified in the General Instructions for section 314(a) requests. Such processes may be electronic, manual, or both.

    - The financial institution searches appropriate records for each information request received. For positive matches:

        – Verify that a response was provided to FinCEN within the designated time period (31 CFR 103.100(b)(2)(ii)).

        – Review the financial institution's documentation (including account analysis) to evaluate how the financial institution determined whether a SAR was warranted. Financial institutions are not required to file SARs solely on the basis of a match with a named subject; instead, account activity should be considered in determining whether a SAR is warranted.

    - The financial institution uses information only in the manner and for the purposes allowed and keeps information secure and confidential (31 CFR 103.100(b)(2)(iv)). (This requirement can be verified through discussions with management.)

12. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with information sharing.

Purchase and Sale of Monetary Instruments Recordkeeping — Overview

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.*

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, Medicare, or 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[96] 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.
  - Dollar amounts of each of the instruments purchased in currency.
  - Specific identifying information, if applicable.[97]

---

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

[97] 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

- 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.

---

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.

Examination Procedures

Purchase and Sale of Monetary Instruments Recordkeeping

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.*

1. Determine whether the bank maintains the required records (in a manual or an automated system) for sales of bank checks or drafts including foreign drafts, cashier's checks, money orders, and traveler's checks for currency in amounts between $3,000 and $10,000, inclusive, to purchasers who have deposit accounts with the bank.

2. Determine whether the bank's policies, procedures, and processes permit currency sales of monetary instruments to purchasers who do not have deposit accounts with the bank (nondepositors):

   - If so, determine whether the bank maintains the required records for sales of monetary instruments to nondepositors.

   - If not permitted, determine whether the bank allows sales on an exception basis.

Transaction Testing

3. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of monetary instruments sold for currency in amounts between $3,000 and $10,000, inclusive, to determine whether the bank obtains, verifies, and retains the required records to ensure compliance with regulatory requirements.

4. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with the purchase and sale of monetary instruments.

5. On the basis of the previous conclusion and the risks associated with the bank's activity in this area, proceed to expanded examination procedures, if necessary.

Funds Transfers Recordkeeping — Overview

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

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).[98] The rule requires each bank involved in funds transfers[99] to collect and retain certain information in connection with funds transfers of $3,000 or more.[100] 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).[101] The requirements may also vary depending on whether an originator or beneficiary is an 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).[102] This requirement is commonly referred to as the "Travel Rule."

---

[98] 31 CFR 103.33(e) is the recordkeeping rule for banks, and 31 CFR 103.33(f) imposes similar requirements for nonbank financial institutions that engage in funds transfers. The procedures in this core overview section address only the rules for banks in 31 CFR 103.33(e).

[99] 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 31 CFR 103.33(e), (f) and (g).

[100] 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.

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

[102] The rule applies to both banks and nonbanks (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

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 Recordkeeping Requirements for Nonestablished Customers

If the originator is not an established customer of the bank, the originator's bank must 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.
- Number of the identification document (e.g., driver's license).

"transmittor's financial institution" instead of "originating bank." The broader terms include the bank-specific terms.

- 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 whom 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.

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,[103] 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[104] on file and the address information is retrievable upon request by law enforcement.

---

[103] 68 Fed. Reg. 66708 (November 23, 2003).

[104] Consistent with 31 CFR 103.121, an "address" for purposes of the Travel Rule is as follows: for an individual, "address" 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 31 CFR 103.121 applies 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 31 CFR 103.121.

Examination Procedures

Funds Transfers Recordkeeping

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

1. Verify that the bank obtains and maintains appropriate records for compliance with 31 CFR 103.33(e).

2. Verify that the bank transmits payment information as required by 31 CFR 103.33(g) (the "Travel Rule").

3. Verify that the bank files CTRs when currency is received or dispersed in a funds transfer that exceeds $10,000 (31 CFR 103.22).

4. If the bank sends or receives funds transfers to or from institutions in other countries, especially those with strict privacy and secrecy laws, assess whether the bank has policies, procedures, and processes to determine whether amounts, the frequency of the transfer, and countries of origin or destination are consistent with the nature of the business or occupation of the customer.

Transaction Testing

5. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of funds transfers processed as an originator's bank, an intermediary bank, and a beneficiary's bank to ensure the institution collects, maintains, or transmits the required information, depending on the institution's role in the transfer.

6. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with funds transfers.

7. On the basis of the previous conclusion and the risks associated with the bank's activity in this area, proceed to expanded examination procedures, if necessary.

Foreign Correspondent Account Recordkeeping and Due Diligence — Overview

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 examination procedures regarding specific money laundering risks associated with foreign correspondent accounts.*

One of the central goals of the USA 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 USA PATRIOT Act prohibits accounts with foreign shell banks. Foreign correspondent accounts, as noted in past U.S. Senate investigative reports,[105] 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 USA PATRIOT Act and by the implementing regulations at 31 CFR 103.175, 103.176, 103.177, and 103.185. Additional discussions and procedures regarding specific money laundering risks for foreign correspondent banking activities, such as bulk shipments of currency, pouch activity, U.S. dollar drafts, and payable through accounts, are included in the expanded sections.

Foreign Shell Bank Prohibition and Foreign Correspondent Account Recordkeeping

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, or to make payments or other disbursements on behalf of the 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)). Accounts maintained by foreign banks for financial institutions covered by the rule are not "correspondent accounts" subject to this regulation.[106]

---

[105] *Correspondent Banking: A Gateway for Money Laundering*. Refer to Senate Hearing 107-84. The report appears on page 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.

[106] 71 Fed. Reg. 499. FinCEN has issued interpretive guidance, *Application of Correspondent Account Rules to the Presentation of Negotiable Instruments Received by a Covered Financial Institution for Payment*, FIN-2008-G001 (January 30, 2008), found at www.fincen.gov, which states, "In the ordinary course of business, a covered financial institution may receive negotiable instruments for payment from a

Under 31 CFR 103.177, a bank is prohibited from establishing, maintaining, 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.[107] An exception, however, permits a bank to maintain a correspondent account for a foreign shell bank that is a regulated affiliate.[108] 31 CFR 103.177 also requires that a bank take reasonable steps to ensure that any correspondent account established, maintained, administered, or managed in the United States for a foreign bank is not being used by that foreign bank 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.[109] 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.[110] 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.

---

foreign financial institution with which it maintains a correspondent relationship . . . FinCEN does not view the transaction-by-transaction presentation of a negotiable instrument to a foreign paying institution—either directly or through a clearing facility — to be the establishment of a formal banking or business relationship by a covered financial institution for purposes of complying with the correspondent account rule."

[107] "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.

[108] 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.

[109] 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.

