BSA Exam Manual

Shelf Version
April 2020

Consultants to the Financial Industry
Young & Associates, Inc.
121 E. Main Street
P.O. Box 711
Kent, OH 44240
Phone: 330.678.0524
Fax: 330.678.6219
www.younginc.com

Table of Contents

Section 1: Introduction (revised 2014)

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 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. For more guidance, refer to Appendix A ("BSA Laws and Regulations"), Appendix B ("BSA/AML Directives"), and Appendix C ("BSA/AML References").

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

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
- BSA/AML Risk Assessment
- BSA/AML Compliance Program
- Developing Conclusions and Finalizing the Examination.

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," 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 are likely to be applicable to every banking organization. The specific examination procedures that 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, which established requirements for record keeping and reporting by private individuals, banks, 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. The Money Laundering Control Act of 1986 precludes circumvention of the BSA requirements by imposing criminal liability on a person or financial institution that knowingly assists in the laundering of money, or that structures transactions to avoid reporting them. The 1986 statute directed banks to establish and maintain procedures reasonably designed to ensure and monitor compliance with the reporting and recordkeeping requirements of the BSA. As a result, on January 27, 1987, all federal banking agencies issued essentially similar regulations requiring banks to develop programs for BSA compliance.

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

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

In response to the September 11, 2001, terrorist attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (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. 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 Reserve), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), and Office of the Comptroller of the Currency (OCC). Internationally there are various multilateral government bodies that support the fight against money laundering and terrorist financing. Refer to Appendix E ("International Organizations") for additional information.

U.S. Treasury

The BSA authorizes the Secretary of the Treasury to require financial institutions to establish AML programs, file certain reports, and keep certain records of transactions. Certain BSA provisions have been extended to cover not only traditional depository institutions, such as banks, savings associations, and credit unions, but also 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 (NCUA and OCC), insuring (FDIC and NCUA), regulating, and supervising banks. 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 FDIA or section 206 of the FCUA, to enforce compliance with appropriate banking rules and regulations, including compliance with the BSA.

The federal banking agencies require each bank under their supervision to establish and maintain a BSA compliance program. 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 1020.210 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 governing such programs. This manual refers 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 sufficient detail in reports to law enforcement agencies to make the reports useful for investigating suspicious transactions that are reported. Refer to Appendixes 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.

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," 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.

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, 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") 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. Any property involved in a transaction or traceable to the proceeds of the criminal activity, including property such as loan collateral, personal property, and, under certain conditions, entire bank accounts (even if some of the money in the account is legitimate), may be subject to forfeiture. Pursuant to various statutes, banks and individuals may incur criminal and civil liability for violating AML and terrorist financing laws. For instance, pursuant to 18 USC 1956 and 1957, the U.S. Department of Justice may bring criminal actions for money laundering that may include criminal fines, imprisonment, and forfeiture actions. 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. 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. 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.

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.

Section 2: Scoping and Planning (revised 2020)

Scoping and Planning Introduction

Objective: ***Develop an understanding of the bank's money laundering, terrorist financing (ML/TF), and other illicit financial activity risk profile. Based on the bank's risk profile, develop a risk-focused examination scope, and document the Bank Secrecy Act/anti-money laundering (BSA/AML) examination plan.***

Examiners assess the adequacy of the bank's Bank Secrecy Act/anti-money laundering (BSA/AML) compliance program, relative to its risk profile, and the bank's compliance with BSA regulatory requirements. The scoping and planning process enables examiners to understand the money laundering, terrorist financing (ML/TF), and other illicit financial activity risk profile of the bank. The scoping and planning process also enables examiners to focus their reviews of risk management practices and compliance with BSA requirements on areas of greatest ML/TF and other illicit financial activity risks. Examiners assess whether the bank has developed and implemented adequate processes to identify, measure, monitor, and control those risks and comply with BSA regulatory requirements.

The scoping and planning process should include determining BSA/AML examination staffing needs, including technical expertise, and identifying the BSA/AML examination and testing procedures to be completed. The federal banking agencies generally allocate more resources to higher-risk areas and fewer resources to lower-risk areas. Each section in this Manual includes an introductory overview and accompanying examination and testing procedures, as applicable, for examiners to follow.

Whenever possible, the scoping and planning process should be completed before the onsite portion of the examination, although some information may not be available during this process. The scope of a BSA/AML examination varies by bank and should be tailored primarily to the bank's risk profile. Other factors to consider in determining the examination scope may include the bank's size or complexity, and organizational structure. The request letter should also be tailored to, and correspond with, the planned examination scope.

The scoping and planning process generally begins with a review of the bank's BSA/AML risk assessment, independent testing (audit), analyses and conclusions from previous examinations, other information available through offsite and ongoing monitoring processes, and request letter items received from the bank. Subsections of Scoping and Planning provide information to help examiners understand the bank's risk profile and develop the BSA/AML examination plan.

Many banks rely on technology to aid in BSA/AML compliance and, therefore, the scoping and planning process should include developing an understanding of the bank's information technology sources, systems, and processes used in the BSA/AML compliance program. This information assists examiners in the scoping and planning process to determine what, if any, additional examiner subject matter expertise is warranted.

Office of Foreign Assets Control (OFAC) regulations are not part of the BSA, and an OFAC review is not required during each examination cycle. However, OFAC compliance programs are

frequently assessed in conjunction with BSA/AML examinations. Factors to consider when determining whether to include a review of OFAC compliance in the examination scope include the bank's OFAC risk profile, in particular the number, dollar amount, and type of international activity; the bank's size or complexity; and organizational structure. The federal banking agencies' primary role relative to OFAC is to evaluate the sufficiency of the bank's implementation of policies, procedures, and processes for complying with OFAC-administered laws and regulations, not to identify apparent OFAC violations.[3] If OFAC compliance will be part of the review, examiners should also review the bank's OFAC risk assessment and related independent testing to determine the appropriate scope of the review. Refer to the Office of Foreign Assets Control section for more information.

Risk-Focused BSA/AML Supervision

Objective: ***Based on the bank's risk profile, determine the BSA/AML examination activities necessary to assess the adequacy of the bank's BSA/AML compliance program and the bank's compliance with BSA regulatory requirements.***

The agencies use a risk-focused approach for planning and performing BSA/AML examinations, which is reinforced in the "Joint Statement on the Risk-Focused Approach to BSA/AML Supervision." Examiners should assess the adequacy of the bank's BSA/AML compliance program, relative to its risk profile, and the bank's compliance with BSA regulatory requirements. The extent of BSA/AML examination activities necessary to assess the bank generally depends on the bank's risk profile and the quality of risk management processes to identify, measure, monitor, and control risks, and to report potential ML/TF and other illicit financial activity. Given that banks vary in size, complexity, and organizational structure, each bank has a unique risk profile, and the scope of a BSA/AML examination varies by bank.

To conduct risk-focused BSA/AML examinations, examiners should tailor their examination plans, including examination and testing procedures, to each bank's risk profile. To understand the bank's risk profile, examiners should consider available information including, but not limited to, the following:

- The bank's BSA/AML risk assessment.
- Independent testing or audits.
- Analyses and conclusions from previous examinations.
- Management's responses, including the current status of issues, regarding independent testing or audit results and examination findings.
- Offsite and ongoing monitoring.
- Information received from the bank in response to the request letter.
- Other communications with the bank.
- BSA reporting available from the Financial Crimes Enforcement Network (FinCEN).

As explained in more detail below, examiners should review the bank's BSA/AML risk assessment and independent testing when evaluating the bank's ability to identify, measure, monitor, and control risks. BSA/AML risk assessments and independent testing that properly consider and test all risk areas (including products, services, customers, and geographic locations

in which the bank operates and conducts business) are used in determining the BSA/AML examination and testing procedures that should be performed.

BSA/AML Risk Assessment

The scoping and planning process is guided by examiner review of the BSA/AML risk assessment for the bank. The information contained in the BSA/AML risk assessment assists examiners in developing an understanding of the bank's risk profile, risk-focusing the examination scope, and assessing the adequacy of the bank's overall BSA/AML compliance program and its compliance with BSA regulatory requirements.

The *BSA/AML Risk Assessment* section provides information and procedures for examiners in determining whether the bank has developed a risk assessment process that adequately identifies the ML/TF and other illicit financial activity risks within its banking operations. If the bank has not developed a BSA/AML risk assessment, this fact should be discussed with management. Whenever the bank has not completed a BSA/AML risk assessment, or the BSA/AML risk assessment is inadequate, examiners must develop a BSA/AML risk assessment for the bank.

Independent Testing

Examiners should obtain and evaluate independent testing (audit) report(s) of the bank's BSA/AML compliance program, including any scope and supporting workpapers. The independent testing should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties (not involved in the function being tested or other BSA-related functions at the bank that may present a conflict of interest or lack of independence). Independent testing results should be reported directly to the board of directors or a designated board committee composed primarily, or completely, of outside directors.

The scope and quality of independent testing may provide examiners with information regarding the bank's particular risks, how these risks are being managed and controlled, and the status of the bank's BSA compliance. Independent testing report(s) and supporting workpapers can assist examiners in understanding audit coverage and the quality and quantity of transaction testing that was performed as part of the independent testing. This knowledge assists examiners in risk focusing the BSA/AML examination plan by identifying areas for greater (or lesser) review, and by identifying when additional examination and testing procedures may be necessary.

If the bank's independent testing is adequate, findings from the independent testing may be leveraged to reduce the examination areas covered and the testing necessary to assess the bank's BSA/AML compliance program. To determine the adequacy of the bank's independent testing, examiners should determine whether the testing was independent and assessed all appropriate ML/TF and other illicit financial activity risks within the bank's operations. Examiners must have access to the appropriate independent testing scope and supporting workpapers to leverage findings from the bank's independent testing. Refer to the BSA/AML Independent Testing section for more information.

BSA Reporting Available From FinCEN

FinCEN Query is the system used to access all BSA reports. BSA/AML examination planning should include an analysis of BSA reports that the bank has filed, such as Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs), and CTR exemptions, for a defined time period. SARs, CTRs, and CTR exemptions may be exported, downloaded, or obtained directly online from FinCEN Query. Each federal banking agency has staff authorized to obtain this data from FinCEN Query. When requesting searches from FinCEN Query, examiners should contact the appropriate person(s) within their agency sufficiently in advance of the examination start date to obtain the requested information. When a bank has recently purchased or merged with another bank, examiners should obtain SARs, CTRs, and CTR exemptions data on the acquired bank.

Downloaded information from FinCEN Query may be important to the examination, as it helps examiners:

- Identify high-volume currency customers.
- Identify the volume and characteristics of SARs filed.
- Identify frequent SAR subjects.
- Identify the volume and nature of CTRs and CTR exemptions.
- Select accounts, transactions, or BSA filings for testing, if warranted.

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

Information available through FinCEN Query is sensitive, and in some instances confidential, and may only be retrieved and used by examiners for official business. The dissemination of information obtained through FinCEN Query is subject to specific legal requirements, restrictions, and conditions. Examiners must adhere to the "FinCEN Re-Dissemination Guidelines for Bank Secrecy Act Information" and the "FinCEN Bank Secrecy Act Information Access Security Plan" when accessing information through FinCEN Query. These documents can be obtained through each agency's FinCEN Query coordinator and should be reviewed by anyone accessing FinCEN Query.

Risk-Focused Testing

Examiners perform testing to assess the adequacy of the bank's BSA/AML compliance program, relative to its risk profile, and the bank's compliance with BSA regulatory requirements. Examiners also perform testing to assess the implementation of policies, procedures, and processes, and to evaluate controls, information technology sources, systems, and processes used for BSA compliance.

Testing performed during BSA/AML examinations should be risk-focused and can take the form of testing specific transactions, or performing analytical or other reviews. Examiners must perform some testing during each BSA/AML examination cycle. Testing may focus on any of the regulatory requirements and may address different areas of the BSA/AML compliance program, but may not be necessary for every regulation or BSA area examined. Where transaction testing

typically involves reviewing specific transactions or files, analytical reviews are usually higher level without transaction or file details, such as analyzing reports.

Under a risk-focused examination approach, the size and composition of the sample selected for testing, as well as the type of testing, should be commensurate with the bank's risk profile and the examination scope. While examiners generally test different areas in successive examinations, it may be appropriate to test the same areas in successive examinations based on previous examination findings, as well as the bank's risk profile and risk assessment, including any changes therein. Examiners should limit the extent and type of testing for smaller or less complex institutions with lower risk profiles for ML/TF and other illicit financial activity. Examples of testing may include the following:

- Sampling suspicious activity alerts, discussing (at a high level) the investigation process with staff, and reviewing the decision-making process regarding SAR filings.
- Determining whether reports, such as SARs and CTRs, are complete and accurate.
- Comparing filed CTRs against reportable transactions that can be identified on the bank's large cash transaction report.
- Determining whether eligible Phase II CTR-exempt customers (non-listed businesses) have been exempted appropriately by reviewing annual reportable cash transactions.
- Confirming the bank has collected and verified Customer Identification Program (CIP) and collected customer due diligence (CDD) data on a sample of new accounts.
- Determining whether the bank has collected beneficial ownership information on a sample of legal entity customers by comparing internal reports with customer files.
- Determining whether independent testing findings have been reported to the board of directors, or to a designated board committee, by reviewing the board or committee minutes.
- Comparing staff training records with the standards outlined in the bank's training policy.

When determining the testing to perform, examiners should consider changes in the bank's business strategies, geographic locations, transaction activity, products, services, customer types, operations, and/or technology. Banks that have had significant changes in these areas since the previous BSA/AML examination may need more extensive testing to determine the adequacy of the BSA/AML compliance program.

Testing should be sufficient to assess the bank's adherence to, and the appropriateness of, its policies, procedures, and processes. Procedures for testing are found within the specific examination procedures sections of this Manual. Examiners should document in the BSA/AML examination plan the rationale regarding the extent and type of testing to be performed. The scope of testing can be expanded to address any issues or concerns identified as part of examination activities. Examiners should also document the rationale for changes to the scope of testing.

Examination Procedures - Risk-Focused BSA/AML Supervision

Objective: ***Determine the examination activities necessary to assess the adequacy of the bank's BSA/AML compliance program, relative to its risk profile, and the bank's compliance with BSA regulatory requirements. If included within the scope of the examination, determine appropriate OFAC compliance examination activities.***

1 Obtain and review the following documents, as appropriate:
- Prior examination reports, supporting workpapers, management's responses to any previously identified BSA issues, and any recommendations for the next examination.
- The BSA/AML risk assessment, if one has been completed by the bank. If the bank has not developed a BSA/AML risk assessment, examiners must develop one. Refer to the *BSA/AML Risk Assessment* section for more information.
- The bank's internal and external BSA/AML independent testing (audit) report(s), including any scope and supporting workpapers.
- Management's responses, including the current status of issues, regarding independent testing or audit results and examination findings.
- Any other information available through the offsite and ongoing monitoring process or from information received from the bank in response to the request letter. This may include:
- BSA reporting available from FinCEN.
- Any other information or correspondence obtained between examinations related to the BSA/AML compliance program, including systems and processes the bank uses to monitor and file on currency transactions and suspicious activity, law enforcement inquiries or engagements, or higher-risk banking operations.

2 Determine whether independent testing is adequate and may be leveraged for use in assessing the bank's BSA/AML compliance program and the bank's compliance with BSA regulatory requirements. To determine the adequacy, consider whether testing was independent and assessed all appropriate ML/TF and other illicit financial activity risks within the bank's operations, and consider whether access was provided to the appropriate independent testing scope and supporting workpapers.

3 Review SARs, CTRs, and CTR exemption information. As appropriate, determine accounts that should be considered for further testing. Consider and analyze the information below for unusual patterns.
- High-volume currency customers.
- The volume and characteristics of SARs filed.
- Frequent SAR subjects.
- The volume and nature of CTRs and CTR exemptions.
- The volume of SARs and CTRs in relation to the bank's products and services, size, asset or deposit growth, and geographic locations

4 Review correspondence between the bank and its regulator(s), if not already completed by the examiner-in-charge or other examination personnel. In addition, review correspondence that the bank and its regulator(s) have received from, or sent to, outside regulatory and law enforcement agencies relating to BSA/AML compliance. Communications, particularly those received from FinCEN, may provide information relevant to the examination, such as the following:
- Filing errors for SARs, CTRs, and CTR exemptions from FinCEN's BSA E-Filing System.
- Civil money penalties issued by, or in process from, FinCEN or state agencies.
- Law enforcement subpoenas, seizures, or "keep-open" requests.

- 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.
- Law enforcement letters acknowledging that the bank provided highly useful information, as necessary and relevant.
- Participation in law enforcement-related information exchanges, as necessary and relevant.

5 Review the bank's information technology sources, systems, and processes used in its BSA/AML compliance program to determine whether additional examiner subject matter expertise is warranted.

6 If included within the scope of the examination, review the bank's policies, procedures, and processes for complying with OFAC-administered laws and regulations. This should include the bank's OFAC risk assessment, independent testing of its OFAC compliance program, and any correspondence between the bank and OFAC (e.g., periodic reporting of prohibited transactions and, if applicable, annual OFAC reports on blocked property, voluntary self-disclosures, and Cautionary or No Action Letters from OFAC). Also, review the bank's use of information technology sources, systems, and processes used in its OFAC compliance program to determine whether additional examiner subject matter expertise is warranted.

Developing the BSA/AML Examination Plan

Objective: ***Based on the bank's risk profile, develop and document the BSA/AML examination plan, including the BSA/AML examination and testing procedures to be completed.***

Examiners must review a bank's BSA/AML compliance program during each examination cycle by conducting appropriate examination and testing procedures. While the BSA/AML examination plan may be adjusted as a result of examination findings, an initial examination plan enables the examiner to establish the examination and testing procedures needed to assess the adequacy of the bank's BSA/AML compliance program, relative to its risk profile, and the bank's compliance with BSA regulatory requirements.

Examiners should develop and document an initial BSA/AML examination plan based on their review of the information highlighted in the *Risk-Focused BSA/AML Supervision* section in this Manual. At a minimum, examiners should assess the adequacy of the BSA/AML compliance program using the examination and testing procedures included in this section (*Developing the BSA/AML Examination Plan*) and in the *Risk-Focused BSA/AML Supervision, BSA/AML Risk Assessment*, *Assessing the BSA/AML Compliance Program*, and *Developing Conclusions and Finalizing the Examination* sections.

In addition to the minimum examination and testing procedures, the following factors should be considered when determining additional examination and testing procedures, if any, to assess the adequacy of the bank's BSA/AML compliance program and the bank's compliance with BSA regulatory requirements:

- The bank's risk profile, size or complexity, and organizational structure.
- The quality of independent testing.
- Changes to the bank's BSA/AML compliance officer or department.
- Expansionary activities.
- Innovations and new technologies.
- Other relevant factors.

Examiners should consider which examination and testing procedures in the *Assessing Compliance with BSA Regulatory Requirements* section are appropriate. BSA/AML examination and testing procedures specific to the bank's products, services, customers, and geographic locations are found in *Risks Associated with Money Laundering and Terrorist Financing*. Not all of the examination and testing procedures are likely to be applicable to every bank or during every examination. Examiners should document any changes to the examination plan resulting from findings that occur after the examination has started.

At larger or more complex banking organizations, examiners may complete various types of BSA/AML examinations or targeted reviews throughout the supervisory plan or cycle to assess BSA/AML compliance. These reviews, which are used to collectively assess the bank's BSA/AML compliance program and compliance with BSA regulatory requirements, may focus on one or more business lines or customer types (e.g., private banking, trade finance, foreign correspondent banking relationships, or currency exchangers), or bank systems (e.g., suspicious activity monitoring or customer due diligence) based on the bank's BSA/AML risk assessment, independent testing, and previous BSA/AML examination findings.

Examiners should determine examination staffing needs based on the scope of work in the examination plan. Consideration should be given to specific BSA/AML expertise needs based on the risk and complexity of the institution as well as information technology sources, systems and processes.

Request Letter Items

Once the examiner determines the necessary examination and testing procedures to be performed, the examiner should prepare a request letter to the bank. Request letter items should be based on the bank's products, services, customers, and geographic locations and should be tailored to the examination plan areas that will be reviewed rather than submitting a comprehensive list to the bank. Additional materials may be requested as needed. Examples of request letter items are detailed in *Appendix H - Request Letter Items*.

Examination Procedures - Developing the BSA/AML Examination Plan

Objective: ***Based on the bank's risk profile, develop and document a BSA/AML examination plan that includes the BSA/AML examination and testing procedures to be completed.***

1. Based on the review of relevant examination documents, in conjunction with the review of the bank's BSA/AML risk assessment, develop and document an initial BSA/AML examination plan. At a minimum, the plan should address:
   - The risk profile of the bank.
   - The scope and adequacy of the bank's BSA/AML independent testing and whether the independent testing can be leveraged to assist in the assessment of the bank's BSA/AML compliance program and the bank's compliance with BSA regulatory requirements.
   - The examination staffing needs, including any subject matter expertise (BSA and non-BSA).
   - The scope of the BSA/AML examination, including the examination and testing procedures necessary to assess the adequacy of the bank's BSA/AML compliance program, the bank's compliance with BSA regulatory requirements, and the bank's adherence to, and the appropriateness of, its policies, procedures, and processes.

2. Based on the review of relevant examination information and the bank's risk profile, determine the examination and testing procedures to be completed. Determine the request letter items that are necessary to complete those examination and testing procedures. Examples of request letter items are detailed in *Appendix H - Request Letter Items*. Examiners are expected to review the request letter items provided by the bank prior to their onsite work.

Section 3: BSA/AML Risk Assessment (revised 2020)

BSA/AML Risk Assessment

Objective: ***Review the bank's BSA/AML risk assessment process, and determine whether the bank has adequately identified the ML/TF and other illicit financial activity risks within its banking operations.***

Examiners must develop an understanding of the bank's ML/TF and other illicit financial activity risks to evaluate the bank's BSA/AML compliance program. This is primarily achieved by reviewing the bank's BSA/AML risk assessment during the scoping and planning process. This section is designed to provide standards for examiners to assess the adequacy of the bank's BSA/AML risk assessment process.

BSA/AML Risk Assessment Process

To assure that BSA/AML compliance programs are reasonably designed to meet BSA regulatory requirements, banks structure their compliance programs to be risk-based. While not a specific legal requirement, a well-developed BSA/AML risk assessment assists the bank in identifying ML/TF and other illicit financial activity risks and in developing appropriate internal controls (i.e., policies, procedures, and processes). Understanding its risk profile enables the bank to better apply appropriate risk management processes to the BSA/AML compliance program to mitigate and manage risk and comply with BSA regulatory requirements. The BSA/AML risk assessment process also enables the bank to better identify and mitigate any gaps in controls. The BSA/AML risk assessment should provide a comprehensive analysis of the bank's ML/TF and other illicit financial activity risks. Documenting the BSA/AML risk assessment in writing is a sound practice to effectively communicate ML/TF and other illicit financial activity risks to appropriate bank personnel. The BSA/AML risk assessment should be provided to all business lines across the bank, the board of directors, management, and appropriate staff.

The development of the BSA/AML risk assessment generally involves the identification of specific risk categories (e.g., products, services, customers, and geographic locations) unique to the bank, and an analysis of the information identified to better assess the risks within these specific risk categories.

Identification of Specific Risk Categories

Generally, the first step in developing the risk assessment is to identify the bank's risk categories. Money laundering, terrorist financing, or other illicit financial activities can occur through any number of different methods or channels. A spectrum of risks may be identifiable even within the same risk category. The bank's BSA/AML risk assessment process should address the varying degrees of risk associated with its products, services, customers, and geographic locations, as appropriate. Improper identification and assessment of risk can have a cascading effect, creating deficiencies in multiple areas of internal controls and resulting in an overall weakened BSA/AML compliance program.

The identification of risk categories is bank-specific, and a conclusion regarding the risk categories should be based on a consideration of all pertinent information. There are no required risk categories, and the number and detail of these categories vary based on the bank's size or complexity, and organizational structure. Any single indicator does not necessarily determine the existence of lower or higher risk.

The subsections within Risks Associated with Money Laundering and Terrorist Financing provide information and discussions on certain products, services, customers, and geographic locations that may present unique challenges and exposures, which banks may need to address through specific policies, procedures, and processes.

Analysis of Specific Risk Categories

Generally, the second step in developing the BSA/AML risk assessment entails an analysis of the information obtained when identifying specific risk categories. The purpose of this analysis is to assess ML/TF and other illicit financial activity risks in order to develop appropriate internal controls to mitigate overall risk. This step may involve evaluating transaction data pertaining to the bank's activities relative to products, services, customers, and geographic locations. For example, it may be useful to quantify risk by assessing the number and dollar amount of domestic and international funds transfers, the nature of private banking customers or foreign correspondent accounts, the existence of payable through accounts, and the domestic and international geographic locations where the bank conducts or transacts business. A detailed analysis is important, because the risks associated with the bank's activities vary. Additionally, the appropriate level and sophistication of the analysis varies by bank.

The following example illustrates the value of the two-step risk assessment process. The information collected by two banks in the first step reflects that each sends 100 international funds transfers per day. Further analysis by the first bank shows that approximately 90 percent of its funds transfers are recurring well-documented transactions for long-term customers. Further analysis by the second bank shows that 90 percent of its funds transfers are nonrecurring or are processed for noncustomers. While these percentages appear to be the same, the risks may be different. This example illustrates that information collected for purposes of the bank's customer identification program and developing the customer due diligence customer risk profile is important when conducting a detailed analysis. Refer to the Customer Identification Program, Customer Due Diligence, and Appendix J – Quantity of Risk Matrix sections for more information.

Various methods and formats may be used to complete the BSA/AML risk assessment; therefore, there is no expectation for a particular method or format. Bank management designs the appropriate method or format and communicates the ML/TF and other illicit financial activity risks to all appropriate parties. When the bank has established an appropriate BSA/AML risk assessment process, and has followed existing policies, procedures, and processes, examiners should not criticize the bank for individual risk or process decisions unless those decisions impact the adequacy of some aspect of the bank's BSA/AML compliance program or the bank's compliance with BSA regulatory requirements.

Updating the Risk Assessment

Generally, risk assessments are updated (in whole or in part) to include changes in the bank's products, services, customers, and geographic locations and to remain an accurate reflection of the bank's ML/TF and other illicit financial activity risks. For example, the bank may need to update its BSA/AML risk assessment when new products, services, and customer types are introduced or the bank expands through mergers and acquisitions. However, there is no requirement to update the BSA/AML risk assessment on a continuous or specified periodic basis.

Assessing the Bank's BSA/AML Risk Assessment

When evaluating the BSA/AML risk assessment, examiners should focus on whether the bank has effective processes resulting in a well-developed BSA/AML risk assessment. Examiners should not take any single indicator as determinative of the existence of a lower- or higher-risk profile for the bank. 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. The bank may determine that some factors should be weighted more heavily than others. For example, the number of funds transfers may be one factor the bank considers when assessing risk. However, to identify and weigh the risks, the bank's risk assessment process may need to consider 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. Regardless of the bank's approach, sound practice would be to document the factors considered, including any weighting.

Examiners should assess whether the bank has developed a BSA/AML risk assessment that identifies its ML/TF and other illicit financial activity risks. Examiners should also assess whether the bank has considered all products, services, customers, and geographic locations, and whether the bank analyzed the information relative to those risk categories.

For the purposes of the examination, whenever the bank has not developed a BSA/AML risk assessment, or the BSA/AML risk assessment is inadequate, examiners must develop a BSA/AML risk assessment for the bank based on available information. An examiner-developed BSA/AML risk assessment generally is not as comprehensive as one developed by the bank. Examiners should have a general understanding of the bank's ML/TF and other illicit financial activity risks from the examination scoping and planning process. This information should be evaluated using the two-step approach detailed in the BSA/AML Risk Assessment Process subsection above. Examiners may also refer to **Appendix J - Quantity of Risk Matrix** when completing this evaluation.

Developing a BSA/AML Compliance Program Based on the BSA/AML Risk Assessment

The bank structures its BSA/AML compliance program to address its risk profile, based on the bank's assessment of risks, as well as to comply with BSA regulatory requirements. Specifically, the bank should develop appropriate policies, procedures, and processes to monitor and control its ML/TF and other illicit financial activity risks. For example, the bank's monitoring system to identify, research, and report suspicious activity should be risk-based to incorporate any necessary

additional screening for higher-risk products, services, customers, and geographic locations as identified by the bank's BSA/AML risk assessment. Independent testing (audit) should review the bank's BSA/AML risk assessment, including how it is used to develop the BSA/AML compliance program. Refer to Appendix I - Risk Assessment Link to the BSA/AML Compliance Program for a chart depicting the expected link of the BSA/AML risk assessment to the BSA/AML compliance program.

Consolidated BSA/AML Risk Assessment

Banks that choose to implement a consolidated or partially consolidated BSA/AML compliance program should assess risk within business lines and across activities and legal entities. Consolidating ML/TF and other illicit financial activity risks for larger or more complex banking organizations may assist senior management and the board of directors in identifying, understanding, and appropriately mitigating risks within and across the banking organization. To understand ML/TF and other illicit financial activity risk exposures, the banking organization should communicate across all business lines, activities, and legal entities. Identifying a vulnerability in one aspect of the banking organization may indicate vulnerabilities elsewhere. Refer to the *BSA/AML Compliance Program Structures* section for more information.

BSA/AML Risk Assessment Exam Procedures

Objective. ***Determine the adequacy of the bank's BSA/AML risk assessment process, and determine whether the bank has adequately identified the ML/TF and other illicit financial activity risks within its banking operations.***

1. Determine whether the bank has identified ML/TF and other illicit financial activity risks associated with the products, services, customers, and geographic locations unique to the bank.

2. Determine whether the bank has analyzed, and assessed the ML/TF and other illicit financial activity risks within the products, services, customers, and geographic locations unique to the bank.

3. Determine whether the bank has a process for updating its BSA/AML risk assessment as necessary to reflect changes in the bank's products, services, customers, and geographic locations and to remain an accurate reflection of its ML/TF and other illicit financial activity risks.
4. If the bank has not developed a BSA/AML risk assessment, or if the BSA/AML risk assessment is inadequate, complete a BSA/AML risk assessment for the bank.

5. Document and discuss with the bank any findings related to the BSA/AML risk assessment process.

Section 4: Assessing the BSA/AML Compliance Program (revised 2020)

Assessing the BSA/AML Compliance Program

Objective: ***Assess whether the bank has designed, implemented, and maintains an adequate BSA/AML compliance program that complies with BSA regulatory requirements.***

Banks must establish and maintain procedures reasonably designed to assure and monitor compliance with BSA regulatory requirements (BSA/AML compliance program). The BSA/AML compliance program must be written, approved by the board of directors, and noted in the board minutes. To achieve the purposes of the BSA, the BSA/AML compliance program should be commensurate with the bank's ML/TF and other illicit financial activity risk profile. Refer to the BSA/AML Risk Assessment section and Appendix I - Risk Assessment Link to the BSA/AML Compliance Program for more information.

Written policies, procedures, and processes alone are not sufficient to have an adequate BSA/AML compliance program; practices that correspond with the bank's written policies, procedures, and processes are needed for implementation. Importantly, policies, procedures, processes, and practices should align with the bank's unique ML/TF and other illicit financial activity risk profile. The BSA/AML compliance program must provide for the following requirements:

- A system of internal controls to assure ongoing compliance.
- Independent testing for compliance to be conducted by bank personnel or by an outside party.
- Designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance (BSA compliance officer).
- Training for appropriate personnel.

In addition, the BSA/AML compliance program must include a customer identification program (CIP) with risk-based procedures that enable the bank to form a reasonable belief that it knows the true identity of its customers. The BSA/AML compliance program must also include appropriate risk-based procedures for conducting ongoing customer due diligence (CDD) and complying with beneficial ownership requirements for legal entity customers as set forth in regulations issued by Financial Crimes Enforcement Network (FinCEN). Refer to the Customer Identification Program, Customer Due Diligence, and Beneficial Ownership Requirements for Legal Entity Customers sections for more information.

The assessment of the adequacy of the bank's BSA/AML compliance program is bank-specific, and examiners should consider all pertinent information. A 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 examination and testing procedures is necessary to support overall conclusions regarding the BSA/AML compliance program. BSA/AML examination findings should be discussed with relevant bank management, and findings must be included in

the report of examination (ROE) or supervisory correspondence.

Examination Procedures - Assessing the BSA/AML Compliance Program

Objective: ***Determine whether the bank has designed, implemented, and maintains an adequate BSA/AML compliance program that complies with BSA regulatory requirements.***

1. Confirm that the bank's BSA/AML compliance program is written, has been approved by the board of directors, and that the approval was noted in the board minutes.

2. Review the BSA/AML compliance program and determine whether it is tailored to the bank's ML/TF and other illicit financial activity risk profile. Determine whether the bank's compliance program contains the following requirements:

   - A system of internal controls to assure ongoing compliance.
   - Independent testing for compliance to be conducted by bank personnel or an outside party.
   - Designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance (BSA compliance officer).
   - Training for appropriate personnel.

3. Determine whether the bank's CIP, risk-based CDD, and beneficial ownership procedures are included as part of the BSA/AML compliance program.

4. Determine whether the initial BSA/AML examination plan should be adjusted based on new information identified during the examination. Document and support any changes made.

Preliminary Evaluation

Once examiners complete the review of the bank's BSA/AML compliance program, they should develop and document a preliminary assessment of the bank's program. At this point, examiners should revisit the initial BSA/AML examination plan to determine whether additional areas of review are necessary to assess the adequacy of the bank's BSA/AML compliance program, relative to its risk profile, and the bank's compliance with BSA regulatory requirements. These adjustments to the initial examination plan could be based on information identified during the review, such as a new product or business line at the bank or independent testing report findings. Examiners should document and support any changes to the examination plan, if necessary, then proceed to the applicable examination and testing procedures in Assessing Compliance with BSA Regulatory Requirements, Risks Associated with Money Laundering and Terrorist Financing, and Office of Foreign Assets Control. Once all relevant examination and testing procedures are completed as documented in the examination plan, examiners should proceed to Developing Conclusions and Finalizing the Examination.

BSA/AML Internal Controls

Objective: ***Assess the bank's system of internal controls to assure ongoing compliance with BSA regulatory requirements.***

The board of directors, acting through senior management, is ultimately responsible for ensuring that the bank maintains a system of internal controls to assure ongoing compliance with BSA regulatory requirements. Internal controls are the bank's policies, procedures, and processes designed to mitigate and manage ML/TF and other illicit financial activity risks and to achieve compliance with BSA regulatory requirements. The board of directors plays an important role in establishing and maintaining an appropriate culture that places a priority on compliance, and a structure that provides oversight and holds senior management accountable for implementing the bank's BSA/AML internal controls. The system of internal controls, including the level and type, should be commensurate with the bank's size or complexity, and organizational structure. Large or more complex banks may implement specific 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, bank-wide BSA/AML compliance program.

Examiners should determine whether the bank's internal controls are designed to assure ongoing compliance with BSA regulatory requirements and:

- Incorporate the bank's BSA/AML risk assessment and the identification of ML/TF and other illicit financial activity risks, along with any changes in those risks.
- Provide for program continuity despite changes in operations, management, or employee composition or structure.
- Facilitate oversight of information technology sources, systems, and processes that support BSA/AML compliance.
- Provide for timely updates in response to changes in regulations.
- Incorporate dual controls and the segregation of duties to the extent possible. For example, employees who complete the reporting forms (such as suspicious activity reports (SARs), currency transaction reports (CTRs), and CTR exemptions) generally should not also be responsible for the decision to file the reports or grant the exemptions.
- Include mechanisms to identify and inform the board of directors, or a committee thereof, and senior management of BSA compliance initiatives, identified compliance deficiencies and corrective action taken, and notify the board of directors of SARs filed.
- Identify and establish specific BSA compliance responsibilities for bank personnel and provide oversight for execution of those responsibilities, as appropriate.

This list is not all-inclusive and should be tailored to reflect the bank's ML/TF and other illicit financial activity risk profile. More information concerning individual regulatory requirements and specific risk areas is in the Assessing Compliance with BSA Regulatory Requirements and Risks Associated with Money Laundering and Terrorist Financing sections.

Examiners should determine whether the bank's system of internal controls is designed to mitigate and manage the ML/TF and other illicit financial activity risks, and comply with BSA regulatory requirements. Examiners should assess the adequacy of internal controls based on the factors listed above.

Examination Procedures - BSA/AML Internal Controls

Objective: ***Determine whether the bank has implemented a system of internal controls that assures ongoing compliance with BSA regulatory requirements.***

1. Determine whether the bank's system of internal controls (i.e., policies, procedures, and processes) is designed to:
   - Mitigate and manage ML/TF and other illicit financial activity risks, and
   - Assure ongoing compliance with BSA regulatory requirements.

2. Determine whether the internal controls:
   - Incorporate the bank's BSA/AML risk assessment and the identification of ML/TF and other illicit financial activity risks, along with any changes in those risks.
   - Provide for program continuity despite changes in operations, management, or employee composition or structure.
   - Facilitate oversight of information technology sources, systems, and processes that support BSA/AML compliance.
   - Provide for timely updates to implement changes in regulations.
   - Incorporate dual controls and the segregation of duties to the extent possible.
   - Include mechanisms to identify and escalate BSA compliance issues to management and the board of directors, or a committee thereof, as appropriate.
   - Inform the board of directors, or a committee thereof, and senior management of compliance initiatives, identified compliance deficiencies, and corrective action taken, and notify the board of directors of SARs filed.
   - Identify and establish specific BSA compliance responsibilities for bank personnel and provide oversight for execution of those responsibilities, as appropriate.

BSA/AML Independent Testing

Objective: ***Assess the adequacy of the bank's independent testing program.***

The purpose of independent testing (audit) is to assess the bank's compliance with BSA regulatory requirements, relative to its risk profile, and assess the overall adequacy of the BSA/AML compliance program. Independent testing should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties.

Banks that do not employ outside auditors or consultants or do not have internal audit departments may comply with this requirement by using qualified bank staff who are not involved in the function being tested. Banks engaging outside auditors or consultants should ensure that the persons conducting the BSA/AML independent testing are not involved in other BSA-related functions at the bank that may present a conflict of interest or lack of independence, such as training or developing policies and procedures. Regardless of who performs the independent testing, the party conducting the BSA/AML independent testing should report directly to the board of directors or to a designated board committee comprised primarily, or completely, of outside directors. Banks with a community focus, less complex operations, and lower-risk profiles for ML/TF and other illicit financial activities may consider utilizing a shared resource as part of

a collaborative arrangement to conduct independent testing.

There is no regulatory requirement establishing BSA/AML independent testing frequency. Independent testing, including the frequency, should be commensurate with the ML/TF and other illicit financial activity risk profile of the bank and the bank's overall risk management strategy. The bank may conduct independent testing over periodic intervals (for example, every 12-18 months) and/or when there are significant changes in the bank's risk profile, systems, compliance staff, or processes. More frequent independent testing may be appropriate when errors or deficiencies in some aspect of the BSA/AML compliance program have been identified or to verify or validate mitigating or remedial actions.