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

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 bank and receives a recertification on or before the three-year anniversary of the execution of the initial or previous certification.[111]

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 the bank must 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 USA 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

[111] Refer to FinCEN Guidance FIN-2006-G003, *Frequently Asked Questions, Foreign Bank Recertifications under 31 CFR 103.177*, February 3, 2006, at www.fincen.gov.

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 (31 USC 5318(k)(2)).

Special Due Diligence Program for Foreign Correspondent Accounts

Section 312 of the USA PATRIOT Act added subsection (i) to 31 USC 5318 of the BSA. This subsection requires each U.S. financial institution that establishes, maintains, administers, or manages a correspondent account in the United States for a foreign financial institution to take certain AML measures for such accounts. In addition, section 312 of the USA PATRIOT Act specifies additional standards for correspondent accounts maintained for certain foreign banks.

On January 4, 2006, FinCEN published a final regulation (31 CFR 103.176) implementing the due diligence provisions of 31 USC 5318(i)(1). Subsequently, on August 9, 2007, FinCEN published an amendment to that final regulation, implementing the EDD provisions of 31 USC 5318(i)(2) with respect to correspondent accounts established or maintained for certain foreign banks.

General Due Diligence

31 CFR 103.176(a) requires banks to establish a due diligence program that includes appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures, and controls that are reasonably designed to enable the bank to detect and report, on an ongoing basis, any known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed by the bank in the United States for a foreign financial institution[112] ("foreign correspondent account").

[112] The term "foreign financial institution" as defined in 31 CFR 103.175(h) generally includes:

- A foreign bank.
- A foreign branch or office of a U.S. bank, broker/dealer in securities, futures commission merchant, introducing broker, or mutual fund.

Due diligence policies, procedures, and controls must include each of the following:

- Determining whether each such foreign correspondent account is subject to EDD (refer to "Enhanced Due Diligence" below).
- Assessing the money laundering risks presented by each such foreign correspondent account.
- Applying risk-based procedures and controls to each such foreign correspondent account reasonably designed to detect and report known or suspected money laundering activity, including a periodic review of the correspondent account activity sufficient to determine consistency with information obtained about the type, purpose, and anticipated activity of the account.

Risk assessment of foreign financial institutions. A bank's general due diligence program must 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 bank's due diligence program should provide for the risk assessment of foreign correspondent accounts considering all relevant factors, including, as appropriate:

- The nature of the foreign financial institution's business and the markets it serves.
- The type, purpose, and anticipated activity of the foreign correspondent 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).
- The AML and supervisory regime of the jurisdiction that issued the charter or license to the foreign financial institution and, to the extent that information regarding such jurisdiction is reasonably available, of the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered.
- 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.

Banks are not required to evaluate all of the above factors for every correspondent account.

Monitoring of foreign correspondent accounts. As part of ongoing due diligence, banks should periodically review their foreign correspondent accounts. Monitoring will not, in the ordinary situation, involve scrutiny of every transaction taking place within the

---

- Any other person organized under foreign law that, if located in the United States, would be a broker/dealer in securities, futures commission merchant, introducing broker, or mutual fund.
- Any person organized under foreign law that is engaged in the business of, and is readily identifiable as, a currency dealer or exchanger or a money transmitter.

account, but, instead, should involve a review of the account sufficient to ensure that the bank can determine whether the nature and volume of account activity is generally consistent with information regarding the purpose of the account and expected account activity and to ensure that the bank can adequately identify suspicious transactions.

An effective due diligence program will provide for a range of due diligence measures, based upon the bank's risk assessment of each foreign correspondent account. The starting point for an effective due diligence program, therefore, should be a stratification of the money laundering risk of each foreign correspondent account based on the bank's review of relevant risk factors (such as those identified above) to determine which accounts may require increased measures. The due diligence program should identify risk factors that would warrant the institution conducting additional scrutiny or increased monitoring of a particular account. As due diligence is an ongoing process, a bank should take measures to ensure account profiles are current and monitoring should be risk-based. Banks should consider whether risk profiles should be adjusted or suspicious activity reported when the activity is inconsistent with the profile.

Enhanced Due Diligence

31 CFR 103.176(b) requires banks to establish risk-based EDD policies, procedures, and controls when establishing, maintaining, administering, or managing a correspondent account in the United States for certain foreign banks (as identified in 31 CFR 103.176(c)) operating under any one or more of the following:

- An offshore banking license.[113]
- A banking license issued by a foreign country that has been designated as noncooperative with international AML principles or procedures by an intergovernmental group or organization of which the United States is a member, and with which designation the United States representative to the group or organization concurs.[114]
- 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.

If such an account is established or maintained, 31 CFR 103.176(b) requires the bank to establish EDD policies, procedures, and controls to ensure that the bank, at a minimum, takes reasonable steps to:

---

[113] The USA PATRIOT Act (31 USC 5318(i)(4)(A) and 31 CFR 103.175(k)) define 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, or in the local currency of, the jurisdiction that issued the license.

[114] The Financial Action Task Force (FATF) is the only intergovernmental organization of which the United States is a member that has designated countries as noncooperative with international anti-money laundering principles. The United States has concurred with all FATF designations to date.

- Determine, 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.[115]

- Conduct enhanced scrutiny of such account to guard against money laundering and to identify and report any suspicious transactions in accordance with applicable laws and regulations. This enhanced scrutiny is to reflect the risk assessment of the account and shall include, as appropriate:

  - Obtaining and considering information relating to the foreign bank's anti-money laundering program to assess the risk of money laundering presented by the foreign bank's correspondent account.

  - Monitoring transactions to, from, or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity.

  - Obtaining information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable through account, and the sources and the beneficial owner of funds or other assets in the payable through account.

- Determine whether the foreign bank for which the correspondent account is maintained in turn maintains correspondent accounts for other foreign banks that use the foreign bank's correspondent account and, if so, take reasonable steps to obtain information relevant to assess and mitigate money laundering risks associated with the foreign bank's correspondent accounts for other foreign banks, including, as appropriate, the identity of those foreign banks.

In addition to those categories of foreign banks identified in the regulation as requiring EDD, banks may find it appropriate to conduct additional due diligence measures on foreign financial institutions identified through application of the bank's general due diligence program as posing a higher risk for money laundering. Such measures may include any or all of the elements of EDD set forth in the regulation, as appropriate for the risks posed by the specific foreign correspondent account.

As also noted in the above section on general due diligence, a bank's resources are most appropriately directed at those accounts that pose a more significant money laundering risk. Accordingly, where a bank is required or otherwise determines that it is necessary to conduct EDD in connection with a foreign correspondent account, the bank may consider the risk assessment factors discussed in the section on general due diligence when determining the extent of the EDD that is necessary and appropriate to mitigate the risks presented. In particular, the anti-money laundering and supervisory regime of the

[115] An "owner" is any person who directly or indirectly owns, controls, or has the power to vote 10 percent or more of any class of securities of a foreign bank (31 CFR 103.176(b)(3)). "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)) (31 CFR 103.176(b)(3)).

jurisdiction that issued a charter or license to the foreign financial institution may be especially relevant in a bank's determination of the nature and extent of the risks posed by a foreign correspondent account and the extent of the EDD to be applied.