Independent testing of specific BSA requirements should be risk-based and evaluate the quality of risk management related to ML/TF and other illicit financial activity risks for significant banking operations across the organization. Risk-based independent testing focuses on the bank's risk assessment to tailor independent testing to the areas identified as being of greatest risk and concern. Risk-based independent testing programs vary depending on the bank's size or complexity, organizational structure, scope of activities, risk profile, quality of control functions, geographic diversity, and use of technology. Risk-based independent testing should include evaluating pertinent internal controls and information technology sources, systems, and processes used to support the BSA/AML compliance program. Consideration should also be given to the expansion into new product lines, services, customer types, and geographic locations through organic growth or merger activity.

The independent testing should evaluate the overall adequacy of the bank's BSA/AML compliance program and the bank's compliance with BSA regulatory requirements. This evaluation helps inform the board of directors and senior management of weakness, or areas in need of enhancements or stronger controls. Typically, this evaluation includes an explicit statement in the report(s) about the bank's overall compliance with BSA regulatory requirements. At a minimum, the independent testing should contain sufficient information for the reviewer (e.g., board of directors, senior management, BSA compliance officer, review auditor, or an examiner) to reach a conclusion about the overall adequacy of the BSA/AML compliance program.

To contain sufficient information to reach this conclusion, independent testing of the BSA/AML compliance program and BSA regulatory requirements may include a risk-based review of whether:

- The bank's BSA/AML risk assessment aligns with the bank's risk profile (products, services, customers, and geographic locations).
- The bank's policies, procedures, and processes for BSA compliance align with the bank's
- risk profile.
- The bank adheres to its policies, procedures, and processes for BSA compliance.
- The bank complies with BSA recordkeeping and reporting requirements (e.g., customer information program (CIP), customer due diligence (CDD), beneficial ownership, suspicious activity reports (SARs), currency transaction reports (CTRs) and CTR exemptions, and information sharing requests).
- The bank's overall process for identifying and reporting suspicious activity is adequate. This review may include evaluating filed or prepared SARs to determine their accuracy, timeliness, completeness, and conformance to the bank's policies, procedures, and processes.

- The bank's information technology sources, systems, and processes used to support the BSA/AML compliance program are complete and accurate. These may include reports or automated programs used to: identify large currency transactions, aggregate daily currency transactions, record monetary instrument sales and funds transfer transactions, and provide analytical and trend reports.
- Training is provided for appropriate personnel, tailored to specific functions and positions, and includes supporting documentation.
- Management took appropriate and timely action to address any violations and other deficiencies noted in previous independent testing and regulatory examinations, including progress in addressing outstanding supervisory enforcement actions, if applicable.

Auditors should document the independent testing scope, procedures performed, transaction testing completed, and any findings. All independent testing documentation and supporting workpapers should be available for examiner review. Violations; exceptions to bank policies, procedures, or processes; or other deficiencies noted during the independent testing should be documented and reported to the board of directors or a designated board committee in a timely manner. The board of directors, or a designated board committee, and appropriate staff should track deficiencies and document progress implementing corrective actions.

Examiners should review relevant documents such as the auditor's report(s), scope, and supporting workpapers, as needed. Examiners should determine whether there is an explicit statement in the report(s) about the bank's overall compliance with BSA regulatory requirements or, at a minimum, sufficient information to reach a conclusion about the overall adequacy of the BSA/AML compliance program. Examiners should determine whether the testing was conducted in an independent manner. Examiners may also evaluate, as applicable, the subject matter expertise, qualifications and independence of the person or persons performing the independent testing. Examiners should determine whether the independent testing sufficiently covers ML/TF and other illicit financial activity risks within the bank's operations and whether the frequency is commensurate with the bank's risk profile. Examiners should also review whether violations; exceptions to policies, procedures, or processes; or other deficiencies are reported to the board of directors or a designated board committee in a timely manner, whether they are tracked, and whether corrective actions are documented.

Examination Procedures - BSA/AML Independent Testing

Objective: ***Determine whether the bank has designed, implemented, and maintains an adequate BSA/AML independent testing program for compliance with BSA regulatory requirements.***

1. Determine whether the BSA/AML independent testing (audit) is independent (i.e., performed by a person or persons not involved with the function being tested or other BSA-related functions at the bank that may present a conflict of interest or lack of independence).

2. Determine whether independent testing addresses the overall adequacy of the BSA/AML compliance program, including policies, procedures, and processes. Typically, the report includes an explicit statement about the bank's overall compliance with BSA regulatory requirements. At a minimum, the independent testing should contain sufficient information for the reviewer to reach a conclusion about the overall adequacy of the BSA/AML compliance program.

3. Through a review of board minutes or other board of directors' materials, determine whether persons conducting the independent testing reported directly to the board of directors or to a designated board committee comprised primarily, or completely, of outside directors. Determine whether independent testing results were provided to the board of directors and senior management.

4. Review independent testing reports, scope, and supporting workpapers to determine whether they are comprehensive, accurate, adequate, and timely, relative to the bank's risk profile. As applicable,[17] evaluate the qualifications and subject matter expertise of the person or persons performing the independent test. Although there are no specific regulatory requirements for the development of an independent test, consider whether the independent testing includes, as applicable, an evaluation of:

   - The BSA/AML risk assessment.
   - The relevant changes in bank activities since the last independent test.
   - The policies, procedures, and processes governing the BSA/AML compliance program and other BSA regulatory requirements, and personnel's adherence to those policies, procedures, and processes.
   - The bank's adherence to BSA reporting and recordkeeping requirements.
   - The bank's information technology sources, systems, and processes used to support the BSA/AML compliance program and whether they are complete and accurate. These may include reports or automated programs used to: identify large currency transactions, aggregate daily currency transactions, record monetary instrument sales and funds transfer transactions, and provide analytical and trend reports.
   - Training for appropriate personnel and whether it is tailored to specific functions and positions and includes supporting documentation.
   - Management's actions to appropriately and timely address any violations and other deficiencies noted in previous independent testing and regulatory examinations, including progress in addressing outstanding supervisory enforcement actions, if applicable.

5. Determine whether independent testing includes, as applicable, an evaluation of suspicious activity monitoring systems and the system's ability to identify potentially suspicious activity. Although there are no specific regulatory requirements for the development of an independent test, consider whether the independent testing includes, as applicable, an evaluation of:

   - The system's methodology for monitoring transactions and accounts for potentially suspicious activity.
   - The system's ability to generate monitoring reports.
   - Filtering criteria, as appropriate, to determine whether they are reasonable, tailored to the bank's risk profile, and include higher-risk products, services, customers, and geographic locations.
   - Policies, procedures, and processes for suspicious activity monitoring systems.

6. Determine whether the independent testing includes a review and evaluation of the overall suspicious activity monitoring and reporting process. Although there are no specific regulatory requirements for the development of an independent test, consider whether the independent testing includes, as applicable, an evaluation of:

   - The identification or alert process.

- The management of alerts, research, SAR decision making, SAR completion and filing, and monitoring of continuous activity.
- Policies, procedures, and processes for referring potentially suspicious activity from all operational areas and business lines (such as, trust services, private banking, foreign correspondent banking) to the personnel or department responsible for evaluating potentially suspicious activity.

7. Determine whether the independent testing performed was adequate, relative to the bank's risk profile.

BSA Compliance Officer

Objective: ***Confirm that the bank's board of directors has designated a qualified individual or individuals (BSA compliance officer) responsible for coordinating and monitoring day-to-day compliance with BSA regulatory requirements. Assess whether the BSA compliance officer has the appropriate authority, independence, access to resources, and competence to effectively execute all duties.***

The bank's board of directors must designate a qualified individual or individuals to serve as the BSA compliance officer. 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, including managing the bank's compliance with BSA regulatory requirements. The board of directors is ultimately responsible for the bank's BSA/AML compliance and should provide oversight for senior management and the BSA compliance officer in the implementation of the bank's board-approved BSA/AML compliance program.

The act by the bank's board of directors of appointing a BSA compliance officer is not, by itself, sufficient to meet the regulatory requirement to establish and maintain a BSA/AML compliance program reasonably designed to assure and monitor compliance with the BSA. The board of directors is responsible for ensuring that the BSA compliance officer has appropriate authority, independence, and access to resources to administer an adequate BSA/AML compliance program based on the bank's ML/TF and other illicit financial activity risk profile. The BSA compliance officer should regularly report the status of ongoing compliance with the BSA to the board of directors and senior management so that they can make informed decisions about existing risk exposure and the overall BSA/AML compliance program. Reporting to the board of directors or a designated board committee about the status of ongoing compliance should include pertinent BSA-related information, including the required notification of suspicious activity report (SAR) filings.

The BSA compliance officer is responsible for carrying out the board's direction, including the implementation of the bank's BSA/AML policies, procedures, and processes. The BSA compliance officer may delegate BSA/AML duties to staff, but the officer is responsible for overseeing the day-to-day BSA/AML compliance program.

The BSA compliance officer should be competent, as demonstrated by knowledge of the BSA and related regulations, implementation of the bank's BSA/AML compliance program, and understanding of the bank's ML/TF and other illicit financial activity risk profile associated with

its banking activities. The actual title of the individual responsible for overall BSA compliance is not important; however, the individual's authority, independence, and access to resources within the bank is critical.

Indicators of appropriate authority of the BSA compliance officer may include senior management seeking the BSA compliance officer's input regarding: the ML/TF and other illicit financial activity risks related to expansion into new products, services, customer types and geographic locations; or operational changes, such as the implementation of, or adjustments to, systems that impact the BSA compliance function. Indicators of appropriate independence of the BSA compliance officer may include, but are not limited to: clear lines of reporting and communication ultimately up to the board of directors or a designated board committee that do not compromise the BSA compliance officer's independence, the ability to undertake the BSA compliance officer's role without undue influence from the bank's business lines, and identification and reporting of issues to senior management and the board of directors.

The BSA compliance officer should have access to suitable resources. This may include, but is not limited to: adequate staffing with the skills and expertise necessary for the bank's overall risk level (based on products, services, customers, and geographic locations), size or complexity, and organizational structure; and systems to support the timely identification, measurement, monitoring, reporting, and management of the bank's ML/TF and other illicit financial activity risks.

Examiners should confirm that the bank's board of directors has designated an individual or individuals responsible for the overall BSA/AML compliance program who are appropriately qualified. Examiners should review reports to the board of directors and senior management regarding the status of ongoing compliance and pertinent BSA-related information, including the required notification of SAR filings. Examiners should confirm that the BSA compliance officer has the appropriate authority, independence, and access to resources.

Examination Procedures - BSA Compliance Officer

Objective: ***Confirm that the bank's board of directors has designated a qualified individual or individuals (BSA compliance officer) responsible for coordinating and monitoring day-to-day compliance with BSA regulatory requirements. Determine whether the BSA compliance officer has the appropriate authority, independence, access to resources, and competence to effectively execute all duties.***

1. Confirm that the bank's board of directors has designated an individual or individuals responsible for the overall BSA/AML compliance program.

2. Confirm that the BSA compliance officer regularly updates the board of directors and senior management about the status of ongoing compliance with the BSA and pertinent BSA-related information, including the required notification of SAR filings.

3. Determine whether the BSA compliance officer is competent, as demonstrated by knowledge of the BSA and related regulations, implementation of the bank's BSA/AML compliance program, and understanding of the bank's ML/TF and other illicit financial activity risk profile associated with its banking activities.

4. Determine whether the BSA compliance officer has the appropriate authority.

5. Determine whether the BSA compliance officer has the appropriate independence. Indicators of appropriate independence may include, but are not limited to:
   - Clear lines of reporting and communication ultimately up to the board of directors, or a designated board committee, that do not compromise the BSA compliance officer's independence.
   - The ability to undertake the BSA compliance officer's role without undue influence from the bank's business lines.
   - Identification and reporting of issues to senior management and the board of directors.

6. Determine whether the BSA compliance officer has access to suitable resources. Indicators of suitable resources may include, but are not limited to:
   - Adequate staffing with the skills and expertise for the bank's overall risk level (based on products, services, customers, and geographic locations), size or complexity, and organizational structure.
   - Systems to support the identification, measurement, monitoring, reporting, and management of the bank's ML/TF and other illicit financial activity risks.

BSA/AML Training

Objective: ***Confirm that the bank has developed a BSA/AML training program and delivered training to appropriate personnel.***

Banks must provide training for appropriate personnel. Training should cover the aspects of the BSA that are relevant to the bank and its risk profile, and appropriate personnel includes those whose duties require knowledge or involve some aspect of BSA/AML compliance. Training should cover BSA regulatory requirements, supervisory guidance, and the bank's internal BSA/AML policies, procedures, and processes. Training should be tailored to each individual's specific responsibilities, as appropriate. In addition, targeted training may be necessary for specific ML/TF and other illicit financial activity risks and requirements applicable to certain business lines or operational units, such as lending, trust services, foreign correspondent banking, and private banking. An overview of the purposes of the BSA and its regulatory requirements are typically provided to new staff during employee orientation or reasonably thereafter. The BSA compliance officer and BSA compliance staff should receive periodic training that is relevant and appropriate to remain informed of changes to regulatory requirements and changes to the bank's risk profile.

The board of directors and senior management should receive foundational training and be informed of changes and new developments in the BSA, including its implementing regulations, the federal banking agencies' regulations, and supervisory guidance. While the board of directors may not require the same degree of training as banking operations personnel, the training should provide board members with sufficient understanding of the bank's risk profile and BSA regulatory requirements. Without a general understanding of the BSA, it is more difficult for the board of directors to provide adequate oversight of the BSA/AML compliance program, including approving the written BSA/AML compliance program, establishing appropriate independence for

the BSA/AML compliance function, and providing sufficient BSA/AML resources.

Periodic training for appropriate personnel should incorporate current developments and changes to BSA regulatory requirements; supervisory guidance; internal policies, procedures, and processes; and the bank's products, services, customers, and geographic locations. Changes to information technology sources, systems, and processes used in BSA compliance may be covered during training for appropriate personnel. The training program may be used to reinforce the importance that the board of directors and senior management place on the bank's compliance with the BSA and that all employees understand their role in maintaining an adequate BSA/AML compliance program.

Training programs should include examples of money laundering and suspicious activity monitoring and reporting that are tailored, as appropriate, to each operational area. For example, training for tellers should focus on examples involving large currency transactions or suspicious activities, and training for the loan department should provide examples involving money laundering through lending arrangements. The bank should provide training for any agents who are responsible for conducting BSA-related functions on behalf of the bank. If the bank relies on another financial institution or other party to perform training, appropriate documentation should be maintained.

Banks should document their training programs. Training and testing materials (if training-related testing is used by the bank), and the dates of training sessions should be maintained by the bank. Additionally, training materials and records should be available for auditor or examiner review. The bank should maintain documentation of attendance records and any failures of personnel to take the required training in a timely manner, as well as any corrective actions taken to address such failures.

Examiners should determine whether all personnel whose duties require knowledge of the BSA are included in the training program and whether materials include training on BSA regulatory requirements, supervisory guidance, and the bank's internal BSA/AML policies, procedures, and processes.

Examination Procedures - BSA/AML Training

Objective: ***Determine whether the bank has developed a BSA/AML training program and delivered training to appropriate personnel.***

1. Determine whether all personnel whose duties require knowledge of the BSA are included in the training program, that the BSA compliance officer and BSA compliance staff have received periodic training that is relevant and appropriate, and that the board of directors receives appropriate training that may include changes or new developments in the BSA.

2. Determine whether the bank's training program materials address:
   - The importance that the board of directors and senior management place on ongoing education, training, employee accountability, and compliance.
   - Results of previous findings of noncompliance with internal policies and regulatory requirements, if applicable.
   - An overview of the purposes of the BSA and its regulatory requirements, supervisory guidance, and the bank's internal policies, procedures, and processes.

- Different forms of ML/TF and other illicit financial activity risks as they relate to identification and examples of suspicious activity.
- Information tailored to specific risks of individual business lines or operational units.
- Information on current developments and changes to the BSA regulatory requirements.
- Adequate training for any agents who are responsible for conducting BSA-related functions on behalf of the bank.

3. Determine whether the bank maintains documentation of the dates of training sessions and training and testing materials (if testing is used by the bank). Documentation should include attendance records and any failures of personnel to take the requisite training in a timely manner, as well as any corrective actions taken to address such failures.

Section 5: Developing Conclusions and Finalizing the Exam (revised 2020)

Developing Conclusions and Finalizing the Exam

Objective: ***Formulate conclusions about the adequacy of the bank's BSA/AML compliance program, relative to its risk profile, and the bank's compliance with BSA regulatory requirements; develop an appropriate supervisory response; and communicate BSA/AML examination findings to the bank.***

In the final phase of the BSA/AML examination, examiners should assemble all findings from the examination and testing procedures completed. From those findings, examiners should develop and document conclusions about the adequacy of the bank's BSA/AML compliance program, relative to its risk profile, and the bank's compliance with BSA regulatory requirements. When formulating conclusions, examiners are reminded that banks have flexibility in the design of their BSA/AML compliance programs, which will vary based on the bank's risk profile, size or complexity, and organizational structure. Examiners should primarily focus on whether the bank has established appropriate processes to manage ML/TF and other illicit financial activity risks, and that the bank has complied with BSA requirements.

Examiners should discuss with the bank their preliminary conclusions, which may include strengths, weaknesses, any deficiencies or violations, if applicable, and necessary remediation of any deficiencies or violations. Minor weaknesses, deficiencies, and technical violations alone are not indicative of an inadequate BSA/AML compliance program and should not be communicated as such. Conclusions regarding the adequacy of the bank's BSA/AML compliance program and any significant findings should be presented in a written format for inclusion in the report of examination (ROE).

In formulating a written conclusion for the ROE, examiners do not need to discuss every procedure performed during the examination. Written comments should convey to the reader whether the overall BSA/AML compliance program is adequate. The comments should cover areas or subjects pertinent to examiner findings and conclusions. Examiners should prepare workpapers in sufficient detail to support discussions in the ROE. To the extent items are discussed in the workpapers but not the ROE, the workpapers should appropriately document each item, 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 findings included in the ROE. Examiners should organize and reference workpapers and document conclusions and supporting information within internal agency systems, as appropriate.

Examiners should determine and document what supervisory response, if any, is recommended. The BSA/AML examination findings may include violations of laws or regulations or other deficiencies. Any substantive deficiencies in the BSA/AML compliance program, including violations, should be included in the ROE in such a manner that allows the reader to understand the cause of the deficiencies. The extent to which violations and other deficiencies affect the examiner's evaluation of the adequacy of the bank's BSA/AML compliance program and the bank's

compliance with BSA regulatory requirements is based on the nature, duration, and severity of the problem. In some cases, the appropriate supervisory response is for the bank to correct the violations or other deficiencies as part of the normal supervisory process. These remediation efforts should be documented in the ROE. In appropriate circumstances, however, an agency may take either informal or formal enforcement actions to address violations of BSA regulatory requirements.

Violations or deficiencies can be caused by a number of issues including, but not limited to, the following:

- Management has not appropriately assessed the bank's ML/TF and other illicit financial activity risks.
- Management has not created or enhanced policies, procedures, and processes.
- Management or employees disregard, are unaware of, or misunderstand regulatory requirements or internal policies, procedures, or processes.
- Management has not adjusted the BSA/AML compliance program commensurate with growth in higher-risk operations (products, services, customers, and geographic locations).
- Management has not provided sufficient staffing for the bank's risk profile.
- Management has not appropriately communicated changes in internal policies, procedures, and processes.

Systemic or Repeat Violations

Systemic or repeat violations involve either a substantive deficiency or a repeated failure to comply with BSA regulatory requirements, including the requirement to establish and maintain a reasonably designed BSA/AML compliance program. A substantive deficiency or repeated failure to comply with BSA regulatory requirements could negatively affect the bank's ability to manage ML/TF and other illicit financial activity risks. Systemic violations are the result of substantively deficient systems or processes that fail to obtain, analyze, or maintain required information, or to report customers, accounts, or transactions, as required under various provisions of the BSA. Repeat violations are repetitive occurrences of the same or similar issues.