Special Procedures When Due Diligence Cannot Be Performed

A bank's due diligence policies, procedures, and controls established pursuant to 31 CFR 103.176 must include procedures to be followed in circumstances when appropriate due diligence or EDD cannot be performed with respect to a foreign correspondent account, including when the bank should:

- Refuse to open the account.
- Suspend transaction activity.
- File a SAR.
- Close the account.

Examination Procedures

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 examination procedures regarding specific money laundering risks associated with foreign correspondent accounts.*

1. Determine whether the bank engages in foreign correspondent banking.

Foreign Shell Bank Prohibition and Foreign Correspondent Account Recordkeeping

2. If so, review the bank's policies, procedures, and processes. At a minimum, policies, procedures, and processes should accomplish the following:
   - Prohibit dealings with foreign shell banks and specify the responsible party for obtaining, updating, and managing certifications or information for foreign correspondent accounts.
   - Identify foreign correspondent accounts and address the sending, tracking, receiving, and reviewing of certification requests or requests for information.
   - Evaluate the quality of information received in responses to certification requests or requests for information.
   - Determine whether and when a SAR should be filed.
   - Maintain sufficient internal controls.
   - Provide for ongoing training.
   - Independently test the bank's compliance with 31 CFR 103.177.
3. Determine whether the bank has on file a current certification or current information (that would otherwise include the information contained within a certification) for each foreign correspondent account to determine whether the foreign correspondent is not a foreign shell bank (31 CFR 103.177(a)).
4. If the bank has foreign branches, determine whether the bank has taken reasonable steps to ensure that any correspondent accounts maintained for its foreign branches are not used to indirectly provide banking services to a foreign shell bank.

Special Due Diligence Program for Foreign Correspondent Accounts

5. Determine whether the bank has established a general due diligence program that includes appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures, and controls for correspondent accounts established, maintained, administered, or managed in the United States for foreign financial institutions ("foreign correspondent account"). The general due diligence program must be applied to each foreign correspondent account. Verify that due diligence policies, procedures, and controls include:

   - Determining whether any foreign correspondent account is subject to EDD (31 CFR 103.176(a)(1)).
   - Assessing the money laundering risks presented by the foreign correspondent account (31 CFR 103.176(a)(2)).
   - Applying risk-based procedures and controls to each foreign correspondent account reasonably designed to detect and report known or suspected money laundering activity, including a periodic review of the correspondent account activity sufficient to determine consistency with information obtained about the type, purpose, and anticipated activity of the account (31 CFR 103.176(a)(3)).

6. Review the due diligence program's policies, procedures, and processes governing the BSA/AML risk assessment of foreign correspondent accounts (31 CFR 103.176(a)(2)). Verify that the bank's due diligence program considers the following factors, as appropriate, as criteria in the risk assessment:

   - The nature of the foreign financial institution's business and the markets it serves.
   - The type, purpose, and anticipated activity of the foreign correspondent account.
   - The nature and duration of the bank's relationship with the foreign financial institution and any of its affiliates.
   - The AML and supervisory regime of the jurisdiction that issued the charter or license to the foreign financial institution, and, to the extent that information regarding such jurisdiction is reasonably available, of the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered.
   - Information known or reasonably available to the bank about the foreign financial institution's AML record.

7. Ensure the program is reasonably designed to:

   - Detect and report, on an ongoing basis, known or suspected money laundering activity.

- Perform periodic reviews of correspondent account activity to determine consistency with the information obtained about the type, purpose, and anticipated activity of the account.

8. For foreign banks subject to EDD, evaluate the criteria that the U.S. bank uses to guard against money laundering in, and report suspicious activity in connection with, any correspondent accounts held by such foreign banks. Verify that the EDD procedures are applied to each correspondent account established for foreign banks operating under:

   - An offshore banking license.
   - A banking license issued by a foreign country that has been designated as noncooperative with international AML principles or procedures by an intergovernmental group or organization of which the United States is a member, and with which designation the 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 AML concerns.

9. Review the bank's policies, procedures, and processes and determine whether they include reasonable steps for conducting enhanced scrutiny of foreign correspondent accounts to guard against money laundering and to identify and report any suspicious transactions in accordance with applicable laws and regulations (31 CFR 103.176(b)(1)). Verify that this enhanced scrutiny reflects the risk assessment of each foreign correspondent account that is subject to such scrutiny and includes, as appropriate:

   - Obtaining and considering information relating to the foreign bank's anti-money laundering program to assess the risk of money laundering presented by the foreign bank's correspondent account (31 CFR 103.176(b)(1)(i)).
   - Monitoring transactions to, from, or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity (31 CFR 103.176(b)(1)(ii)).
   - Obtaining information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable through account, and the sources and beneficial owner of funds or other assets in the payable through account (31 CFR 103.176(b)(1)(iii)).

10 Review the bank's policies, procedures, and processes for determining whether foreign correspondent banks subject to EDD maintain correspondent accounts for other foreign banks, and, if so, determine whether the bank's policies, procedures, and processes include reasonable steps to obtain information relevant to assess and mitigate money laundering risks associated with the foreign correspondent bank's correspondent accounts for other foreign banks, including, as appropriate, the identity of those foreign banks (31 CFR 103.176(b)(2)).

11. Determine whether policies, procedures, and processes require the bank to take reasonable steps to identify each of the owners with the power to vote 10 percent or more of any class of securities of a nonpublicly traded foreign correspondent bank for which it opens or maintains an account that is subject to EDD. For such accounts, evaluate the bank's policies, procedures, and processes to determine each such owner's interest (31 CFR 103.176(b)(3)).

Transaction Testing

Foreign Shell Bank Prohibition and Foreign Correspondent Account Recordkeeping

12. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of foreign bank accounts. From the sample selected, determine the following:

    - Whether certifications and information on the accounts are complete and reasonable.
    - Whether the bank has adequate documentation to evidence that it does not maintain accounts for, or indirectly provide services to, foreign shell banks.
    - For account closures, whether closures were made within a reasonable time period and that the relationship was not re-established without sufficient reason.
    - Whether there are any federal law enforcement requests for information regarding foreign correspondent accounts. If so, ascertain that requests were met in a timely manner.
    - Whether the bank received any official notifications to close a foreign financial institution account.[116] If so, ascertain that the accounts were closed within ten business days.
    - Whether the bank retains, for five years from the date of account closure, the original of any document provided by a foreign financial institution, as well as the original or a copy of any document relied on in relation to any summons or subpoena of the foreign financial institution issued under 31 CFR 103.185.