When evaluating whether deficiencies constitute systemic or repeat violations, examiners must analyze the pertinent facts and the totality of circumstances, including whether the deficiencies are frequently recurring, regular, or usual, and whether the deficiencies are of the same or similar nature.

Considerations in determining whether a violation is systemic 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

consider 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 the violations 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 (e.g., the bank's currency transaction reporting thresholds are inconsistent with BSA regulations).
- Whether there is a common source or cause of the violations.
- Whether the violations were the result of errors in software programming or implementation.

Systemic or repeat violations of the BSA or other deficiencies could have a negative impact on the adequacy of the bank's BSA/AML compliance program. *Appendix R – Interagency Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements* for more information regarding when a bank's BSA/AML compliance program may be deficient as a result of systemic noncompliance. All systemic violations and substantive deficiencies should be brought to the attention of the bank's board of directors and senior management and documented in the ROE or other supervisory correspondence directed to the board of directors. When systemic instances of noncompliance are identified, examiners should consider the noncompliance in the context of the overall program (internal controls, independent testing, designated individual or individuals, and training) and refer to *Appendix R – Interagency Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements* for more information regarding when a bank's BSA/AML compliance program may be deficient as a result of systemic noncompliance. All systemic violations and substantive deficiencies should be brought to the attention of the bank's board of directors and senior management and documented in the ROE or other supervisory correspondence directed to the board of directors.

Types of systemic or repeat 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 1010.620).
- Frequent, consistent, or recurring late currency transaction report (CTR) or suspicious activity report (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 Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements" 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 potentially suspicious activity, involves a pattern or practice of noncompliance with the filing requirement, or represents a significant or egregious situation."

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. Corrective action for isolated or technical violations is usually undertaken by the bank within the normal course of business.

Multiple isolated or technical violations throughout bank departments or divisions can indicate systemic or repeat violations. Examiners should consider multiple isolated or technical violations in the context of all examination findings, oversight provided by the bank's board of directors and senior management, and the bank's risk profile.

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.
- 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.

Section 6: Customer Identification Program (revised 2014)

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. 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. 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 1020.100).

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 is obtained from each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each customer. Banks should conduct a risk assessment of their customer base and product offerings, and in determining the risks, consider:

- The types of accounts offered by the bank.
- The bank's methods of opening accounts.
- The types of identifying information available.
- The bank's size, location, and customer base, 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. 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. 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 1020.315(b)(1) through (4).

Customer Information Required

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

- Name.
- Date of birth for individuals.
- Address.
- Identification number.

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 1020.220] paragraph (a)(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 uses documents, nondocumentary methods, or a combination of both.

Verification Through Documents

A bank using documentary methods to verify a customer's identity must have procedures that set forth the minimum acceptable documentation. The CIP rule gives examples of types of documents that have long been considered primary sources of identification. The rule reflects the federal banking agencies' expectations that banks 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 uses. 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 obtains 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. For credit cards, the retention period is five years after the account closes or becomes dormant.

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

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

Editor's Note: We have elected to omit footnotes. However the footnote for this subject states:

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 1010.430.

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, Federal Reserve, FDIC, NCUA, OCC, and OTS, April 28, 2005.

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. Banks are 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.

As of the publication date of this manual, there are no designated government lists to verify specifically for CIP purposes. Customer comparisons to Office of Foreign Assets Control lists and 31 CFR 1010.520 (commonly referred to as section 314(a) requests) remain separate and distinct requirements.

Adequate Customer Notice

The CIP must include procedures for providing customers with adequate notice that the bank is requesting information to verify their identities. The notice must generally describe the bank's identification requirements and be provided in a manner that is reasonably designed to allow a customer to view it or otherwise receive the notice before the account is opened.

Examples include posting the notice in the lobby, on a Web site, or within loan application documents. Sample language is provided in the regulation:

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

Reliance on Another Financial Institution

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

- The relied-upon financial institution is subject to a rule implementing the AML program requirements of 31 USC 5318(h) and is regulated by a federal functional regulator.
- 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.

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.

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 1020.220(a)(1)).

5. Evaluate the bank's audit and training programs to ensure that the CIP is adequately incorporated (31 CFR 1020.220(a)(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 1020.220(a)(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. [51]
   - 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 1020.220(a)(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 1020.220(a)(2)).)
   - Obtained from each customer, before opening the account, the identity information required by the CIP (31 CFR 1020.220(a)(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 1020.220(a)(2)(ii)).
- Appropriately resolved situations in which customer identity could not be reasonably established (31 CFR 1020.220(a)(2)(iii)).
- 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 1020.220(a)(3)).
- Compared the customer's name against the list of known or suspected terrorists or terrorist organizations, if applicable (31 CFR 1020.220(a)(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, non-systemic errors (such as an insignificant number of data entry errors) from CIP requirements without compromising the effectiveness of its CIP (31 CFR 1020.220(a)(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 1020.220(a)(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 1020.220(a)(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 1020.220(a)(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.

Section 7: Customer Due Diligence (revised 2018)

Customer Due Diligence — Overview

Objective. ***Assess the bank's compliance with the regulatory requirements for customer due diligence (CDD).***

The cornerstone of a strong BSA/AML compliance program is the adoption and implementation of risk-based 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 is to enable the bank to understand the nature and purpose of customer relationships, which may include understanding the types of transactions in which a customer is likely to engage. These processes assist the bank in determining when transactions are potentially suspicious.

Effective CDD policies, procedures, and processes provide the critical framework that enables the bank to comply with regulatory requirements including monitoring for and reporting of 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 activity that potentially exposes the bank to financial loss, increased expenses, or other risks.
- 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

FinCEN's final rule on CDD became effective July 11, 2016, with a compliance date of May 11, 2018. The rule codifies existing supervisory expectations and practices related to regulatory requirements and therefore, nothing in this final rule is intended to lower, reduce, or limit the due diligence expectations of the federal functional regulators or in any way limit their existing regulatory discretion.

In accordance with regulatory requirements, all banks must develop and implement appropriate risk-based procedures for conducting ongoing customer due diligence,[2] including, but not limited to:

- Obtaining and analyzing sufficient customer information to understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
- Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, including information regarding

the beneficial owner(s) of legal entity customers. Additional guidance can be found in the examination procedures "Beneficial Ownership Requirements for Legal Entity Customers."

At a minimum, the bank must establish risk-based CDD procedures that:

- Enable the bank to understand the nature and purpose of the customer relationship in order to develop a customer risk profile.
- Enable the bank to conduct ongoing monitoring
  - for the purpose of identifying and reporting suspicious transactions and,
  - on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers.

In addition, the bank's risk-based CDD policies, procedures, and processes should:

- Be commensurate with the bank's BSA/AML risk profile, with increased focus on higher risk customers.
- Contain a clear statement of management's and staff's responsibilities, including procedures, authority, and responsibility for reviewing and approving changes to a customer's risk profile, as applicable.
- Provide standards for conducting and documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.

Customer Risk Profile

The bank should have an understanding of the money laundering and terrorist financing risks of its customers, referred to in the rule as the customer risk profile.[3] This concept is also commonly referred to as the customer risk rating. Any customer account may be used for illicit purposes, including money laundering or terrorist financing. Further, a spectrum of risks may be identifiable even within the same category of customers. The bank's program for determining customer risk profiles should be sufficiently detailed to distinguish between significant variations in the money laundering and terrorist financing risks of its customers. Improper identification and assessment of a customer's risk can have a cascading effect, creating deficiencies in multiple areas of internal controls and resulting in an overall weakened BSA compliance program.

The assessment of customer risk factors is bank-specific, and a conclusion regarding the customer risk profile should be based on a consideration of all pertinent customer information, including ownership information generally. Similar to the bank's overall risk assessment, there are no required risk profile categories and the number and detail of these categorizations will vary based on the bank's size and complexity. Any one single indicator is not necessarily determinative of the existence of a lower or higher customer risk.

Examiners should primarily focus on whether the bank has effective processes to develop customer risk profiles as part of the overall CDD program. Examiners may review individual customer risk decisions as a means to test the effectiveness of the process and CDD program. In those instances where the bank has an established and effective customer risk decision-making

process, and has followed existing policies, procedures, and processes, the bank should not be criticized for individual customer risk decisions unless it impacts the effectiveness of the overall CDD program, or is accompanied by evidence of bad faith or other aggravating factors.

The bank should gather sufficient information about the customer to form an understanding of the nature and purpose of customer relationships at the time of account opening. This understanding may be based on assessments of individual customers or on categories of customers. An understanding based on "categories of customers" means that for certain lower-risk customers, the bank's understanding of the nature and purpose of a customer relationship can be developed by inherent or self-evident information such as the type of customer, the type of account opened, or the service or product offered.

The factors the bank should consider when assessing a customer risk profile are substantially similar to the risk categories considered when determining the bank's overall risk profile. The bank should identify the specific risks of the customer or category of customers, and then conduct an analysis of all pertinent information in order to develop the customer's risk profile. In determining a customer's risk profile, the bank should consider risk categories, such as the following, as they relate to the customer relationship:

- Products and Services.
- Customers and Entities.
- Geographic Locations.

As with the risk assessment, the bank may determine that some factors should be weighted more heavily than others. For example, certain products and services used by the customer, the type of customer's business, or the geographic location where the customer does business, may pose a higher risk of money laundering or terrorist financing. Also, actual or anticipated activity in a customer's account can be a key factor in determining the customer risk profile. Refer to the further description of identification and analysis of specific risk categories in the "BSA/AML Risk Assessment - Overview" section of the FFIEC BSA/AML Examination Manual.

Customer Information – Risk-Based Procedures

As described above, the bank is required to form an understanding of the nature and purpose of the customer relationship. The bank may demonstrate its understanding of the customer relationship through gathering and analyzing information that substantiates the nature and purpose of the account. Customer information collected under CDD requirements for the purpose of developing a customer risk profile and ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, includes beneficial ownership information for legal entity customers. However, the collection of customer information regarding beneficial ownership is governed by the requirements specified in the beneficial ownership rule. The beneficial ownership rule requires the bank to collect beneficial ownership information at the 25 percent ownership threshold regardless of the customer's risk profile. In addition, the beneficial ownership rule does not require the bank to collect information regarding ownership or control for certain customers that are exempted or not included in the definition of legal entity customer, such as certain trusts, or certain other legal entity customers.

Other than required beneficial ownership information, the level and type of customer information should be commensurate with the customer's risk profile, therefore the bank should obtain more customer information for those customers that have a higher customer risk profile and may find that less information for customers with a lower customer risk profile is sufficient. Additionally, the type of appropriate customer information will generally vary depending on the customer risk profile and other factors, for example, whether the customer is a legal entity or an individual. For lower risk customers, the bank may have an inherent understanding of the nature and purpose of the customer relationship (*i.e.,* the customer risk profile) based upon information collected at account opening. As a result, the bank may not need to collect any additional customer information for these customers in order to comply with this part of the CDD requirements.

Customer information collected under the CDD rule may be relevant to other regulatory requirements, including but not limited to identifying suspicious activity, identifying nominal and beneficial owners of private banking accounts, and determining OFAC sanctioned parties. The bank should define in its policies, procedures and processes how customer information will be used to meet other regulatory requirements. For example, the bank is expected to use the customer information and customer risk profile in its suspicious activity monitoring process to understand the types of transactions a particular customer would normally be expected to engage in as a baseline against which suspicious transactions are identified and to satisfy other regulatory requirements.

The bank may choose to implement CDD policies, procedures, and processes on an enterprise-wide basis. To the extent permitted by law, this implementation may include sharing or obtaining customer information across business lines, separate legal entities within an enterprise, and affiliated support units. To encourage cost effectiveness, enhance efficiency, and increase availability of potentially relevant information, the bank may find it useful to cross-check for customer information in data systems maintained within the financial institution for other purposes, such as credit underwriting, marketing, or fraud detection.

Higher Risk Profile Customers

Customers that pose higher money laundering or terrorist financing risks, (*i.e.,* higher risk profile customers), present increased risk exposure to banks. As a result, due diligence policies, procedures, and processes should define both when and what additional customer information will be collected based on the customer risk profile and the specific risks posed. Collecting additional information about customers that pose heightened risk, referred to as enhanced due diligence (EDD), for example, in the private and foreign correspondent banking context, is part of an effective due diligence program. Even within categories of customers with a higher risk profile, there can be a spectrum of risks and the extent to which additional ongoing due diligence measures are necessary may vary on a case-by-case basis. Based on the customer risk profile, the bank may consider obtaining, at account opening (and throughout the relationship), more customer information in order to understand the nature and purpose of the customer relationship, such as:

- Source of funds and wealth.
- Occupation or type of business (of customer or other individuals with ownership or control over the account).

- Financial statements for business customers.
- Location where the business customer is organized and where they maintain their principal place of business.
- Proximity of the customer's residence, place of employment, or place of business to the bank.
- Description of the business customer's primary trade area, whether transactions are expected to be domestic or international, and the expected volumes of such transactions.
- Description of the business operations, such as total sales, the volume of currency transactions, and information about major customers and suppliers.

Performing an appropriate level of ongoing due diligence that is commensurate with the customer's risk profile is especially critical in understanding the customer's transactions in order to assist the bank in determining when transactions are potentially suspicious. This determination is necessary for a suspicious activity monitoring system that helps to mitigate the bank's compliance and money laundering risks.

Consistent with the risk-based approach, the bank should do more in circumstances of heightened risk, as well as to mitigate risks generally. Information provided by higher risk profile customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the bank. The bank should establish policies and procedures for determining whether and/or when, on the basis of risk, obtaining and reviewing additional customer information, for example through negative media search programs, would be appropriate.

While not inclusive, certain customer types, such as those found in the "Persons and Entities" section of the FFIEC BSA/AML Examination Manual, may pose heightened risk. In addition, existing laws and regulations may impose, and supervisory guidance may explain expectations for, specific customer due diligence and, in some cases, enhanced due diligence requirements for certain accounts or customers, including foreign correspondent accounts, payable-through accounts, private banking accounts, politically exposed persons, and money services businesses. The bank's risk-based customer due diligence and enhanced due diligence procedures must ensure compliance with these existing requirements and should meet these supervisory expectations.

Ongoing Monitoring of the Customer Relationship

The requirement for ongoing monitoring of the customer relationship reflects existing practices established to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

Therefore, in addition to policies, procedures, and processes for monitoring to identify and report suspicious transactions, the bank's CDD program must include risk-based procedures for performing ongoing monitoring of the customer relationship, on a risk basis, to maintain and update customer information, including beneficial ownership information of legal entity customers.[11] For more information on beneficial ownership of legal entity customers, refer to the "Beneficial Ownership Requirements for Legal Entity Customers" section of the FFIEC BSA/AML Examination Manual.

The requirement to update customer information is event-driven and occurs as a result of normal monitoring. Should the bank become aware as a result of its ongoing monitoring that customer information, including beneficial ownership information, has materially changed, it should update the customer information accordingly. Additionally, if this customer information is material and relevant to assessing the risk of a customer relationship, then the bank should reassess the customer risk profile/rating and follow established bank policies, procedures, and processes for maintaining or changing the customer risk profile/rating. One common indication of a material change in the customer risk profile is transactions or other activity that are inconsistent with the bank's understanding of the nature and purpose of the customer relationship or with the customer risk profile.

The bank's procedures should establish criteria for when and by whom customer relationships will be reviewed, including updating customer information and reassessing the customer's risk profile. The procedures should indicate who in the organization is authorized to change a customer's risk profile. A number of factors may be relevant in determining when it is appropriate to review a customer relationship including, but not limited to:

- Significant and unexplained changes in account activity
- Changes in employment or business operation
- Changes in ownership of a business entity
- Red flags identified through suspicious activity monitoring
- Receipt of law enforcement inquiries and requests such as criminal subpoenas, National Security Letters (NSL), and section 314(a) requests
- Results of negative media search programs
- Length of time since customer information was gathered and the customer risk profile assessed

The ongoing monitoring element does not impose a categorical requirement that the bank must update customer information on a continuous or periodic basis.

However, the bank may establish policies, procedures, and processes for determining whether and when, on the basis of risk, periodic reviews to update customer information should be conducted to ensure that customer information is current and accurate.

Examination Procedures - Customer Due Diligence

Objective. ***Assess the bank's compliance with the regulatory requirements for customer due diligence (CDD).***

1. Determine whether the bank has developed and implemented appropriate written risk-based procedures for conducting ongoing CDD and that they:

   - Enable the bank to understand the nature and purpose of the customer relationship in order to develop a customer risk profile.
   - Enable the bank to conduct ongoing monitoring
     - for the purpose of identifying and reporting suspicious transactions and,

  - on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers.
- Enable the bank to use customer information and the customer risk profile to understand the types of transactions a particular customer would be expected to engage in and as a baseline against which suspicious transactions are identified.

2. Determine whether the bank, as part of the overall CDD program, has effective processes to develop customer risk profiles that identify the specific risks of individual customers or categories of customers.

3. Determine whether the risk-based CDD policies, procedures, and processes are commensurate with the bank's BSA/AML risk profile with increased focus on higher risk customers.

4. Determine whether policies, procedures, and processes contain a clear statement of management's and staff's responsibilities, including procedures, authority, and responsibility for reviewing and approving changes to a customer's risk profile, as applicable.

5. Determine that the bank has policies, procedures, and processes to identify customers that may pose higher risk for money laundering or terrorist financing that include whether and/or when, on the basis of risk, it is appropriate to obtain and review additional customer information.

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

7. Determine whether the bank has defined in its policies, procedures, and processes how customer information, including beneficial ownership information for legal entity customers, is used to meet other relevant regulatory requirements, including but not limited to, identifying suspicious activity, identifying nominal and beneficial owners of private banking accounts, and determining OFAC sanctioned parties.

Transaction Testing

8. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of customer information. Determine whether the bank collects appropriate information sufficient to understand the nature and purpose of the customer relationship and effectively incorporates customer information, including beneficial ownership information for legal entity customers, into the customer risk profile. 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.

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

Section 8: Beneficial Ownership - (revised 2018)

Beneficial Ownership Requirements for Legal Entity Customers - Overview

Objective. ***Assess the bank's written procedures and overall compliance with regulatory requirements for identifying and verifying beneficial owner(s) of legal entity customers.***

Under the Beneficial Ownership Rule, a bank must establish and maintain written procedures that are reasonably designed to identify and verify beneficial owner(s) of legal entity customers and to include such procedures in its anti-money laundering compliance program.

Legal entities, whether domestic or foreign, can be used to facilitate money laundering and other crimes because their true ownership can be concealed. The collection of beneficial ownership information by banks about legal entity customers can provide law enforcement with key details about suspected criminals who use legal entity structures to conceal their illicit activity and assets. Requiring legal entity customers seeking access to banks to disclose identifying information, such as the name, date of birth, and Social Security number of natural persons who own or control them will make such entities more transparent, and thus less attractive to criminals and those who assist them.

Similar to other customer information that a bank may gather, beneficial ownership information collected under the rule may be relevant to other regulatory requirements. These other regulatory requirements include, but are not limited to, identifying suspicious activity, and determining Office of Foreign Assets Control (OFAC) sanctioned parties. Banks should define in their policies, procedures, and processes how beneficial ownership information will be used to meet other regulatory requirements.

Legal Entity Customers

For the purposes of the Beneficial Ownership Rule, a legal entity customer is defined as a corporation, limited liability company, or other entity that is created by the filing of a public document with a Secretary of State or other similar office, a general partnership, and any similar entity formed under the laws of a foreign jurisdiction that opens an account. A number of types of business entities are excluded from the definition of legal entity customer under the Beneficial Ownership rule. In addition, and subject to certain limitations, banks are not required to identify and verify the identity of the beneficial owner(s) of a legal entity customer when the customer opens certain types of accounts. For further information on exclusions and exemptions to the Beneficial Ownership Rule, see Appendix 1. These exclusions and exemptions do not alter or supersede other existing requirements related to BSA/AML and OFAC sanctions.

Beneficial Owner(s)

Beneficial ownership is determined under both a control prong and an ownership prong. Under the control prong, the beneficial owner is a single individual with significant responsibility to control, manage or direct a legal entity customer. This includes, an executive officer or senior manager (Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, President), or any other individual who regularly performs similar functions. One beneficial owner must be identified under the control prong for each legal entity customer.

Under the ownership prong, a beneficial owner is each individual, *if any*, who, directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, owns 25 percent or more of the equity interests of a legal entity customer. If a trust owns directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, 25 percent or more of the equity interests of a legal entity customer, the beneficial owner is the trustee. Identification of a beneficial owner under the ownership prong is *not required* if no individual owns 25 percent or more of a legal entity customer. Therefore, all legal entity customers will have a total of between one and five beneficial owner(s) – one individual under the control prong and zero to four individuals under the ownership prong.

Banks may rely on the information supplied by the legal entity customer regarding the identity of its beneficial owner or owners, provided that it has no knowledge of facts that would reasonably call into question the reliability of such information. However, bank staff who know, suspect, or have reason to suspect that equity holders are attempting to avoid the reporting threshold may, depending on the circumstances, be required to file a SAR. More information on filing of SARs may be found in the "Suspicious Activity Reporting Overview" section in the FFIEC BSA/AML Examination Manual.

Identification of Beneficial Ownership Information

A bank must establish and maintain written procedures detailing the identifying information that must be obtained for each beneficial owner of a legal entity customer opening a new account after May 11, 2018. At a minimum, the bank must obtain the following identifying information for each beneficial owner of a legal entity customer:

- Name.
- Date of birth.
- Address.
- Identification number.

A bank may obtain identifying information for beneficial owner(s) of legal entity customers through a completed certification form from the individual opening the account on behalf of the legal entity customer, or by obtaining from the individual the information required by the form by another means, provided the individual certifies, to the best of the individual's knowledge, the accuracy of the information. A bank may rely on the information supplied by the individual opening the account on behalf of the legal entity customer regarding the identity of its beneficial owner(s), provided that it has no knowledge of facts that would reasonably call into question the reliability of such information. If a legal entity customer opens multiple accounts a bank may rely

on the pre-existing beneficial ownership records it maintains, provided that the bank confirms (verbally or in writing) that such information is up-to-date and accurate at the time each account is opened.

Banks must have procedures to maintain and update customer information, including beneficial ownership information for legal entity customers, on the basis of risk. Additionally, banks are not required to conduct retroactive reviews to obtain beneficial ownership information on legal entity customers that were existing customers as of May 11, 2018. However, the bank may need to obtain (and thereafter update) beneficial ownership information for existing legal entity customers based on its ongoing monitoring. For further guidance on maintaining and updating of customer information including beneficial ownership information, please see the "Ongoing Monitoring of Customer Relationship" section of the "Customer Due Diligence Overview" section of the FFIEC BSA/AML Examination Manual.

Verification of Beneficial Owner Information

A bank must establish and maintain written risk-based procedures for verifying the identity of each beneficial owner of a legal entity customer within a reasonable period of time after the account is opened. These procedures must contain the elements required for verifying the identity of customers that are individuals under 31 CFR 1020.220(a)(2), provided, that in the case of documentary verification, the bank may use photocopies or other reproductions of the documents listed in paragraph (a)(2)(ii)(A)(*1*) of 31 CFR 1020.220. Guidance on documentary and non-documentary verification methods may be found in the core overview section "Customer Identification Program," of the FFIEC BSA/AML Examination Manual.

A bank need not establish the accuracy of every element of identifying information obtained, but must verify enough information to form a reasonable belief that it knows the true identity of the beneficial owner(s) of the legal entity customer. The bank's procedures for verifying the identity of the beneficial owners must describe when it uses documents, non-documentary methods, or a combination of methods.

Lack of Identification and Verification of Beneficial Ownership Information

Also consistent with 31 CFR 1020.220, the bank should establish policies, procedures, and processes for circumstances in which the bank cannot form a reasonable belief that it knows the true identity of the beneficial owner(s) of a legal entity customer. These policies, procedures, and processes 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 identity of the beneficial owner(s) of a legal entity customer.
- When the bank should close an account, after attempts to verify the identity of the beneficial owner(s) of a legal entity customer have failed.
- When the bank should file a SAR in accordance with applicable law and regulation.

Recordkeeping and Retention Requirements

A bank must establish recordkeeping procedures for beneficial ownership identification and verification information. At a minimum, the bank must maintain any identifying information obtained, including without limitation the certification (if obtained), for a period of five years after the date the account is closed.

The bank must also keep a description of any document relied on (noting the type, any identification number, place of issuance and, if any, date of issuance and expiration), of any non-documentary methods and the results of any measures undertaken, and of the resolution of each substantive discrepancy for five years after the record is made.

Reliance on Another Financial Institution

A bank is permitted to rely on the performance by another financial institution (including an affiliate) of the requirements of the Beneficial Ownership Rule with respect to any legal entity customer of the covered financial institution that is opening, or has opened, an account or has established a similar business relationship with the other financial institution to engage in services, dealings, or other financial transactions, provided that:

- Reliance is reasonable, under the circumstances.
- The relied-upon financial institution is subject to a rule implementing 31 USC 5318(h) and is regulated by a federal functional regulator.[13]
- 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 procedures to comply with the requirements of the Beneficial Ownership Rule.

Examination Procedures - Beneficial Ownership

Objective: ***Assess the bank's written procedures and overall compliance with regulatory requirements for identifying and verifying beneficial owner(s) of legal entity customers.***

1. Determine whether the bank has adequate written procedures for gathering and verifying information required to be obtained, and retained (including name, address, taxpayer identification number (TIN), and date of birth) for beneficial owner(s) of legal entity customers who open an account after May 11, 2018.
2. Determine whether the bank has adequate risk-based procedures for updating customer information, including beneficial owner information, and maintaining current customer information.

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 new accounts opened for legal entity customers since May

11, 2018 to review for compliance with the Beneficial Ownership Rule. The sample should include a cross-section of account types. From this sample, determine whether the bank has performed the following procedures:

- Opened the account in accordance with the requirements of the Beneficial Ownership Rule (31 CFR 1010.230).
- Obtained the identifying information for each beneficial owner of a legal entity customer as required (e.g. name, date of birth, address, and identification number).
- Within a reasonable time after account opening, verified enough of the beneficial owner's identity information to form a reasonable belief as to the beneficial owner's true identity.
- Appropriately resolved situations in which beneficial owner's identity could not be reasonably established.
- Maintained a record of the identity information required by the Beneficial Ownership Rule, the method used to verify identity, and verification results (31 CFR 1010.230(i)).
- Filed SARs as appropriate.

4. On the basis of the examination procedures completed, including transaction testing, form a conclusion about the adequacy of procedures for complying with the Beneficial Ownership Rule.

Section 9: Suspicious Activity Reports (revised 2014)

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

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

Safe Harbor for Banks From Civil Liability for Suspicious Activity

Reporting

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

Systems to Identify, Research, and Report Suspicious Activity

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 five 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 five 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.
- Monitoring and SAR filing on continuing activity.

These 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, SAR completion and filing, and monitoring and SAR filing on continuing activity.

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 section 314(a) and section 314(b) requests, advisories issued by regulatory or law enforcement agencies, 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.

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. 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.
- Information from credit bureaus.
- Financial records from financial institutions.

NSLs are highly confidential documents; for that reason, examiners will not review or sample specific NSLs. Pursuant to 12 USC 3414(a)(3) and (5)(D), no bank, or officer, employee or agent of the institution, can disclose to any person that a government authority or the FBI has sought or obtained access to records through a Right to Financial Privacy Act NSL. Banks that receive NSLs must take appropriate measures to ensure the confidentiality of the letters and should have procedures in place for processing and maintaining the confidentiality of NSLs.

If a bank files a SAR after receiving a NSL, the SAR should not contain any reference to the receipt or existence of the NSL. The SAR should reference only those facts and activities that support a finding of unusual or suspicious transactions identified by the bank.

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, ATM transaction 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, 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 through policies and procedures. Controls should ensure limited access to the monitoring systems,

and changes should generally require the approval of the BSA compliance officer or senior management. Management should document and be able to explain filtering criteria, thresholds used, and how both are appropriate for the bank's risks. Management should also periodically review and test 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. The independent validation should also verify the policies in place and that management is complying with those policies.

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." 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," for further guidance.

Identifying Underlying Crime

Banks are required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing, [63] 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. Suspicious Activity Information, Part II of the SAR provides a number of categories with different types of suspicious activity. Within each category, there is the option of selecting "Other" if none of the suspicious activities apply. However, the use of "Other" should be limited to situations that cannot be broadly identified within the categories 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.

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

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 have suggested that banks should report continuing suspicious activity by filing a report at least every 90 calendar days. Subsequent guidance permits banks with SAR requirements to file SARs for continuing activity after a 90 day review with the filing deadline being 120 calendar days after the date of the previously related SAR filing. Banks may also file SARs on continuing activity earlier than the 120 day deadline if the bank believes the activity warrants earlier review by law enforcement. This practice will notify law enforcement of the continuing nature of the activity in aggregate. In addition, this practice reminds 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.

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.
- 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 SARs 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. FinCEN developed a new electronic BSA Suspicious Activity Report (BSAR) that replaced FinCEN SAR-DI form TD F 90-22.47. The BSAR provides a uniform data collection format that can be used across multiple industries. As of April 1, 2013, the BSAR is mandatory and must be filed through FinCEN's BSA E-Filing System. The BSAR does not create or otherwise change existing statutory and regulatory expectations for banks.

The BSAR includes a number of additional data elements pertaining to the type of suspicious activity and the financial services involved. Certain fields in the BSAR are marked as "critical" for technical filing purposes. This means the BSA E-Filing System will not accept filings in which these fields are left blank. For these items, the bank must either provide the requested information or check the "unknown" box that is provided with each critical field. Banks should provide the most complete filing information available consistent with existing regulatory

expectations, regardless of whether or not the individual fields are deemed critical for technical filing purposes.

Banks should report the information that they know, or that otherwise arises, as part of their case reviews. Other than the critical fields, the addition of the new and expanded data elements does not create an expectation that banks will revise internal programs, or develop new programs, to capture information that reflects the expanded lists. Refer to Appendix T for additional information on filing through the BSA E-Filing System.

Timing of a SAR Filing

The SAR rules require that a SAR be electronically filed through the BSA E-Filing System 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.

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.

Whenever possible, an expeditious review of the transaction or the account is recommended and can be of significant assistance to law enforcement. In any event, the review should be completed in a reasonable period of time. 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.

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.

SAR Quality

Banks are required to file SARs that are complete, thorough, and timely. Banks should include all known subject information on the SAR. The importance of the accuracy of this information cannot be overstated. Inaccurate information on the SAR, 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, is "critical." Thus, a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.

To inform and assist banks in reporting instances of suspected money laundering, terrorist financing, and fraud, FinCEN issues advisories and guidance containing examples of "red flags." In order to assist law enforcement in its efforts to target these activities, FinCEN requests that banks check the appropriate box(es) in the Suspicious Activity Information section and include certain key terms in the narrative section of the SAR. The advisories and guidance can be found on FinCEN's website.

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. The BSAR will accept a single, Microsoft Excel compatible comma separated value (csv) file no larger than one (1) megabyte as an attachment as part of the report. This capability allows a bank to include transactional data such as specific financial transactions and funds transfers or other analytics which is more readable or usable in this format than it would be if otherwise included in the narrative. Such an attachment will be considered a part of the narrative and is not considered to be a substitute for the narrative. For example, narratives should not simply state "see attachment" if the bank included a csv attachment. As with other information that may be prepared in connection with the filing of a SAR, an attachment is considered supporting documentation and should be treated as confidential to the extent that it indicates the existence of a SAR.

More specific guidance is available in Appendix L ("SAR Quality Guidance") to assist banks in writing, and assist examiners in evaluating, SAR narratives.

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, while being mindful of the confidential nature of the 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. The bank can retain copies in paper or electronic format. 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.

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. A SAR and any information that would reveal the existence of a SAR, are confidential, except as is necessary to fulfill BSA obligations and responsibilities. For example, the existence or even the non-existence of a SAR must be kept confidential, as well as the information contained in the SAR to the extent that the information would reveal the existence of a SAR. [78] Furthermore, FinCEN and the federal banking agencies take the position that a bank's internal controls for the filing of SARs should minimize the risks of disclosure.

A bank or its agent may reveal the existence of a SAR to fulfill responsibilities consistent with the BSA, provided no person involved in a suspicious transaction is notified that the transaction has been reported. The underlying facts, transactions, and supporting documents of a SAR may be disclosed to another financial institution for the preparation of a joint SAR, or in connection with certain employment references or termination notices to the full extent authorized in 31 USC 5318(g)(2)(B). The sharing of a SAR by a bank or its agent with certain permissible entities within the bank's corporate organizational structure for purposes consistent with Title II of the Bank Secrecy Act is also allowed.

Any person subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR, except when such disclosure is requested by FinCEN or an appropriate law enforcement or federal banking agency, shall decline to produce the SAR or to provide any information that would disclose that a SAR has been prepared or filed, citing 31 CFR 1020.320(e) and 31 USC 5318(g)(2)(A)(i). FinCEN and the bank's federal banking agency should be notified of any such request and of the bank's response.

Examiners should follow their respective agency's protocol on discovery of the improper disclosure of a SAR. Examiners also should ensure the bank has notified the appropriate federal banking agency and FinCEN of the improper disclosure.

Sharing SARs with Head Offices, Controlling Companies, and Certain U.S. Affiliates

Previously issued guidance clarified that sharing of a SAR or, more broadly, any information that would reveal the existence of a SAR, with a head office or controlling company (including overseas) promotes compliance with the applicable requirements of the BSA by enabling the head office or controlling company to discharge its oversight responsibilities with respect to enterprise-wide risk management, including oversight of a bank's compliance with applicable laws and regulations.

- 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.

In addition, a bank that has filed a SAR may share the SAR, or any information that would reveal the existence of the SAR, with an affiliate provided the affiliate is subject to a SAR regulation. An affiliate is defined as any company under common control with, or controlled by, that depository institution. Under "common control" means that another company:

- Directly or indirectly or acting through one or more other persons owns, controls, or has the power to vote 25 percent or more of any class of the voting securities of the company and the depository institution; or
- Controls in any manner the election of a majority of the directors or trustees of the company and the depository institution.

Controlled by means that the depository institution:

- Directly or indirectly has the power to vote 25 percent or more of any class of the voting securities of the company; or
- Controls in any manner the election of a majority of the directors or trustees of the company. See 12 U.S.C. 1841(a)(2).

Because foreign branches of U.S. banks are regarded as foreign banks for the purposes of the BSA, they are affiliates that are not subject to a SAR regulation. Accordingly, a U.S. bank that has filed a SAR may not share the SAR, or any information that would reveal the existence of the SAR, with its foreign branches.

Banks should maintain appropriate arrangements with head offices, controlling companies, and affiliates to protect the confidentiality of SARs. The bank should have policies and procedures

in place to protect the confidentiality of the SAR as part of their internal controls.

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 (NSLs)) 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, ATM transaction 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 (i.e., the SAR narrative should not simply state "see attachment" if the bank included a csv file).

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.

Section 10: Currency Transaction Reporting (revised 2014)

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 electronically file a Currency Transaction Report (CTR) for each transaction in currency (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," 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.

In cases where multiple businesses share a common owner, the presumption is that separately incorporated entities are independent persons. The currency transactions of separately incorporated businesses should not automatically be aggregated as being on behalf of any one person simply because those businesses are owned by the same person. Financial institutions should determine, based on information obtained in the ordinary course of business, whether multiple businesses that share a common owner are being operated independently depending on all the facts and circumstances.

However, if a financial institution determines that these businesses (or one or more of the businesses and the private accounts of the owner) are not operating separately or independently of one another or their common owner (e.g., the businesses are staffed by the same employees and are located at the same address, the bank accounts of one business are repeatedly used to pay the expenses of another business, or the business bank accounts are repeatedly used to pay the personal expenses of the owner) the financial institution may determine that aggregating the businesses' transactions is appropriate because the transactions were made on behalf of a single person.

If a financial institution determines that the businesses are independent, then it should not aggregate the separate transactions of these businesses. Alternatively, once a financial institution determines that the businesses are not independent of each other or their common owner, then the transactions of these businesses should be aggregated going forward.

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, monetary instrument purchases, and certain transactions involving armored car services.

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 and Record Retention

FinCEN developed a new electronic Bank Secrecy Act Currency Transaction Report (BCTR) that replaced FinCEN CTR Form 104. The BCTR provides a uniform data collection format that can be used across multiple industries. As of April 1, 2013, the BCTR is mandatory and must be filed through FinCEN's BSA E-Filing System. The BCTR does not create or otherwise change existing statutory and regulatory expectations for banks.

The BCTR includes a number of additional data elements pertaining to the financial services involved. Certain fields in the BCTR are marked as "critical" for technical filing purposes; this means the BSA E-Filing System will not accept filings in which these fields are left blank. For these items, the bank must either provide the requested information or check the "unknown" box that is provided with each critical field. Banks should provide the most complete filing information available consistent with existing regulatory expectations, regardless of whether or not the individual fields are deemed critical for technical filing purposes.

Other than the critical fields, the addition of the new and expanded data elements does not create an expectation that banks will revise internal programs, or develop new programs, to capture information that reflects the expanded lists.

A completed BCTR must be electronically filed with FinCEN within 15 calendar days after the date of the transaction. The bank must retain copies of CTRs for five years from the date of the report (31 CFR 1010.306(a)(2)). The bank can retain hard copies or copies in electronic format.

Refer to Appendix T for additional information on filing through the BSA E-Filing System.

CTR Backfiling

If a bank has failed to file CTRs on reportable transactions, the bank should begin filing CTRs from that point forward and should contact the FinCEN's Regulatory Helpline[87] to request a determination on whether the backfiling of unreported transactions is necessary.

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.

2. Review correspondence that the bank has electronically received from FinCEN's BSA E-Filing System (refer to Appendix T for additional information on filing through the BSA E-Filing System). 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 electronic format) 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.
   - 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 assess whether tellers have the capability to override currency aggregation systems. If so, the examiner should review controls in place to ensure the override capability is used appropriately. Controls may include supervisory approval, generation of exception reports, and BSA officer and internal audit review of exception reports.
   - Discrepancies exist between the bank's records of CTRs and the CTRs reflected in the BSA-reporting database.
   - The bank retains copies (hard copy or electronic format) of CTRs for five years from the date of the report (31 CFR 1010.306(a)(2)).

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.

Section 11: CTR Exemptions (revised 2014)

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.

Phase I CTR Exemptions (31 CFR 1020.315(b)(1)-(5))

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.

Filing Time Frames

Banks must file a one-time Designation of Exempt Person report (DOEP) to exempt each eligible listed public company or eligible subsidiary from currency transaction reporting. The report must be filed electronically through the BSA E-Filing System within 30 days after the first transaction in currency that the bank wishes to exempt.

Banks do not need to file a DOEP 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 1020.315(b)(6)-(7))

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[88] engages in transactions in currency with the bank in excess of $10,000; and (iii) is incorporated or organized under the laws of the United States or a state, or is registered as and 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 1020.315(e)(8)). 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, such as marijuana-related businesses.

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[91] 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 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.

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 frequently[93] 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 report through the BSA E-Filing System 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 1020.315(e)(10)(g)) provide a safe harbor that a bank is not liable for the failure to file a CTR for a transaction in currency by an exempt person, unless the bank knowingly provides false or incomplete information or has reason to believe that the customer does not qualify as an exempt customer. In the absence of any specific knowledge or information indicating that a customer no longer meets the requirements of an exempt person, the bank is entitled to a safe harbor from civil penalties to the extent it continues to treat that customer as an exempt customer until the date of the customer's annual review.