Special Due Diligence Program for Foreign Correspondent Accounts

13. From a sample selected, determine whether the bank consistently follows its general due diligence policies, procedures, and processes for foreign correspondent accounts. It may be necessary to expand the sample to include correspondent accounts

[116] Official notifications to close a foreign financial institution's account must be signed by either the Secretary of the Treasury or the U.S. Attorney General (31 CFR 103.185(d)).

maintained for foreign financial institutions other than foreign banks (such as money transmitters or currency exchangers), as appropriate.

14. From the original sample, determine whether the bank has implemented EDD procedures for foreign banks operating under:
    - An offshore banking license.
    - A banking license issued by a foreign country that has been designated as noncooperative with international AML principles or procedures.
    - A banking license issued by a foreign country that has been designated by the Secretary of the Treasury as warranting special measures due to AML concerns.
15. From a sample of accounts that are subject to EDD, verify that the bank has taken reasonable steps, in accordance with the bank's policies, procedures, and processes, to:
    - Determine, for any such foreign bank whose shares are not publicly traded, the identity of each of the owners of the foreign bank with the power to vote 10 percent or more of any class of securities of the bank, and the nature and extent of the ownership interest of each such owner.
    - Conduct enhanced scrutiny of any accounts held by such banks to guard against money laundering and report suspicious activity.
    - Determine whether such foreign bank provides correspondent accounts to other foreign banks and, if so, obtain information relevant to assess and mitigate money laundering risks associated with the foreign bank's correspondent accounts for other foreign banks, including, as appropriate, the identity of those foreign banks.
16. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes to meet regulatory requirements associated with foreign correspondent account recordkeeping and due diligence.
17. On the basis of the previous conclusion and the risks associated with the bank's activity in this area, proceed to expanded examination procedures, if necessary.

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

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 examination procedures regarding specific money laundering risks associated with private banking.*

Private banking can be broadly defined as providing personalized financial services to wealthy clients. Section 312 of the USA PATRIOT Act added subsection (i) to 31 USC 5318 of the BSA. This subsection requires each U.S. financial institution that establishes, maintains, administers, or manages a private banking account in the United States for a non-U.S. person to take certain AML measures with respect to these accounts. In particular, a bank must establish appropriate, specific, and, where necessary, EDD policies, procedures, and controls that are reasonably designed to enable the bank to detect and report instances of money laundering through such accounts. In addition, section 312 mandates enhanced scrutiny to detect and, if appropriate, report transactions that may involve proceeds of foreign corruption for private banking accounts that are requested or maintained by or on behalf of a senior foreign political figure or the individual's immediate family and close associates. On January 4, 2006, FinCEN issued a final regulation (31 CFR 103.178) to implement the private banking requirements of 31 USC 5318(i).

The overview and examination 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, "Private Banking," pages 284 to 285.

Private Banking Accounts

For purposes of 31 CFR 103.178, a "private banking account" is an account (or any combination of accounts) maintained at a bank that satisfies all three of the following criteria:

- Requires a minimum aggregate deposit of funds or other assets of not less than $1,000,000.
- Is established on behalf of or for the benefit of one or more non-U.S. persons who are direct or beneficial owners[117] of the account.

[117] "Beneficial owner" of an account means an individual who has a level of control over, or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual, directly or indirectly, to control, manage, or direct the account. The ability to fund the account or the entitlement to the funds of the

- Is assigned to, or is administered by, in whole or in part, an officer, employee, or agent of a bank acting as a liaison between a financial institution covered by the regulation and the direct or beneficial owner of the account.

With regard to the minimum deposit requirement, a "private banking account" is an account (or combination of accounts) that *requires* a minimum deposit of not less than $1,000,000. A bank may offer a wide range of services that are generically termed private banking, and even if certain (or any combination, or all) of the bank's private banking services do not *require* a minimum deposit of not less than $1,000,000, these relationships should be subject to a greater level of due diligence under the bank's risk-based BSA/AML compliance program but are not subject to 31 CFR 103.178. Refer to the expanded overview section, "Private Banking," pages 279 to 283, for further guidance.

Due Diligence Program

A bank must establish and maintain a due diligence program that includes policies, procedures, and controls that are reasonably designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving any private banking account for a non-U.S. person that is established, maintained, administered, or managed in the United States by the bank. The due diligence program must ensure that, at a minimum, the bank takes reasonable steps to do each of the following:

- Ascertain the identity of all nominal and beneficial owners of a private banking account.
- Ascertain whether the nominal or beneficial owner of any private banking account is a senior foreign political figure.
- Ascertain the source(s) of funds deposited into a private banking account and the purpose and expected use of the account.
- Review the activity of the account to ensure that it is consistent with the information obtained about the client's source of funds, and with the stated purpose and expected use of the account, and to file a SAR, as appropriate, to report any known or suspected money laundering or suspicious activity conducted to, from, or through a private banking account.

---

account alone, however, without any corresponding authority to control, manage, or direct the account (such as in the case of a minor child beneficiary), does not cause the individual to be a beneficial owner (31 CFR 103.175(b)).

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

The nature and extent of due diligence conducted on private banking accounts for non-U.S. persons will likely vary for each client depending on the presence of potential risk factors. More extensive due diligence, for example, may be appropriate for new clients; clients who operate in, or whose funds are transmitted from or through, jurisdictions with weak AML controls; and clients whose lines of business are primarily currency-based (e.g., casinos or currency exchangers). Due diligence should also be commensurate with the size of the account. Accounts with relatively more deposits and assets should be subject to greater due diligence. In addition, if the bank at any time learns of information that casts doubt on previous information, further due diligence would be appropriate.

Ascertaining Source of Funds and Monitoring Account Activity

Banks that provide private banking services generally obtain considerable information about their clients, including the purpose for which the customer establishes the private banking account. This information can establish a baseline for account activity that will enable a bank to better detect suspicious activity and to assess situations where additional verification regarding the source of funds may be necessary. Banks are not expected, in the ordinary course of business, to verify the source of every deposit placed into every private banking account. However, banks should monitor deposits and transactions as necessary to ensure that activity is consistent with information that the bank has received about the client's source of funds and with the stated purpose and expected use of the account. Such monitoring will facilitate the identification of accounts that warrant additional scrutiny.

Enhanced Scrutiny of Private Banking Accounts for Senior Foreign Political Figures

For the purposes of private banking accounts under 31 CFR 103.175(r), the regulation defines the term "senior foreign political figure" to include one or more of the following:

- A current or former:
  - Senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government (whether elected or not).
  - Senior official of a major foreign political party.
  - Senior executive of a foreign-government-owned commercial enterprise.[118]

[118] For purposes of this definition, the terms "senior official" or "senior executive" mean an individual with substantial authority over policy, operations, or the use of government-owned resources.

- A corporation, business, or other entity that has been formed by, or for the benefit of, any such individual.
- An immediate family member (including spouses, parents, siblings, children, and a spouse's parents and siblings) of any such individual.
- A person who is widely and publicly known (or is actually known by the relevant bank) to be a close associate of such individual.

Senior foreign political figures as defined above are often referred to as "politically exposed persons" or PEPs. Refer to the expanded overview section, "Politically Exposed Persons," pages 297 to 300, for additional guidance, in particular with respect to due diligence on accounts maintained for PEPs that do not meet the regulatory definition of "private banking account" set forth in 31 CFR 103.175(o).

For private banking accounts for which a senior foreign political figure is a nominal or beneficial owner, the bank's due diligence program must include enhanced scrutiny that is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption. The term "proceeds of foreign corruption" means any asset or property that is acquired by, through, or on behalf of a senior foreign political figure through misappropriation, theft, or embezzlement of public funds, the unlawful conversion of property of a foreign government, or through acts of bribery or extortion, and includes any other property into which any such assets have been transformed or converted.[119] In those cases when a bank files a SAR concerning a transaction that may involve the proceeds of foreign corruption, FinCEN has instructed banks to include the term "foreign corruption" in the narrative portion of the SAR.[120]

Enhanced scrutiny of private banking accounts for senior foreign political figures should be risk-based. Reasonable steps to perform enhanced scrutiny may include consulting publicly available information regarding the home country of the client, contacting branches of the U.S. bank operating in the home country of the client to obtain additional information about the client and the political environment, and conducting greater scrutiny of the client's employment history and sources of income. For example, funds transfers from a government account to the personal account of a government official with signature authority over the government account may raise a bank's suspicions of possible political corruption. In addition, if a bank's review of major news sources indicates that a client may be or is involved in political corruption, the bank should review the client's account for unusual activity.

---

[119] Additional red flags regarding transactions that may be related to the proceeds of foreign corruption are listed in *Guidance on Enhanced Scrutiny for Transactions That May Involve the Proceeds of 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.

[120] Refer to FIN-2008-G005, *Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption,* April 17, 2008, available at www.fincen.gov.

Identifying Senior Foreign Political Figures

Banks are required to establish policies, procedures, and controls that include reasonable steps to ascertain the status of an individual as a senior foreign political figure. Procedures should require obtaining information regarding employment and other sources of income, and the bank should seek information directly from the client regarding possible senior foreign political figure status. The bank should also check references, as appropriate, to determine whether the individual holds or has previously held a senior political position or may be a close associate of a senior foreign political figure. In addition, the bank should make reasonable efforts to review public sources of information regarding the client.

Banks applying reasonable due diligence procedures in accordance with 31 CFR 103.178 may not be able to identify in every case individuals who qualify as senior foreign political figures, and, in particular, their close associates, and thus may not apply enhanced scrutiny to all such accounts. If the bank's due diligence program is reasonably designed to make this determination, and the bank administers this program effectively, then the bank should generally be able to detect, report, and take appropriate action when suspected money laundering is occurring with respect to these accounts, even in cases when the bank has not been able to identify the accountholder as a senior foreign political figure warranting enhanced scrutiny.

Special Procedures When Due Diligence Cannot Be Performed

A bank's due diligence policies, procedures, and controls established pursuant to 31 CFR 103.178(a) must include special procedures when appropriate due diligence cannot be performed. These special procedures must include when the bank should:

- Refuse to open the account.
- Suspend transaction activity.
- File a SAR.
- Close the account.

Examination Procedures

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 examination procedures regarding specific money laundering risks associated with private banking.*

1. Determine whether the bank offers private banking accounts in accordance with the regulatory definition of a private banking account. A private banking account means an account (or any combination of accounts) maintained at a financial institution covered by the regulation that satisfies all three of the following criteria:

   - Requires a minimum aggregate deposit of funds or other assets of not less than $1,000,000 (31 CFR 103.175(o)(1)).
   - Is established on behalf of or for the benefit of one or more non-U.S. persons who are direct or beneficial owners of the account (31 CFR 103.175(o)(2)).
   - Is assigned to, or is administered or managed by, in whole or in part, an officer, employee, or agent of the bank acting as a liaison between the bank and the direct or beneficial owner of the account (31 CFR 103.175(o)(3)).

   The final rule reflects the statutory definition found in the USA PATRIOT Act. If an account satisfies the last two criteria in the definition of a private banking account as described above, but the institution does not require a minimum balance of $1,000,000, then the account does not qualify as a private banking account under this rule. However, the account is subject to the internal controls and risk-based due diligence included in the institution's general BSA/AML compliance program.[121]

2. Determine whether the bank has implemented due diligence policies, procedures, and controls for private banking accounts established, maintained, administered, or managed in the United States by the bank for non-U.S. persons. Determine whether the policies, procedures, and controls are reasonably designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving any private banking account.

3. Review the bank's policies, procedures, and controls to assess whether the bank's due diligence program includes reasonable steps to:

[121] Refer to the expanded examination procedures, "Private Banking" and "Politically Exposed Persons" (PEPs), pages 284 to 285 and 301 to 302, respectively, for additional guidance.

- Ascertain the identity of the nominal and beneficial owners of a private banking account (31 CFR 103.178(b)(1)).
- Ascertain whether any nominal or beneficial owner of a private banking account is a senior foreign political figure (31 CFR 103.178(b)(2)).
- Ascertain the source(s) of funds deposited into a private banking account and the purpose and expected use of the private banking account for non-U.S. persons (31 CFR 103.178(b)(3)).
- Review the activity of the account to ensure that it is consistent with the information obtained about the client's source of funds and with the stated purpose and expected use of the account, as needed, to guard against money laundering and to report any known or suspected money laundering or suspicious activity conducted to, from, or through a private banking account for non-U.S. persons (31 CFR 103.178(b)(4)).

4. Review the bank's policies, procedures, and controls for performing enhanced scrutiny to assess whether they are reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption[122] for which a senior foreign political figure[123] is a nominal or beneficial owner (31 CFR 103.178(c)(1)).

Transaction Testing

5. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of customer files to determine whether the bank has ascertained the identity of the nominal and beneficial owners of, and the source of funds deposited into, private banking accounts for non-U.S. persons. From the sample selected determine the following:
   - Whether the bank's procedures comply with internal policies and statutory requirements.

[122] The term "proceeds of foreign corruption" means any assets or property that is acquired by, through, or on behalf of a senior foreign political figure through misappropriation, theft, or embezzlement of public funds, the unlawful conversion of property of a foreign government, or through acts of bribery or extortion, and shall include any other property into which any such assets have been transformed or converted (31 CFR 103.178(c)(2)).