Effect on Other Regulatory Requirements

The exemption procedures do not 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 or ceases to treat a customer as exempt, it may revoke the exemption by filing a Designation of Exempt Persons (DOEP) report and checking the "Exemption Revoked" box or revoke the exemption by filing CTRs on the customer. In the case of improperly exempted accounts, the bank should begin filing CTRs and should contact FinCEN's Regulatory Helpline to request a determination on whether the backfiling of unreported currency transactions is necessary.

Additional information can be found on the FinCEN Web site.

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 1020.315(b)(1)-(5))

2. Determine whether the bank files the Designation of Exempt Person report electronically through FinCEN's E-Filing System to exempt eligible listed public companies and their subsidiaries from CTR reporting as defined in 31 CFR 1020.311. The report 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 1020.315(b)(6)-(7))

Under the regulation, the definition of exempt persons includes "non-listed businesses" and "payroll customers" as defined in 31 CFR 1020.315(b)(6)-(7). Nevertheless, several businesses remain ineligible for exemption purposes; refer to 31 CFR 1020.315(e)(8) and the "Currency Transaction Reporting Exemptions Overview" section of this manual.

4. Determine whether the bank files a Designation of Exempt Person report electronically through the FinCEN E-Filing System 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[95] currency transactions in excess of $10,000 (including 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 (DOEP) reports 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.

Section 12: Information Sharing (revised 2014)

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.

Information Sharing Between Law Enforcement and Financial Institutions - Section 314(a) of the USA PATRIOT Act (31 CFR 1010.520)

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

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).

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. The General Instructions or FAQs are made available to the financial institutions on the SISS.

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.[101] 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 1010.520(b)(3)(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," 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 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. Banks may print or store a search self-verification document from the Web-based 314(a) SISS 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. 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.

Voluntary Information Sharing — Section 314(b) of the USA

PATRIOT Act (31 CFR 1010.540)

Section 314(b) encourages financial institutions and associations of financial institutions located in the United States to share information in order to identify and report activities that may involve terrorist activity or money laundering. Section 314(b) also provides specific protection from civil liability. To avail itself of this statutory safe harbor from liability, a financial institution or an association must notify FinCEN of its intent to engage in information sharing and that it has established and will maintain adequate procedures to protect the security and confidentiality of the information. Failure to comply with the requirements of 31 CFR 1010.540 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. 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 1010.540(b)(4)). Such information may be used only to identify and, where appropriate, report on money laundering and terrorist activities; to determine whether to establish or maintain an account; to engage in a transaction; or to assist in BSA compliance. The procedures to ensure confidentiality will be considered adequate if the financial institution applies procedures similar to the ones it has established to comply with section 501 of the Gramm–Leach–Bliley Act (15 USC 6801) for the protection of its customers' nonpublic personal information. The safe harbor does not extend to sharing of information across international borders. In addition, section 314(b) does not authorize a financial institution to share a SAR, nor does it permit the financial institution to disclose the existence or nonexistence of a SAR. If a financial institution shares information under section 314(b) about the subject of a prepared or filed SAR, the information shared should be limited to underlying 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 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 1010.520, 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.

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.
   - Copies of SISS-generated search self-verification documents.
   - If appropriate, request documentation from FinCEN regarding the bank's history of accessing the SISS.
   - 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 1010.540, (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 1010.540. 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 1010.540(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 section 314(b) voluntary information sharing process. In fact, the information obtained through the section 314(b) 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 1010.520(b)(3)(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 1010.520(b)(3)(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.

Section 13: Purchase and Sale of Monetary Instruments Recordkeeping (revised 2014)

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 1010.415 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[108] 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 1010.415. 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 1010.415 in the normal course of its business.

Recordkeeping and Retention Requirements

Under 31 CFR 1010.415, 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.
- 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.

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.

Section 14: Funds Transfer Recordkeeping (revised 2014)

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 1010.410). [110] The rule requires each bank involved in funds transfers to collect and retain certain information in connection with funds transfers of $3,000 or more. 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). 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 1010.410). This requirement is commonly referred to as the "Travel Rule."

Responsibilities of Originator's Banks

Recordkeeping Requirements

For each payment order in the amount of $3,000 or more that a bank accepts as an originator's bank, the bank must obtain and retain the following records (31 CFR 1020.410(a)(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).
- 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 1010.410(a)(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 1010.410(f)(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 1010.410(f)(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 1020.410(a)(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 1010.410(f), 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, [115] 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 1010.410(f), 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 [116] on file and the address information is retrievable upon request by law enforcement.

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 1020.410(a).

2. Verify that the bank transmits payment information as required by 31 CFR 1010.410(f) (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 1010.311).

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.

Section 15: Foreign Correspondent Account Recordkeeping, Reporting, and Due Diligence (revised 2014)

Foreign Correspondent Account Recordkeeping, Reporting, 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. Assess the bank's compliance with the Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA), if applicable. 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, reports, 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, [117] 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 1010.100, 1010.610, 1010.630, and 1010.670. 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 1010.630 and 1010.670, 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 1010.605(c)). Accounts maintained by foreign banks for financial institutions covered by the rule are not "correspondent accounts" subject to this regulation.

Under 31 CFR 1010.630 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. An exception, however, permits a bank to maintain a correspondent account for a foreign shell bank

that is a regulated affiliate. 31 CFR 1010.6 30 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. 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. Under 31 CFR 1010.670, a bank must produce these records within seven days upon receipt of a written request from a federal law enforcement officer.

The U.S. Treasury, working with the industry and federal banking and law enforcement agencies, developed a "certification process" to assist banks in complying with the recordkeeping provisions. This process includes certification and recertification forms. While banks are not required to use these forms, a bank will be "deemed to be in compliance" with the regulation if it obtains a completed certification form from the foreign bank and receives a recertification on or before the three-year anniversary of the execution of the initial or previous certification.

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 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.

General Due Diligence

31 CFR 1010.610(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 ("foreign correspondent account").

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 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 1010.610(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 1010.610(c) operating under any one or more of the following:

- 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 money laundering concerns.

If such an account is established or maintained, 31 CFR 1010.610(b) requires the bank to establish EDD policies, procedures, and controls to ensure that the bank, at a minimum, takes reasonable steps to:

- 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.
- 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 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 1010.610 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.

Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 Reporting Requirements

The Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA) was signed into law on July 1, 2010. CISADA authorizes the Secretary of the Treasury to prohibit or impose strict conditions on the opening or maintaining in the United States of correspondent accounts and payable through accounts for foreign financial institutions that the Secretary determines have knowingly engaged in sanctionable activities.

On October 11, 2011, FinCEN issued a final rule implementing reporting requirements under section 104(e)(1)(B) of CISADA (31 CFR 1060.300). It is important to note that FinCEN will invoke CISADA reporting requirements in very limited instances, as necessary, to elicit valuable information. The final rule requires U.S. banks to report the following information upon receiving a written request from FinCEN:

- Whether the foreign bank maintains a correspondent account for an Iranian-linked financial institution designated under the International Emergency Economic Powers Act ("IEEPA");
- Whether the foreign bank has processed one or more transfers of funds within the preceding 90 calendar days for or on behalf of, directly or indirectly, an Iranian-linked financial institution designated under IEEPA, other than through a correspondent account; and

- Whether the foreign bank has processed one or more transfers of funds within the preceding 90 calendar days for or on behalf of, directly or indirectly, Iran's Islamic Revolutionary Guard Corps ("IRGC") or any of its agents or affiliates designated under IEEPA.

The U.S. bank must report to FinCEN within 45 calendar days regardless of the foreign bank's response (e.g. positive response, negative response, incomplete response, or no response). If information is received from a foreign bank after the 45 calendar day deadline, the U.S. bank must report to FinCEN within 10 calendar days after receipt. The rule also requires the U.S. bank to report to FinCEN instances in which it does not maintain a correspondent account for the specified foreign bank.

In addition, the rule requires the U.S. bank to request the foreign bank to agree to notify them if the foreign bank subsequently establishes a new correspondent account for an Iranian-linked financial institution designated under IEEPA at any time within 365 calendar days from the date of the foreign bank's initial response. Reports regarding new correspondent accounts for an Iranian-linked financial institution designated under IEEPA are due within 10 calendar days after receipt.

FinCEN has developed a model certification form for a U.S. bank to provide to the foreign bank when making its inquiry required by the rule. The use of the model certification form is optional. However, any alternative form used by a U.S. bank should request the same information as the model certification form.

The rule does not require a bank to take any actions other than those relating to the collection of information regardless of the response received from the foreign bank and the request for information from FinCEN does not relieve the bank of any other regulatory requirement. A bank should assess all of the information it knows about its customer in accordance with its risk-based BSA/AML compliance program to determine whether additional actions should be taken or filing a SAR is warranted.

The bank shall maintain a copy of any report filed with FinCEN and any supporting documentation, including the foreign bank certification, or other responses to an inquiry for a period of five years.

Examination Procedures - Foreign Correspondent Account Recordkeeping, Reporting, 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. Assess the bank's compliance with the Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA), if applicable. 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 1010.630.

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 1010.610(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 1010.610(a)(1)).
   - Assessing the money laundering risks presented by the foreign correspondent account (31 CFR 1010.610(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 1010.610(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 1010.610(a)). 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 1010.610(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 1010.610(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 1010.610(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 1010.610(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 1010.610(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 non-publicly 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 1010.610(b)(3)).

Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 Reporting Requirements

12. If the bank has received a written request from FinCEN on a specified foreign bank, review the bank's policies, procedures, and processes for responding to FinCEN's written request. It is important to note that FinCEN will invoke CISADA reporting requirements in very limited instances, as necessary, to elicit valuable information. At a minimum, policies, procedures, and processes should accomplish the following:

    - Responding to FinCEN's requests within the designated timeframes.
    - Requesting the required information from foreign banks.
    - Complying with recordkeeping requirements.
    - Allowing for changes to a customer's risk rating or profile.

Transaction Testing

Foreign Shell Bank Prohibition and Foreign Correspondent Account Recordkeeping

13. 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. [131] 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 1010.670.

Special Due Diligence Program for Foreign Correspondent Accounts

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

15. 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.

16. 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.

17. 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.

18. 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.

Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 Reporting

Requirements

If the bank has received a written request from FinCEN on a specified foreign bank, the following transaction testing procedures should be performed:

19. If the bank does not use the CISADA certification form, determine whether the bank's reporting format captures the required information (31 CFR 1060.300(c)(1)).

20. Verify the response was provided to FinCEN within the designated timeframe (31 CFR 1060.300(c)(2)).

21. Determine whether the bank maintains a copy of the report filed, any supporting documentation, CISADA certification form or responses by the foreign bank to the inquiry for a period of 5 years.

Section 16: Private Banking Due Diligence Program (Non-U.S. Persons) (revised 2014)

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 1010.620) 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."

Private Banking Accounts

For purposes of 31 CFR 1010.620, 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 of the account.

- 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 1010.620. Refer to the expanded overview section, "Private Banking," 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.

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 1010.605(p), 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.
- 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," 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 1010.605(m).

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. [134] 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. [135]

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.

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 1010.620 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 1010.620(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 1010.605(m)(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 1010.605(m)(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 1010.605(m)(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.

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:

   - Ascertain the identity of the nominal and beneficial owners of a private banking account (31 CFR 1010.620(b)(1)).
   - Ascertain whether any nominal or beneficial owner of a private banking account is a senior foreign political figure (31 CFR 1010.620(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 1010.620(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 1010.620(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[137] for which a senior foreign political figure[138] is a nominal or beneficial owner (31 CFR 1010.620(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.
   - 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.

Section 17: Special Measures (revised 2014)

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 Chapter X.[139] 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 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.

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.

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 the FinCEN Web site 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 FinCEN Web site).

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.

Section 18: Foreign Bank and Financial Accounts Reporting (revised 2014)

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 (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 electronically file a Report of Foreign Bank and Financial Accounts (FBAR) through the BSA E-Filing System if the aggregate value of these financial accounts exceeds $10,000 at any time during the calendar year.[3] 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. A bank must file an FBAR 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 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.

FinCEN issued a final rule that became effective March 28, 2011 regarding reports of foreign financial accounts. Subsequently, FinCEN announced further extensions of time for certain FBAR filings in light of ongoing questions regarding the filing requirement and its application to individuals with signature authority over but no financial interest in certain types of accounts. On February 14, 2012, FinCEN issued Notice 2012-1 to extend the filing date for certain individuals with signature authority over but no financial interest in one or more foreign financial accounts. The FBAR filing deadline for U.S. persons with only signature authority over (but not financial interest in) a foreign financial account was extended to June 30, 2015.

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) 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.

Section 19: International Transportation of Currency or Monetary Instruments Reporting (revised 2014)

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 (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). 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 on a CMIR if they are mailed or shipped through the postal service or by common carrier.[147] 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.

Regardless of whether an exemption from filing a CMIR applies, banks are not relieved of other monitoring and reporting obligations under the BSA. Banks must report the receipt or disbursement of currency in excess of $10,000 on a Currency Transaction Report (CTR) subject to the exemptions at 31 CFR 1020.315. Banks must also monitor for and report suspicious activity.

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

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.

Section 20: Office of Foreign Asset Control (revised 2014)

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 targeted individuals and entities such as foreign countries, regimes, terrorists, international narcotics traffickers, and those engaged in certain activities such as the proliferation of weapons of mass destruction or transnational organized crime.

OFAC acts under Presidential wartime and national emergency powers, as well as various authorities granted by specific legislation, to impose controls on transactions and to freeze assets under U.S. jurisdiction. OFAC has been delegated responsibility by the Secretary of the Treasury for developing, promulgating, and administering U.S. sanctions programs. Many of these 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 national security interests of the United States.

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, including the adequacy of a compliance program in place within an institution to ensure compliance with OFAC regulations.

All U.S. persons, including U.S. banks, bank holding companies, and nonbank subsidiaries, must comply with OFAC's regulations. The federal banking agencies evaluate OFAC compliance programs to ensure that all banks subject to their supervision comply with the sanctions. [152] 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. OFAC encourages banks to take a risk-based approach to designing and implementing an OFAC compliance program. In general, the regulations that OFAC administers require banks to do 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 to 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 into a blocked account. 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 the Sudanese Sanctions Regulations 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 the exportation of services to Sudan, 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 1020.220(a)(4)) 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," for further guidance. However, OFAC's requirements stem from other statutes not limited to terrorism, and OFAC sanctions apply to transactions, in addition to account relationships.

OFAC Licenses

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

Specific licenses are issued on a case-by-case basis. A specific license is a written document issued by OFAC authorizing a particular transaction or set of transactions generally limited to a specified time period. 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 OFAC's internal licensing policies and U.S. foreign policy objectives, the license generally is issued. If a bank's customer claims to have a specific license, the bank should verify that the transaction conforms to the terms and conditions of the license (including the effective dates of the license), and may wish to obtain and retain a copy of the authorizing license for recordkeeping purposes.

OFAC Reporting

Banks must report all blockings to OFAC within 10 business days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30). Once assets or funds are blocked, they should be placed in a separate blocked account. Prohibited transactions that are rejected must also be reported to OFAC within 10 business 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 and other lists, including both entities and individuals; recent OFAC actions; and " Frequently Asked Questions," can be found on OFAC's Web site.

OFAC Compliance Program

While not required by specific regulation, but as a matter of sound banking practice and in order to mitigate the risk of noncompliance with OFAC requirements, banks should establish and maintain an effective, written OFAC compliance program that is 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 personnel in all relevant areas of the bank.

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 the higher-risk areas for potential OFAC sanctions risk. 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.
- Concentration 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".

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, as well as reporting blocked and rejected transactions 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. [160] 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. Banks with lower OFAC risk and those with low volumes of transactions may decide to manually filter for OFAC compliance. Decisions to use interdiction software and the degree of sensitivity of that software should be based on a bank's assessment of its risk and the volume of its transactions. In determining the frequency of OFAC checks and the filtering criteria used (e.g., name derivations), banks should consider the likelihood of incurring a violation and available technology. In addition, banks should periodically reassess their OFAC filtering system. For example, if a bank identifies a name derivation of an OFAC target, then OFAC suggests that the bank add the name to its filtering process.

New accounts should be compared with the OFAC lists prior to being opened or shortly thereafter (e.g., during nightly processing). Banks that perform OFAC checks after account opening should have procedures in place to prevent transactions, other than initial deposits, from

occurring until the OFAC check is completed. Prohibited transactions conducted prior to completing an OFAC check may be subject to possible enforcement 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., weekly, 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 the bank's OFAC compliance program, to be a factor in determining the appropriate enforcement response to an apparent violation of OFAC regulations. [161] 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 have a written agreement in place and 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 sanctioned countries and blocked entities, and individuals, and disseminating such information throughout the bank's domestic operations and its offshore offices, branches and, in the case of Iran and Cuba, 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. ACH transactions may involve persons or parties subject to the sanctions programs administered by OFAC. Refer to the expanded overview section, "Automated Clearing House Transactions," for additional guidance. OFAC has clarified its interpretation of the application of OFAC's rules for domestic and cross-border ACH transactions and provided more detailed guidance on international ACH transactions. [162]

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 sanctions programs. 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," for additional guidance.

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

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. 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 validly blocked or rejected items under the various sanctions programs. When there is a question about the validity of an interdiction, banks can contact OFAC by phone or e-hot line for guidance. 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 OFAC blocking report, a separate SAR should be filed with

FinCEN that would include such 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.

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 OFAC license. If it is unclear whether a particular transaction would be authorized under the terms of the license, the bank should contact OFAC. Maintaining copies of OFAC licenses will also be useful if another bank in the payment chain requests verification of a license's validity. Copies of OFAC 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 changes or updates to the various sanctions programs, and 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 on its OFAC compliance program, procedures and processes. 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, cross-border funds transfers, trade finance products, 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.
   - The assignment of responsibilities within the institution for ensuring compliance with OFAC.
   - Timeliness of obtaining and updating OFAC lists and 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 filing to OFAC.
   - The process to manage blocked accounts (such accounts must be reported to OFAC and earn a commercially reasonable rate of interest while the funds remain blocked).
   - 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 successfully 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 blocked and rejected reports filed to OFAC and evaluate their completeness and timeliness.
   - If the bank is required to maintain blocked accounts, select a sample and ensure that the bank maintains adequate records of amounts blocked and the ownership of blocked funds, pays a commercially reasonable rate of interest on all blocked accounts, and accurately reports required information on blocked property 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.

Section 21: BSA/AML Compliance Program Structures (revised 2014)

BSA/AML Compliance Program Structures - Overview

Objective. ***Assess the structure and management of the organization's BSA/AML compliance program and if applicable, the organization's consolidated or partially consolidated approach to BSA/AML compliance.***

Every bank must have a comprehensive BSA/AML compliance program that addresses BSA requirements applicable to all operations of the organization. Banking organizations have discretion as to how the BSA/AML compliance program is structured and managed. A banking organization may structure and manage the BSA/AML compliance program or some parts of the program within a legal entity; with some degree of consolidation across entities within an organization; or as part of a comprehensive enterprise risk management framework.

Many large, complex banking organizations aggregate risk of all types (e.g., compliance, operational, credit, interest rate risk, etc.) on a firm-wide basis in order to maximize efficiencies and better identify, monitor, and control all types of risks within or across affiliates, subsidiaries, lines of business, or jurisdictions. In such organizations, management of BSA risk is generally the responsibility of a corporate compliance function that supports and oversees the BSA/AML compliance program.