[123] The final rule defines a senior foreign political figure as: a current or former senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government, whether or not they are or were elected officials; a senior official of a major foreign political party; and a senior executive of a foreign government-owned commercial enterprise. The definition also includes a corporation, business, or other entity formed by or for the benefit of such an individual. Senior executives are individuals with substantial authority over policy, operations, or the use of government-owned resources. Also included in the definition of a senior foreign political official are immediate family members of such individuals and persons who are widely and publicly known (or actually known) close associates of a senior foreign political figure.

- Whether the bank has followed its procedures governing risk assessment of private banking accounts for non-U.S. persons.
- Whether the bank performs enhanced scrutiny of private banking accounts for which senior foreign political figures are nominal or beneficial owners, consistent with its policy, regulatory guidance, and statutory requirements.

6. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with private banking due diligence programs.
7. On the basis of the previous conclusion and the risks associated with the bank's activity in this area, proceed to expanded examination procedures, if necessary.

Special Measures — Overview

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

Section 311 of the USA 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 103.[124] 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.

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 records or to file reports, or both, 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

[124] Notices of proposed rulemaking and final rules accompanying the determination "of primary money laundering concern," and imposition of a special measure(s) pursuant to section 311 of the USA PATRIOT Act are available on the FinCEN Web site at www.fincen.gov.

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 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 (i) to identify each customer (and representative) who is permitted to use the account or whose transactions are routed through the account and (ii) to obtain information about each customer (and representative) that is substantially comparable to that which the bank obtains in the ordinary course of business with respect to its customers residing in the United States.[125]

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 States depository institution obtains in the ordinary course of business with respect to its customers residing in the United States.[126]

---

[125] Refer to expanded overview section, "Payable Through Accounts," pages 198 to 200, for additional guidance.

[126] Refer to core overview section, "Foreign Correspondent Account Recordkeeping and Due Diligence," pages 117 to 124, and expanded overview section, "Correspondent Accounts (Foreign)," pages 183 to 185, for additional guidance.

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 in the United States 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 in the United States 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 whether 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 USA 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 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, because any such listing could quickly become dated. Examiners reviewing compliance with this section should visit FinCEN's Web site at 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 for special measures that are proposed.

Examination Procedures

Special Measures

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

1. Determine the extent of the bank's international banking activities and the foreign jurisdictions in which the bank conducts transactions and activities, with particular emphasis on foreign correspondent banking and payable through accounts.

2. As applicable, determine whether the bank has established policies, procedures, and processes to respond to specific special measures imposed by FinCEN that are applicable to its operations. Evaluate the adequacy of the policies, procedures, and processes for detecting accounts or transactions with jurisdictions, financial institutions, or transactions subject to final special measures.

3. Determine, through discussions with management and review of the bank's documentation, whether the bank has taken action in response to final special measures.

Transaction Testing

4. Determine all final special measures issued by FinCEN under section 311 that are applicable to the bank (refer to www.fincen.gov).

5. For any of the first four types of special measures, determine whether the bank obtained, recorded, or reported the information required by each particular special measure.

6. For the fifth special measure (prohibition), determine whether the bank complied with the prohibitions or restrictions required by each particular special measure, and complied with any other actions required by the special measures.

7. As necessary, search the bank's MIS and other appropriate records for accounts or transactions with jurisdictions, financial institutions, or transactions subject to final special measures.

8. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with special measures.

Foreign Bank and Financial Accounts Reporting — Overview

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

Each person[127] (including a bank) subject to U.S. jurisdiction with a financial interest in, or signature or other 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) (TD F 90-22.1) with the IRS if the aggregate value of these financial accounts exceeds $10,000 at any time during the calendar year.[128] As clarified on the revised FBAR form, which was published by the IRS in October 2008 and must be used after December 31, 2008, the term "financial account" generally includes, among other things, accounts in which assets are held in a commingled fund and the account owner holds an equity interest in the fund, (e.g., a mutual fund), as well as debit card and prepaid card accounts.

On August 7, 2009, the IRS issued Notice 2009-62, which indicated that the IRS intended to issue regulations further clarifying the applicability of the FBAR requirements to U.S. persons with only signature authority over (but no financial interest in) a foreign financial account, as well as to U.S. persons with financial interest in or signature authority over foreign commingled funds. Consequently, with respect to these two types of foreign financial accounts, the IRS extended the FBAR filing deadline for U.S. persons for the 2008 and earlier calendar years until June 30, 2010.

A bank must file this form on its own accounts that meet this definition; additionally, 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 or other authority.

An FBAR must be filed with the Commissioner of the IRS on or before June 30 of each calendar year for foreign financial accounts where the aggregate value exceeded $10,000 at any time during the previous calendar year.

---

[127] 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. The instructions to the FBAR further state that the term "United States person" means a citizen or resident of the United States or a person in and doing business in the United States. The IRS has indicated that generally a person is not considered to be "in and doing business in the United States" unless that person is conducting business within the United States on a regular and continuous basis. Refer to *FAQs Regarding Report of Foreign Bank and Financial Accounts (FBAR)*, February 12, 2009, www.irs.gov/businesses/small/article/0,,id=148845,00.html#UPS1. Furthermore, in Announcement 2009-51, 2009-25 I.R.B. 1105, issued June 5, 2009, the IRS indicated that it had suspended temporarily the FBAR filing requirement for persons who are not U.S. citizens, residents, or domestic entities.

[128] 31 CFR 103.24.

Examination Procedures

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.*

1. Determine whether the bank has a financial interest in, or signature or other authority over, bank, securities, or other financial accounts in a foreign country, as well as whether the bank is required to file a Report of Foreign Bank and Financial Accounts (FBAR) (TD F 90-22.1) form for customer accounts, including trust accounts, in which the bank has a financial interest or over which it has signature or other authority.

2. If applicable, review the bank's policies, procedures, and processes for filing annual reports.

Transaction Testing

3. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of accounts to determine whether the bank has appropriately completed, submitted, and retained copies of the FBAR forms.

4. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with FBARs.

International Transportation of Currency or Monetary Instruments Reporting — Overview

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

Each person[129] (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).[130] 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.[131] 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

---

[129] 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.

[130] The obligation to file the CMIR is solely on the person who transports, mails, ships or receives, or causes or attempts to transport, mail, ship, or receive. No other person is under any obligation to file a CMIR. Thus, if a customer walks into the bank and declares that he or she has received or transported currency in an aggregate amount exceeding $10,000 from a place outside the United States and wishes to deposit the currency into his or her account, the bank is under no obligation to file a CMIR on the customer's behalf (Treasury Administrative Ruling 88-2).

[131] 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.

monetary instruments and determine whether a customer's activity is usual and customary for the type of business. If not, a SAR should be considered.

Examination Procedures

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.*

1. Determine whether the bank has (or has caused to be) physically transported, mailed, or shipped currency or other monetary instruments in excess of $10,000, at one time, out of the United States, or whether the bank has received currency or other monetary instruments in excess of $10,000, at one time, that has been physically transported, mailed, or shipped into the United States.

2. If applicable, review the bank's policies, procedures, and processes for filing a Report of International Transportation of Currency or Monetary Instruments (CMIR) (FinCEN Form 105) for each shipment of currency or other monetary instruments in excess of $10,000 out of or into the United States (except for shipments sent through the postal service, common carrier, or to which another exception from CMIR reporting applies).

Transaction Testing

3. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of transactions conducted after the previous examination to determine whether the bank has appropriately completed, submitted, and retained copies of the CMIR forms.

4. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with CMIRs.

5. On the basis of the previous conclusion and the risks associated with the bank's activity in this area, proceed to expanded examination procedures, if necessary.

Office of Foreign Assets Control — Overview

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

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.[132]

On November 9, 2009, OFAC issued a final rule entitled "Economic Sanctions Enforcement Guidelines" in order to provide guidance to persons subject to its regulations. The document explains the procedures that OFAC follows in determining the appropriate enforcement response to apparent violations of its regulations. Some enforcement responses may result in the issuance of a civil penalty that, depending on the sanctions program affected, may be as much as $250,000 per violation or twice the amount of a transaction, whichever is greater. The Guidelines outline the various factors that OFAC takes into account when making enforcement determinations, not the least of which is the adequacy of a compliance program in place within an institution to ensure compliance with OFAC regulations.[133]

---

[132] 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 Act (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).

[133] Refer to 73 Fed. Reg. 57593 (November 9, 2009) for additional information (also available at www.treas.gov/ofac).

All U.S. persons,[134] including U.S. banks, bank holding companies, and nonbank subsidiaries, must comply with OFAC's regulations.[135] The federal banking agencies evaluate OFAC compliance systems to ensure that all banks subject to their supervision comply with the sanctions.[136] 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 of an OFAC-specified country, entity, or individual 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 go 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

[134] 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.

[135] Additional information is provided in *Foreign Assets Control Regulations for the Financial Community*, which is available on OFAC's Web site www.treas.gov/offices/enforcement/ofac.

[136] 31 CFR chapter V.

into a blocked account.[137] 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 (SDN), involving an export to a company in Sudan that also is not an SDN. Because Sudanese Sanctions would only require blocking transactions with the Government of Sudan or an SDN, 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 cannot 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 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 the core overview section, "Customer Identification Program," pages 52 to 58, 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

[137] 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.

license, banks should verify that such transactions meet the relevant criteria of the general license.[138]

Specific licenses are issued on a case-by-case basis.[139] 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 to 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.

OFAC Reporting

Banks must report all blockings to OFAC within 10 days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30).[140] 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 10 days of the occurrence.

Banks must keep a full and accurate record of each rejected transaction for at least five years after the date of the transaction. For blocked property (including blocked transactions), 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.[141]

OFAC Compliance 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 compliance program commensurate with their OFAC risk profile (based on products, services, customers, and geographic locations). The program should identify higher-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

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

[139] Specific licenses require an application directed to: Licensing Division, Office of Foreign Assets Control, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

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

[141] This information is available on OFAC's Web site at www.treas.gov/offices/enforcement/ofac, or by contacting OFAC's hotline toll-free at 800-540-6322.

personnel in all relevant areas of the bank. A bank's OFAC compliance program should be commensurate with its respective OFAC risk profile.

OFAC Risk Assessment

A fundamental element of a sound OFAC compliance program is the bank's assessment of its specific product lines, customer base, and nature of transactions and identification of higher-risk areas for OFAC transactions. The initial identification of higher-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.

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 higher-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) transactions.
- Commercial letters of credit and other trade finance products.
- 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."[142]

Once the bank has identified its areas with higher 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 compliance program should include internal controls for identifying suspect accounts and transactions and reporting to OFAC. Internal controls should include the following elements:

Identifying and reviewing suspect transactions. The bank's policies, procedures, and processes should address how the bank will identify 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 identifying 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.[143] 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 higher-risk area with a high-volume of transactions, the bank's interdiction software should be able to identify 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. Lower-risk banks or areas and those with

[142] This document is available at www.treas.gov/offices/enforcement/ofac/faq/index.shtml.

[143] Due diligence steps for determining a valid match are provided in *Using OFAC's Hotline* on OFAC's Web site at www.treas.gov/offices/enforcement/ofac.

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 lower OFAC risk level may periodically (e.g., monthly or quarterly) compare the customer base against the OFAC list. Transactions such as funds transfers, letters of credit, and noncustomer 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.[144] 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 compliance 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. This would include ensuring that any manual updates of interdiction software are completed in a timely manner.

Screening Automated Clearing House (ACH) transactions. All parties to an ACH transaction are subject to the requirements of OFAC. Refer to the expanded overview section, "Automated Clearing House Transactions," pages 224 to 231, for additional

[144] Refer to 74 Fed. Reg. 57593 (November 9, 2009), *Economic Sanctions Enforcement Guidelines.* www.treas.gov/offices/enforcement/ofac/legal/regs/fr74_57593.pdf. Further information is available on OFAC's Web site at www.treasury.gov/offices/enforcement/ofac

guidance. OFAC has clarified the application of its rules for domestic and cross-border ACH transactions and provided more detailed guidance on international ACH transactions.[145]

With respect to domestic ACH transactions, the Originating Depository Financial Institution (ODFI) is responsible for verifying that the Originator is not a blocked party and making a good faith effort to ascertain that the Originator is not transmitting blocked funds. The Receiving Depository Financial Institution (RDFI) similarly is responsible for verifying that the Receiver is not a blocked party. In this way, the ODFI and the RDFI are relying on each other for compliance with OFAC regulations.

If an ODFI receives domestic ACH transactions that its customer has already batched, the ODFI is not responsible for unbatching those transactions to ensure that no transactions violate OFAC's regulations. If an ODFI unbatches a file originally received from the Originator in order to process "on-us" transactions, that ODFI is responsible for the OFAC compliance for the on-us transactions because it is acting as both the ODFI and the RDFI for those transactions. ODFIs acting in this capacity should already know their customers for the purposes of OFAC and other regulatory requirements. For the residual unbatched transactions in the file that are not "on-us," as well as those situations where banks deal with unbatched ACH records for reasons other than to strip out the on-us transactions, banks should determine the level of their OFAC risk and develop appropriate policies, procedures, and processes to address the associated risks. Such policies might involve screening each unbatched ACH record. Similarly, banks that have relationships with third-party service providers should assess those relationships and their related ACH transactions to ascertain the bank's level of OFAC risk and to develop appropriate policies, procedures, and processes to mitigate that risk.