Other banking organizations may adopt a structure that is less centralized but still consolidates some or all aspects of BSA/AML compliance. For example, risk assessment, internal controls (e.g., suspicious activity monitoring), independent testing, or training may be managed centrally. Such centralization can effectively maximize efficiencies and enhance assessment of risks and implementation of controls across business lines, legal entities, and jurisdictions of operation. For instance, a centralized BSA/AML risk assessment function may enable a banking organization to determine its overall risk exposure to a customer doing business with the organization in multiple business lines or jurisdictions. [168] Regardless of how a consolidated BSA/AML compliance program is organized, it should reflect the organization's business structure, size, and complexity, and be designed to effectively address risks, exposures, and applicable legal requirements across the organization.

A consolidated approach should also include the establishment of corporate standards for BSA/AML compliance that reflect the expectations of the organization's board of directors, with senior management working to ensure that the BSA/AML compliance program implements these corporate standards. Individual lines of business policies would then supplement the corporate standards and address specific risks within the line of business or department.

A consolidated BSA/AML compliance program typically includes a central point where BSA/AML risks throughout the organization are aggregated. Refer to "Consolidated BSA/AML Compliance Risk Assessment." Under a consolidated approach, risk should be assessed both

within and across all business lines, legal entities, and jurisdictions of operation. Programs for global organizations should incorporate the AML laws and requirements of the various jurisdictions in which they operate. Internal audit should assess the level of compliance with the consolidated BSA/AML compliance program.

Examiners should be aware that some complex, diversified banking organizations may have various subsidiaries that hold different types of licenses and banking charters or may organize business activities and BSA/AML compliance program components across their legal entities. For instance, a highly diversified banking organization may establish or maintain accounts using multiple legal entities that are examined by multiple regulators. This action may be taken in order to maximize efficiencies, enhance tax benefits, adhere to jurisdictional regulations, etc. This methodology may present a challenge to an examiner reviewing BSA/AML compliance in a legal entity within an organization. As appropriate, examiners should coordinate efforts with other regulatory agencies in order to address these challenges or ensure the examination scope appropriately covers the legal entity examined.

Structure of the BSA/AML Compliance Function

As discussed above, a banking organization has discretion as to how to structure and manage its BSA/AML compliance program. For example, a small institution may choose to combine BSA/AML compliance with other functions and utilize the same personnel in several roles. In such circumstances, there should still be adequate senior-level attention to BSA/AML compliance, and sufficient dedicated resources. As is the case in all structures, the audit function should remain independent.

A larger, more complex firm may establish a corporate BSA/AML compliance function to coordinate some or all BSA/AML responsibilities. For example, when there is delegation of BSA/AML compliance responsibilities, and BSA/AML compliance staff is located within lines of business, expectations should be clearly set forth in order to ensure effective implementation of the BSA/AML compliance program. In particular, allocation of responsibility should be clear with respect to the content and comprehensiveness of MIS reports, the depth and frequency of monitoring efforts, and the role of different parties within the banking organization (e.g., risk, business lines, operations) in BSA/AML compliance decision-making processes. Clearly communicating which functions have been delegated and which remain centralized helps to ensure consistent implementation of the BSA/AML compliance program among lines of business, affiliates, and jurisdictions. In addition, a clear line of responsibility may help to avoid conflicts of interest and ensure that objectivity is maintained.

Regardless of the management structure or size of the institution, BSA/AML compliance staff located within lines of business is not precluded from close interaction with the management and staff of the various business lines. BSA/AML compliance functions are often most effective when strong working relationships exist between compliance and business line staff.

In some compliance structures, the compliance staff reports to the management of the business line. This can occur in smaller institutions when the BSA/AML compliance staff reports to a senior bank officer; in larger institutions when the compliance staff reports to a line of business manager; or in a foreign banking organization's U.S. operations when the staff reports to a single office or

executive. These situations can present risks of potential conflicts of interest that could hinder effective BSA/AML compliance. To ensure the strength of compliance controls, an appropriate level of BSA/AML compliance independence should be maintained, for example, by:

- Providing BSA/AML compliance staff a reporting line to the corporate compliance or other independent function;
- Ensuring that BSA/AML compliance staff is actively involved in all matters affecting AML risk (e.g., new products, review or termination of customer relationships, filing determinations);
- Establishing a process for escalating and objectively resolving disputes between BSA/AML compliance staff and business line management; and
- Establishing internal controls to ensure that compliance objectivity is maintained when BSA/AML compliance staff is assigned additional bank responsibilities.

Management and Oversight of the BSA/AML Compliance Program

The board of directors and senior management of a bank have different responsibilities and roles in overseeing, and managing BSA/AML compliance risk. The board of directors has primary responsibility for ensuring that the bank has a comprehensive and effective BSA/AML compliance program and oversight framework that is reasonably designed to ensure compliance with BSA/AML regulation. Senior management is responsible for implementing the board-approved BSA/AML compliance program.

Boards of directors. The board of directors is responsible for approving the BSA/AML compliance program and for overseeing the structure and management of the bank's BSA/AML compliance function. The board is responsible for setting an appropriate culture of BSA/AML compliance, establishing clear policies regarding the management of key BSA/AML risks, and ensuring that these policies are adhered to in practice.

The board should ensure that senior management is fully capable, qualified, and properly motivated to manage the BSA/AML compliance risks arising from the organization's business activities in a manner that is consistent with the board's expectations. The board should ensure that the BSA/AML compliance function has an appropriately prominent status within the organization. Senior management within the BSA/AML compliance function and senior compliance personnel within the individual business lines should have the appropriate authority, independence, and access to personnel and information within the organization, and appropriate resources to conduct their activities effectively. The board should ensure that its views about the importance of BSA/AML compliance are understood and communicated across all levels of the banking organization. The board also should ensure that senior management has established appropriate incentives to integrate BSA/AML compliance objectives into management goals and compensation structure across the organization, and that corrective actions, including disciplinary measures, if appropriate, are taken when serious BSA/AML compliance failures are identified.

Senior management. Senior management is responsible for communicating and reinforcing the BSA/AML compliance culture established by the board, and implementing and enforcing the board-approved BSA/AML compliance program. If the banking organization has a separate BSA/AML compliance function, senior management of the function should establish, support, and

oversee the organization's BSA/AML compliance program. BSA/AML compliance staff should report to the board, or a committee thereof, on the effectiveness of the BSA/AML compliance program and significant BSA/AML compliance matters.

Senior management of a foreign banking organization's U.S. operations should provide sufficient information relating to the U.S. operations' BSA/AML compliance to the governance or control functions in its home country, and should ensure that responsible senior management in the home country has an appropriate understanding of the BSA/AML risk and control environment governing U.S. operations. U.S. management should assess the effectiveness of established BSA/AML control mechanisms for U.S. operations on an ongoing basis and report and escalate areas of concern as needed. As appropriate, corrective action then should be developed, implemented and validated.

Consolidated BSA/AML Compliance Programs

Banking organizations that centrally manage the operations and functions of their subsidiary banks, other subsidiaries, and business lines should ensure that comprehensive risk management policies, procedures, and processes are in place across the organization to address the entire organization's spectrum of risk. An adequate consolidated BSA/AML compliance program provides the framework for all subsidiaries, business lines, and foreign branches to meet their specific regulatory requirements (e.g., country or industry requirements). Accordingly, banking organizations that centrally manage a consolidated BSA/AML compliance program should, among other things provide appropriate structure; and advise the business lines, subsidiaries, and foreign branches on the development of appropriate guidelines. For additional guidance, refer to the expanded overview section, "Foreign Branches and Offices of U.S. Banks."

An organization applying a consolidated BSA/AML compliance program may choose to manage only specific compliance controls (e.g., suspicious activity monitoring systems, audit) on a consolidated basis, with other compliance controls managed solely within affiliates, subsidiaries, and business lines. When this approach is taken, examiners must identify which portions of the BSA/AML compliance program are part of the consolidated BSA/AML compliance program. This information is critical when scoping and planning a BSA/AML examination.

When evaluating a consolidated BSA/AML compliance program for adequacy, the examiner should determine reporting lines and how each affiliate, subsidiary, business line, and jurisdiction fits into the overall compliance structure. This should include an assessment of how clearly roles and responsibilities are communicated across the bank or banking organization. The examiner also should assess how effectively the bank or banking organization monitors BSA/AML compliance throughout the organization, including how well the consolidated and nonconsolidated BSA/AML compliance program captures relevant data from subsidiaries.

The evaluation of a consolidated BSA/AML compliance program should take into consideration available information about the adequacy of the individual subsidiaries' BSA/AML compliance program. Regardless of the decision to implement a consolidated BSA/AML compliance program in whole or in part, the program should ensure that all affiliates, including those operating within foreign jurisdictions, meet their applicable regulatory requirements. For example, an audit program implemented solely on a consolidated basis that does not conduct appropriate transaction

testing at all subsidiaries subject to the BSA would not be sufficient to meet regulatory requirements for independent testing for those subsidiaries. If dissemination of certain information is limited and therefore transparency across the organization is restricted, audit should be aware and ensure AML controls are commensurate with those risks.

Suspicious Activity Reporting

Bank holding companies (BHC) or any nonbank subsidiary thereof, or a foreign bank that is subject to the BHC Act or any nonbank subsidiary of such a foreign bank operating in the United States, are required to file SARs. A BHC's nonbank subsidiaries operating only outside the United States, are not required to file SARs. Certain savings and loan holding companies, and their nondepository subsidiaries, are required to file SARs pursuant to Treasury regulations (e.g., insurance companies (31 CFR 1025.320) and broker/dealers (31 CFR 1023.320)). In addition, savings and loan holding companies, if not required, are strongly encouraged to file SARs in appropriate circumstances. On January 20, 2006, the Financial Crimes Enforcement Network, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and the Office of Thrift Supervision issued guidance authorizing banking organizations to share SARs with head offices and controlling companies, whether located in the United States or abroad. Refer to the core overview section, "Suspicious Activity Reporting," for additional information.

Examination Procedures - BSA/AML Compliance Program Structures

Objective. ***Assess the structure and management of the banking organization's BSA/AML compliance program, and, if applicable, the banking organization's consolidated or partially consolidated approach to BSA/AML compliance. A BSA/AML compliance program may be structured in a variety of ways, and an examiner should perform procedures based on the structure of the organization. Completion of these procedures may require communication with other regulators.***

1. Review the structure and management of the BSA/AML compliance program. Communicate with peers at other federal and state banking agencies, as necessary, to confirm their understanding of the organization's BSA/AML compliance program. This approach promotes consistent supervision and lessens regulatory burden for the banking organization. Determine the extent to which the structure of the BSA/AML compliance program affects the organization being examined, by considering:

   - The existence of consolidated or partially consolidated operations or functions responsible for day-to-day BSA/AML operations, including, but not limited to, the centralization of suspicious activity monitoring and reporting, currency transaction reporting, currency exemption review and reporting, or recordkeeping activities.
   - The consolidation of operational units, such as financial intelligence units, dedicated to and responsible for monitoring transactions across activities, business lines, or legal

entities. (Assess the variety and extent of information that data or transaction sources (e.g., banks, broker/dealers, trust companies, Edge Act and agreement corporations, insurance companies, or foreign branches) are entering into the monitoring and reporting systems).
- The extent to which the banking organization (or a corporate-level unit, such as audit or compliance) performs regular independent testing of BSA/AML activities.
- The sufficiency of audit in jurisdictions with restrictive privacy laws that may limit the dissemination of information.
- Whether and to what extent a corporate-level unit sponsors BSA/AML training.

2. Review testing for BSA/AML compliance throughout the banking organization, as applicable, and identify program deficiencies.

3. Review board minutes to determine the adequacy of MIS and of reports provided to the board of directors. Ensure that the board of directors has received appropriate notification of SARs filed.

4. Review policies, procedures, processes, and risk assessments formulated and implemented by the organization's board of directors, a board committee thereof, or senior management. As part of this review, assess effectiveness of the organization's ability to perform the following responsibilities:

   - Manage the BSA/AML compliance program and provide adequate oversight.
   - Set and communicate corporate standards that reflect the expectations of the organization's board of directors and provide for clear allocation of BSA/AML compliance responsibilities.
   - Promptly identify and effectively measure, monitor, and control key risks throughout the organization.
   - Develop an adequate risk assessment and the policies, procedures, and processes to comprehensively manage those risks.
   - Develop procedures for evaluation, approval, and oversight of risk limits, new business initiatives, and strategic changes.
   - Oversee the compliance of subsidiaries with applicable regulatory requirements (e.g., country and industry requirements).
   - Oversee the compliance of subsidiaries with the requirements of the BSA/AML compliance program.
   - Identify weaknesses in the BSA/AML compliance program and implement necessary and timely corrective action, at both the organizational and subsidiary levels.

5. To ensure compliance with regulatory requirements, review the organization's procedures for monitoring and filing SARs. For additional guidance, refer to the core overview and examination procedures, "Suspicious Activity Reporting."

6. Once the examiner has completed the above procedures, the examiner should discuss their findings with the following parties, as appropriate:

   - Examiner in charge.
   - Person (or persons) responsible for ongoing supervision of the organization and subsidiary banks, as appropriate.

- Corporate management.

7. On the basis of examination procedures completed, form a conclusion about the adequacy of the BSA/AML compliance program structures and management including, if applicable, the effectiveness of the consolidated or partially consolidated approach to compliance.

Section 22: Foreign Branches and Offices of U.S. Banks (revised 2014)

Foreign Branches and Offices of U.S. Banks - Overview

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

U.S. banks open foreign branches and offices to meet specific customer demands, to help the bank grow, or to expand products or services offered. Foreign branches and offices vary significantly in size, complexity of operations, and scope of products and services offered. Examiners must take these factors into consideration when reviewing the foreign branches and offices AML compliance program. The definitions of "financial institution" and "bank" in the BSA and its implementing regulations do not encompass foreign offices or foreign investments of U.S. banks or Edge and agreement corporations. Nevertheless, banks are expected to have policies, procedures, and processes in place at all their branches and offices to protect against risks of money laundering and terrorist financing. AML policies, procedures, and processes at the foreign office or branch should comply with local requirements and be consistent with the U.S. bank's standards; however, they may need to be tailored for local or business practices.

Risk Factors

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

The examiner should understand the foreign jurisdiction's various AML requirements. Secrecy laws or their equivalent may affect the ability of the foreign branch or office to share information with the U.S. parent bank, or the ability of the examiner to examine on-site. While banking organizations with overseas branches or subsidiaries may find it necessary to tailor monitoring approaches as a result of local privacy laws, the compliance oversight mechanism should ensure it can effectively assess and monitor risks within such branches and subsidiaries. Although specific BSA requirements are not applicable at foreign branches and offices, banks are expected to have policies, procedures, and processes in place at all their branches and offices to protect against risks of money laundering and terrorist financing. In this regard, foreign branches and offices should be guided by the U.S. bank's BSA/AML policies, procedures, and processes. The

foreign branches and offices must comply with applicable OFAC requirements and all local AML-related laws, rules, and regulations.

Risk Mitigation

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

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

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

Scoping AML Examinations

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

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

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

U.S.-Based Examinations

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

Host Jurisdiction-Based Examinations

On-site work in the host jurisdiction enables examiners not only to better understand the role of the U.S. bank in relation to its foreign branch or office but also, perhaps more importantly, permit examiners to determine the extent to which the U.S. bank's global policies, procedures, and processes are being followed locally.

The standard scoping and planning process will determine the focus of the examination and the resource needs. There may be some differences in the examination process conducted abroad. The host supervisory authority may send an examiner to join the U.S. team or request attendance at meetings at the beginning and at the conclusion of the examination. AML reporting requirements also are likely to be different, as they will be adjusted to local regulatory requirements.

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

Examination Procedures - Foreign Branches and Offices of U.S. Banks

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

1. Review the policies, procedures, and processes related to foreign branches and offices[176] to evaluate their adequacy given the activity in relation to the bank's risk, and assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. On the basis of a review of MIS and internal risk rating factors, determine whether the U.S. bank's head office effectively identifies and monitors foreign branches and offices, particularly those conducting higher-risk transactions or located in higher-risk jurisdictions.

3. Determine whether the U.S. bank's head office system for monitoring foreign branches and offices and detecting unusual or suspicious activities at those branches and offices is adequate given the bank's size, complexity, location, and types of customer relationships. Determine whether the host country requires reporting of suspicious activities and, if permitted and available, review those reports. Determine whether this information is provided to the U.S. bank's head office and filtered into a bank-wide or, if appropriate, a firm-wide assessment of suspicious activities.

4. Review the bank's tiering or organizational structure report, which should include a list of all legal entities and the countries in which they are registered. Determine the locations of foreign

branches and offices, including the foreign regulatory environment and the degree of access by U.S. regulators for on-site examinations and customer records.

5. Review any partnering or outsourcing relationships of foreign branches and offices. Determine whether the relationship is consistent with the bank's AML program.

6. Determine the type of products, services, customers, entities, and geographic locations served by the foreign branches and offices. Review the risk assessments of the foreign branches and offices.

7. Review the management, compliance, and audit structure of the foreign branches and offices. Identify the decisions that are made at the bank's U.S. head office level versus those that are made at the foreign branch or office.

8. Determine the involvement of the U.S. bank's head office in managing and monitoring foreign branches and offices. Conduct a preliminary evaluation of the foreign branches or offices through discussions with senior management at the U.S. bank's head office (e.g., operations, customers, entities, jurisdictions, products, services, management strategies, audit programs, anticipated product lines, management changes, branch expansions, AML risks, and AML programs). Similar discussions should occur with management of the foreign branches and offices, particularly those that may be considered higher risk.

9. Coordinate with the host country supervisor and, if applicable, U.S. federal and state regulatory agencies. Discuss their assessment of the foreign branches' and offices' compliance with local laws. Determine whether there are any restrictions on materials that may be reviewed, copied, or taken out of the country.

10. If available, review the following:

    - Previous regulatory examination reports.
    - Host country's regulatory examination report.
    - Audit reports and supporting documentation.
    - Compliance reviews and supporting documentation.

11. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

12. Make a determination whether transaction testing is feasible. If feasible on the basis of the bank's risk assessment of this activity and prior examination and audit reports, select a sample of higher-risk foreign branch and office activity. Complete transaction testing from appropriate expanded examination procedures sections (e.g., pouch activity).

13. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with the U.S. bank's foreign branches and offices.

Section 23: Parallel Banking (revised 2014)

Parallel Banking - Overview

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

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

Risk Factors

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

Risk Mitigation

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

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

Examination Procedures - Parallel Banking

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

1. Determine whether parallel banking relationships exist through discussions with management or by reviewing inter-party activities involving the bank and another foreign financial institution. Review the policies, procedures, and processes related to parallel banking relationships. Evaluate the adequacy of the policies, procedures, and processes given the bank's parallel banking activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. Determine whether there are any conflicts of interest or differences in policies, procedures, and processes between parallel bank relationships and other foreign correspondent bank relationships. Particular consideration should be given to funds transfer, pouch, and payable through activities because these activities are more vulnerable to money laundering. If the bank engages in any of these activities, examiners should consider completing applicable expanded examination procedures that address each of these topics.

3. From a review of management MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors parallel banking relationships, particularly those that pose a higher-risk for money laundering.

4. Determine whether the bank's system for monitoring parallel banking relationships for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

5. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

6. On the basis of the bank's risk assessment of its parallel banking activities, as well as prior examination and audit reports, select a sample of higher-risk activities from parallel banking relationships (e.g., foreign correspondent banking, funds transfer, payable through accounts, and pouch).

7. Consider the location of the foreign parallel financial institution. If the jurisdiction is higher risk, examiners should review a larger sample of transactions between the two institutions. Banks doing business with parallel foreign banking organizations in countries not designated as higher risk may still require EDD, but that determination will be based on the size, nature, and type of the transactions between the institutions.

8. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with parallel banking organizations. Focus on whether controls exist to ensure independent and arm's-length dealings between the two entities. If significant concerns are raised about the

relationship between the two entities, recommend that this information be forwarded to the appropriate supervisory authorities.