With respect to cross-border screening, similar but somewhat more stringent OFAC obligations hold for International ACH transactions (IAT). In the case of inbound IATs, and regardless of whether the OFAC flag in the IAT is set, an RDFI is responsible for compliance with OFAC requirements. For outbound IATs, however, the ODFI cannot rely on OFAC screening by an RDFI outside of the United States. In these situations, the ODFI must exercise increased diligence to ensure that illegal transactions are not processed.

Due diligence for an inbound or outbound IAT may include screening the parties to a transaction, as well as reviewing the details of the payment field information for an indication of a sanctions violation, investigating the resulting hits, if any, and ultimately blocking or rejecting the transaction, as appropriate. Refer to the expanded overview section, "Automated Clearing House Transactions," pages 224 to 231, for additional guidance.

---

[145] Refer to Interpretive Note 041214-FACRL-GN-02 at www.treas.gov/offices/enforcement/ofac/rulings/. NACHA rules further specify this compliance (refer to page 8 of the Quick Find section of the *2006 NACHA Operating Rules*).

Additional information on the types of retail payment systems (ACH payment systems) is available in the FFIEC *Information Technology Examination Handbook*.[146]

In guidance issued on March 10, 2009, OFAC authorized institutions in the United States when they are acting as an ODFI/Gateway Operator (GO) for inbound IAT debits to reject transactions that appear to involve blockable property or property interests.[147] The guidance further states that to the extent that an ODFI/GO screens inbound IAT debits for possible OFAC violations prior to execution and in the course of such screening discovers a potential OFAC violation, the suspect transaction is to be removed from the batch for further investigation. If the ODFI/GO determines that the transaction does appear to violate OFAC regulations, the ODFI/GO should refuse to process the transfer. The procedure applies to transactions that would normally be blocked as well as to transactions that would normally be rejected for OFAC purposes based on the information in the payment.

Reporting. An OFAC compliance 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 SARs based solely 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 is in possession of additional information not included on the blocking report filed with OFAC, a separate SAR 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.[148]

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

---

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

[147] Refer to www.frbservices.org/files/eventseducation/pdf/iat/031809_ofac_update.pdf.

[148] Refer to FinCEN Release Number 2004-02, *Unitary Filing of Suspicious Activity and Blocking Reports*, 69 Fed. Reg. 76847 (December 23, 2004).

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 compliance program that is performed by the internal audit department, outside auditors, consultants, or other qualified independent parties. 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 compliance 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 compliance program, including the reporting of blocked or rejected transactions to OFAC and the oversight of blocked funds. This individual should 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.

Examination Procedures

Office of Foreign Assets Control

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

1. Determine whether the board of directors and senior management of the bank have developed policies, procedures, and processes based on their risk assessment to ensure compliance with OFAC laws and regulations.

2. Review the bank's OFAC compliance program in the context of the bank's OFAC risk assessment. Consider the following:

   - The extent of, and method for, conducting OFAC searches of each relevant department or business line (e.g., automated clearing house (ACH) transactions, monetary instrument sales, check cashing, trusts, loans, deposits, and investments) as the process may vary from one department or business line to another.
   - The extent of, and method for, conducting OFAC searches of account parties other than accountholders, which may include beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories, and powers of attorney.
   - How responsibility for OFAC is assigned.
   - Timeliness of obtaining and updating OFAC lists or filtering criteria.
   - The appropriateness of the filtering criteria used by the bank to reasonably identify OFAC matches (e.g., the extent to which the filtering or search criteria includes misspellings and name derivations).
   - The process used to investigate potential matches, including escalation procedures for potential matches.
   - The process used to block and reject transactions.
   - The process used to inform management of blocked or rejected transactions.
   - The adequacy and timeliness of reports to OFAC.
   - The process to manage blocked accounts (such accounts are reported to OFAC and pay a commercially reasonable rate of interest).
   - The record retention requirements (e.g., five-year requirement to retain relevant OFAC records; for blocked property, record retention for as long as blocked; once unblocked, records must be maintained for five years).

3. Determine the adequacy of independent testing (audit) and follow-up procedures.

4. Review the adequacy of the bank's OFAC training program based on the bank's OFAC risk assessment.

5. Determine whether the bank has adequately addressed weaknesses or deficiencies identified by OFAC, auditors, or regulators.

Transaction Testing

6. On the basis of a bank's risk assessment, prior examination reports, and a review of the bank's audit findings, select the following samples to test the bank's OFAC compliance program for adequacy, as follows:

   - Sample new accounts (e.g., deposit, loan, trust, safe deposit, investments, credit cards, and foreign office accounts,) and evaluate the filtering process used to search the OFAC database (e.g., the timing of the search), and documentation maintained evidencing the searches.

   - Sample appropriate transactions that may not be related to an account (e.g., funds transfers, monetary instrument sales, and check-cashing transactions), and evaluate the filtering criteria used to search the OFAC database, the timing of the search, and documentation maintained evidencing the searches.

   - If the bank uses an automated system to conduct searches, assess the timing of when updates are made to the system, and when the most recent OFAC changes were made to the system. Also, evaluate whether all of the bank's databases are run against the automated system, and the frequency upon which searches are made. If there is any doubt regarding the effectiveness of the OFAC filter, then run tests of the system by entering test account names that are the same as or similar to those recently added to the OFAC list to determine whether the system identifies a potential hit.

   - If the bank does not use an automated system, evaluate the process used to check the existing customer base against the OFAC list and the frequency of such checks.

   - Review a sample of potential OFAC matches and evaluate the bank's resolution for blocking and rejecting processes.

   - Review a sample of reports to OFAC and evaluate their completeness and timeliness.

   - If the bank is required to maintain blocked accounts, select a sample and evaluate that the bank maintains adequate records of amounts blocked and ownership of blocked funds, that the bank is paying a commercially reasonable rate of interest on all blocked accounts, and that it is accurately reporting required information annually (by September 30) to OFAC. Test the controls in place to verify that the account is blocked.

- Pull a sample of false hits (potential matches) to check their handling; the resolution of a false hit should take place outside of the business line.

7. Identify any potential matches that were not reported to OFAC, discuss with bank management, advise bank management to immediately notify OFAC of unreported transactions, and immediately notify supervisory personnel at your regulatory agency.

8. Determine the origin of deficiencies (e.g., training, audit, risk assessment, internal controls, management oversight), and conclude on the adequacy of the bank's OFAC compliance program.

9. Discuss OFAC related examination findings with bank management.

10. Include OFAC conclusions within the report of examination, as appropriate.