Section 24: Expanded Examination Overview and Procedures for Products and Services (revised 2014)

Correspondent Accounts (Domestic) - Overview

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

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

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

Bankers' Banks

A bankers' bank, which is organized and chartered to do business with other banks, is generally owned by the banks it services. Bankers' banks, which do not conduct business directly with the public, offer correspondent banking services to independent community banks, thrifts, credit unions, and real estate investment trusts. Bankers' banks provide services directly, through outsourcing arrangements, or by sponsoring or endorsing third parties. The products bankers' banks offer normally consist of traditional correspondent banking services. Bankers' banks should have risk-based policies, procedures, and processes to manage the BSA/AML risks involved in these correspondent relationships to detect and report suspicious activities.

Generally, a bankers' bank signs a service agreement with the respondent bank outlining each party's responsibilities. The service agreement may include the following:

- Products and services provided.
- Responsibility for record keeping (e.g., CTRs filed).
- Responsibility for task performed (e.g., OFAC filtering).
- Review of oversight documentation (e.g., audit and consultants reports).

Risk Factors

Because domestic banks must follow the same regulatory requirements, BSA/AML risks in domestic correspondent banking, including bankers' banks, are minimal in comparison to other types of financial services, especially for proprietary accounts (i.e., the domestic bank is using the correspondent account for its own transactions). Each bank, however, has its own approach for conducting its BSA/AML compliance program, including customer due diligence, MIS, account monitoring, and reporting suspicious activities. Furthermore, while a domestic correspondent account may not be considered higher risk, transactions through the account, which may be conducted on behalf of the respondent's customer, may be higher risk. Money laundering risks can be heightened when a respondent bank allows its customers to direct or execute transactions through the correspondent account, especially when such transactions are directed or executed through an ostensibly proprietary account.

The correspondent bank also faces heightened risks when providing direct currency shipments for customers of respondent banks. This is not to imply that such activities necessarily entail money laundering, but these direct currency shipments should be appropriately monitored for unusual and suspicious activity. Without such a monitoring system, the correspondent bank is essentially providing these direct services to an unknown customer.

Risk Mitigation

Banks that offer correspondent bank services to respondent banks should have policies, procedures, and processes to manage the BSA/AML risks involved in these correspondent relationships and to detect and report suspicious activities. Banks should ascertain whether domestic correspondent accounts are proprietary or allow third-party transactions. When the respondent bank allows third-party customers to transact business through the correspondent account, the correspondent bank should ensure that it understands the due diligence and monitoring procedures applied by the respondent on its customers that utilize the account.

The level of risk varies depending on the services provided and the types of transactions conducted through the account and the respondent bank's BSA/AML compliance program, products, services, customers, entities, and geographic locations. Each bank should appropriately monitor transactions of domestic correspondent accounts relative to the level of assessed risk. In addition, domestic banks are independently responsible for OFAC compliance for any transactions that flow through their banks. Appropriate filtering should be in place. Refer to core overview section and examination procedures, "Office of Foreign Assets Control."

Examination Procedure - Correspondent Accounts (Domestic)

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

1. Review the policies, procedures, and processes, and any bank service agreements related to domestic correspondent banking relationships. Evaluate the adequacy of the policies, procedures, and processes given the bank's domestic correspondent accounts and the risks they

present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. From a review of MIS and internal risk rating factors, determine whether the bank has identified any domestic correspondent banking activities as higher risk.

3. Determine whether the bank's system for monitoring domestic correspondent accounts for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

4. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

5. On the basis of the bank's review of respondent accounts[9] with unusual or higher-risk activity, its risk assessment, and prior examination and audit reports, select a sample of respondent accounts. From the sample selected, perform the following examination procedures:

   - Review bank statements for domestic correspondent accounts.
   - Review large or unusual transactions to determine their nature. As necessary, obtain and review copies of credit or debit advices, general ledger tickets, and other supporting documentation.
   - Note any currency shipments or deposits made on behalf of a respondent bank's customer. Based on this information determine whether:
     - Currency shipments are adequately documented.
     - The respondent bank has performed due diligence on customers that conduct large currency transactions.
     - CTRs are properly filed and activity is commensurate with expected activity.

6. Review the bank statements for domestic correspondent account records, or telex records of accounts controlled by the same person for large deposits of cashier's checks, money orders, or similar instruments drawn on other banks in amounts under $10,000. These funds may possibly be transferred elsewhere in bulk amounts. Note whether the instruments under $10,000 are sequentially numbered.

7. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with domestic correspondent bank relationships.

Correspondent Accounts (Foreign) - Overview

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

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

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

Contractual Agreements

Each relationship that a U.S. bank has with a foreign correspondent financial institution should be governed by an agreement or a contract describing each party's responsibilities and other relationship details (e.g., products and services provided, acceptance of deposits, clearing of items, forms of payment, and acceptable forms of endorsement). The agreement or contract should also consider the foreign financial institution's AML regulatory requirements, customer base, due diligence procedures, and permitted third-party usage of the correspondent account.

Risk Factors

Some foreign financial institutions are not subject to the same or similar regulatory guidelines as U.S. banks; therefore, these foreign institutions may pose a higher money laundering risk to their respective U.S. bank correspondent(s). Investigations have disclosed that, in the past, foreign correspondent accounts have been used by drug traffickers and other criminal elements to launder funds. Shell companies are sometimes used in the layering process to hide the true ownership of accounts at foreign correspondent financial institutions.

Because of the large amount of funds, multiple transactions, and the U.S. bank's potential lack of familiarity with the foreign correspondent financial institution's customer, criminals and terrorists can more easily conceal the source and use of illicit funds. Consequently, each U.S. bank, including all overseas branches, offices, and subsidiaries, should closely monitor transactions related to foreign correspondent accounts.

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

Nested Accounts

Nested accounts occur when a foreign financial institution gains access to the U.S. financial system by operating through a U.S. correspondent account belonging to another foreign financial institution. If the U.S. bank is unaware that its foreign correspondent financial institution customer is providing such access to third-party foreign financial institutions, these third-party financial institutions can effectively gain anonymous access to the U.S. financial system. Unacceptable nested activity and other activity of concern may be characterized by transactions to jurisdictions in which the foreign financial institution has no known business activities or interests and transactions in which the total volume and frequency significantly exceeds expected activity for the foreign financial institution, considering its customer base or asset size. U.S. banks should also focus on nested account transactions with any entities the bank has designated as higher risk.

Risk Mitigation

U.S. banks that offer foreign correspondent financial institution services should have policies, procedures, and processes to manage the BSA/AML risks inherent with these relationships and should closely monitor transactions related to these accounts to detect and report suspicious activities. The level of risk varies depending on the foreign financial institution's strategic profile, including its size and geographic locations, the products and services it offers, and the markets and customers it serves. The Clearing House Association, LLC., and The Wolfsberg Group have published suggested industry standards and guidance for banks that provide foreign correspondent banking services. When dealing with foreign correspondent account relationships, it is important for the bank to keep in mind regulatory requirements related to special measures issued under 311 of the USA PATRIOT Act contained in the expanded overview section, "Special Measures." Additional information relating to risk assessments and due diligence is contained in the core overview section, "Foreign Correspondent Account Recordkeeping, Reporting, and Due Diligence."

The U.S. bank's policies, procedures, and processes should:

- Specify appropriate account-opening/on-boarding procedures, which may include minimum levels of documentation to be obtained from prospective customers; an account review and approval process that is independent of the correspondent account business line for potential higher-risk customers; and a description of circumstances when the bank does not open an account.
- Assess the risks posed by a prospective foreign correspondent customer relationship utilizing consistent, well-documented risk-rating methodologies, and incorporate that risk determination into the bank's suspicious activity monitoring system.
- Understand the intended use and purpose of the accounts and expected account activity (e.g., determine whether the relationship serves as a payable through account).
- Understand the foreign correspondent financial institution's other correspondent

relationships (e.g., determine whether and how nested accounts are to be utilized).
- Conduct adequate and ongoing due diligence on the foreign correspondent financial institution relationships, which may include periodic site visits based on risk.
- Determine whether the foreign correspondent financial institution has in place acceptable AML compliance processes and controls.
- Ensure that appropriate due diligence standards are applied to those accounts determined to be higher risk.
- Ensure that foreign correspondent financial institution relationships are appropriately included within the U.S. bank's suspicious activity monitoring and reporting systems.
- Follow up on account activity and transactions that do not fit the foreign financial institution customer's strategic profile (i.e., transactions involving customers, industries or products that are not generally part of that foreign financial institution's customer base or market).
- Establish a formalized process for escalating suspicious information on potential and existing customers to an appropriate management level for review.
- Establish criteria for closing the foreign correspondent financial institution account.

As a sound practice, U.S. banks are encouraged to communicate their AML-related expectations to their foreign correspondent financial institution customers. Moreover, the U.S. bank should generally understand and assess the quality of the AML controls at the foreign correspondent financial institution, including customer due diligence practices, suspicious activity identification processes, and recordkeeping documentation. They should also have an understanding of the effectiveness of the AML regime of the foreign jurisdictions in which their foreign correspondent banking customers operate.

Examination Procedures - Correspondent Accounts (Foreign)

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

1. Review the policies, procedures, and processes related to foreign correspondent financial institution account relationships. Evaluate the adequacy of the policies, procedures, and processes. Assess whether the controls are adequate to reasonably protect the U.S. bank from money laundering and terrorist financing.

2. From a review of MIS and internal risk-rating factors, determine whether the U.S. bank effectively identifies and monitors foreign correspondent financial institution account relationships, particularly those that pose a higher risk for money laundering.

3. If the U.S. bank has a standardized foreign correspondent agreement, review a sample agreement to determine whether each party's responsibilities, products, and services provided, and allowable third party usage of the correspondent account, are covered under the contractual arrangement. If the U.S. bank does not have a standardized agreement, refer to the transaction testing examination procedures.

4. Determine whether the U.S. bank's system for monitoring foreign correspondent financial institution account relationships for suspicious activities, and for reporting suspicious activities, is adequate given the U.S. bank's size, complexity, location, and types of customer relationships.

5. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control." for guidance.

Transaction Testing

6. On the basis of the U.S. bank's risk assessment of its foreign correspondent activities, as well as prior examination and audit reports, select a sample of higher-risk foreign correspondent financial institution account relationships. The higher-risk sample should include relationships with foreign financial institutions located in jurisdictions that do not cooperate with international AML efforts and in other jurisdictions that the U.S. bank has determined pose a higher risk. From the sample selected, perform the following examination procedures:

    - Review a foreign correspondent agreement or contract that delineates each party's responsibilities and the products and services provided.
    - Review U.S. bank statements for foreign correspondent accounts and, as necessary, specific transaction details. Compare expected transactions with actual activity.
    - Determine whether actual activity is consistent with the nature of the customer's business. Identify any unusual or suspicious activity.
    - Review large or unusual transactions to determine their nature. As necessary, obtain and review copies of credit or debit advices, general ledger tickets, and other supporting documentation.
    - Analyze transactions to identify behavior indicative of nested accounts, intermediary or clearing agent services, or other services for third-party foreign financial institutions that have not been clearly identified.

7. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with foreign correspondent financial institution relationships.

Bulk Shipments of Currency - Overview

Objective. ***Assess the adequacy of the U.S. bank's systems to manage the risks associated with receiving and sending bulk shipments of currency and management's implementation of effective monitoring and reporting systems.***

Bulk shipments of currency, sometimes referred to as wholesale cash, entails the transportation of large volumes of U.S. or foreign bank notes. Bulk shipments of currency can be sent from sources either inside or outside the United States to a bank in the United States. Shipments are also made from a bank in the United States to a recipient in a foreign jurisdiction..

This business uses common carriers of currency, private couriers, or the Postal Service to physically transport shipments. These shipments can involve pedestrians, railways, roads, sea or air. Often, but not always, shipments take the form of containerized cargo.

Regardless of the business model employed, each physical transportation involves multiple parties that are responsible for fulfilling one or more specific roles in the delivery process. FinCEN guidance defines these roles to include:

- the common carrier,
- the shipper,
- the consignee,
- the currency originator, and
- the currency recipient.

Typically, a common carrier of currency transports currency or other monetary instruments as a business, for a person that engages the carrier for a fee (the "shipper"), from one place to another, to be delivered to the person appointed by the shipper to receive the currency or monetary instruments (the "consignee"). The shipper may be acting of its own accord or on instructions from a different person (the "currency originator"), and the consignee may be instructed to deliver the currency or other monetary instruments to the account of a final beneficiary (the "currency recipient"). The same person may fulfill more than one role in the same shipment.

The same person may be both the shipper, and the currency originator (i.e., individuals or businesses that generate currency from cash sales of commodities or other products or services (including monetary instruments or exchanges of currency). Shippers also may be 31 CFR 1010.100(k) defines "common carrier" as any person engaged in the business of transporting individuals or goods for a fee who holds itself out as ready to engage in such transportation for hire and who undertakes to do so indiscriminately for all persons who are prepared to pay the fee for the particular service offered. This section addresses a subgroup of common carriers, those persons engaged as a business in the transportation of currency, other monetary instruments, or commercial papers, referred to herein as "common carriers of currency." An armored car service is a type of this subgroup of common carriers. intermediaries that ship currency gathered from other shippers, who in turn are gathering currency from their customers who are currency originators. Intermediaries may be other banks, central banks, nondeposit financial institutions, or agents of these entities. Banks receive bulk shipments of currency directly when they take possession of an actual shipment. Banks receive bulk shipments of currency indirectly when they take possession of the economic equivalent of a currency shipment, such as through a cash letter notification or deposit into the bank's account at the Federal Reserve. In the case of a shipment

received indirectly, the actual shipment usually moves toward the bank only as far as a Federal Reserve Bank or branch, where the value of the currency becomes recorded as held on the bank's behalf. Whether the shipment to or from the bank is direct or indirect, banks are required to report the receipt or disbursement of currency in excess of $10,000 via a Currency Transaction Report (CTR) (31 CFR 1010.311) subject to the exemptions at 31 CFR 1020.315. Note that most categories of CTR exempt persons apply only to the extent of the exempt person's domestic operations, 31 CFR 1020.315(b)(1-7). For more information on CTRs refer to the Currency Transaction Reporting Overview.

Report of International Transportation of Currency or Monetary Instruments Subject to certain exemptions, each person who physically transports, mails or ships, or causes to be physically transported, mailed, or shipped currency or other monetary instruments, is required to report shipments in an aggregate amount exceeding $10,000 received from or shipped to locations outside the U.S. via a Report of International Transportation of Currency or Monetary Instruments (CMIR) (31 CFR 1010.340) For more information on CMIRs refer to the International Transportation of Currency or Monetary Instruments Overview.

Regardless of whether an exemption from filing a CMIR or CTR applies, banks must still monitor for, and report, suspicious activity.

Risk Factors

Bulk shipments of currency to banks from shippers that are presumed to be reputable may nevertheless originate from illicit activity. The monetary proceeds of criminal activities, for example, often reappear in the financial system as seemingly legitimate funds that have been placed and finally integrated by flowing through numerous intermediaries and layered transactions that disguise the origin of the funds. Layering can include shipments to or through other jurisdictions. Accordingly, banks that receive direct or indirect bulk shipments of currency risk becoming complicit in money laundering or terrorist financing schemes.

In recent years, the smuggling of bulk currency has become a preferred method for moving illicit funds across borders. Because bulk cash that is smuggled out of the United States is usually denominated in U.S. dollars, those who receive the smuggled bulk cash must find ways to re-integrate the currency into the global banking system. Often, this occurs through the use of a foreign financial institution, many times a money services business, that wittingly or unwittingly receives the illicit U.S.-dollar denominated proceeds, and then originates a cash letter instrument (or a funds transfer) for processing by, or deposit into, a U.S. bank. The foreign financial institution then initiates the process of physically repatriating (shipping) the cash back into the United States. Experience has shown a direct correlation between the smuggling of bulk currency, the heightened use of wire transfers, remote deposit capture (RDC) transactions or cash letter instruments from certain foreign financial institutions and/or jurisdictions, and bulk shipments of currency into the United States from the same foreign financial institutions or jurisdictions.

The activity of shipping currency in bulk is not necessarily indicative of criminal or terrorist activity. Many individuals and businesses, both domestic and foreign, generate currency from legitimate cash sales of commodities or other products or services or certain industries such as tourism or commerce. Also, intermediaries gather and ship currency from single or multiple currency originators whose activities are legitimate. Banks may legitimately offer services to receive such shipments. However, banks should be aware of the potential misuse of their services

by shippers of bulk currency. Banks should also guard against introducing the monetary proceeds of criminal or terrorist activity into the financial system. Banks should have a clear understanding of the appropriate volumes of currency shipments that are commensurate with the currency originator's or shipper's profile (size, location, strategic focus, customer base, geographic footprint) and the economic activity that generates the cash.

To inform banks on the topic of bulk currency shipments, FinCEN has issued a number of advisories that set forth certain activities that may be associated with currency smuggling. According to FinCEN, U.S. law enforcement has observed a dramatic increase in the smuggling of bulk cash proceeds from the sale of narcotics and other criminal activities from the United States into Mexico. Although the FinCEN advisories deal specifically with the shipment of bulk currency to and from the United States and Mexico, the issues discussed could be pertinent to shipping bulk currency to and from other jurisdictions as well. Banks should look at each situation on a case by case basis.

Law enforcement has identified the following activities that, in various combinations, may be associated with currency smuggling:

- An increase in the sale of large denomination U.S. bank notes to foreign financial institutions by U.S. banks.
- Small denomination U.S. bank notes smuggled into a foreign country being exchanged for large denomination U.S. bank notes possessed by foreign financial institutions.
- Large volumes of small denomination U.S. bank notes being sent from foreign nonbank financial institutions to their accounts in the United States via armored transport, or sold directly to U.S. banks.
- Multiple wire transfers initiated by foreign nonbank financial institutions that direct U.S. banks to remit funds to other jurisdictions that bear no apparent business relationship with that foreign nonbank financial institution (recipients include individuals, businesses, and other entities in free trade zones and other locations).
- The exchange of small denomination U.S. bank notes for large denomination U.S. bank notes that may be sent to foreign countries.
- Deposits by foreign nonbank financial institutions to their accounts at U.S. banks that include third-party items (including sequentially numbered monetary instruments).
- Deposits of currency and third-party items by foreign nonbank financial institutions into their accounts at foreign financial institutions and thereafter direct wire transfers to the foreign nonbank financial institution's accounts at U.S. banks.
- Structuring of currency deposits into an account in one geographic area, with the funds subsequently withdrawn in a different geographic region with little time elapsing between deposit and withdrawal. This is usually known as "funnel account" or "interstate cash" activity.

Risk Mitigation

U.S. banks that offer services to receive bulk shipments of currency should have policies, procedures, and processes in place that mitigate and manage the BSA/AML risks associated with the receipt of bulk currency shipments. Banks should also closely monitor bulk currency shipment transactions to detect and report suspicious activity, with particular emphasis on the source of funds and the reasonableness of transaction volumes from currency originators and intermediaries.

Risk mitigation begins with an effective risk assessment process that distinguishes relationships and transactions that present a higher risk of money laundering or terrorist financing. Risk assessment processes should consider currency originator and intermediary ownership, geographies, economic factors and the nature, source, location, and control of bulk currency. For additional information relating to risk assessments and due diligence, refer to the core overview sections "BSA/AML Risk Assessment" and "Customer Due Diligence."

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

- Specify appropriate risk-based relationship opening procedures, which may include minimum levels of documentation to be obtained from prospective currency originators and intermediaries; specify relationship approval process that, for potential higher-risk relationships, is independent of the business line and may include a visit to the prospective shipper or shipping-preparation sites; and describe the circumstances under which the bank does not open a relationship.
- Determine the intended use of the relationship, the expected volumes, frequency of activity arising from transactions, sources of funds, reasonableness of volumes based on originators and shippers (e.g., based on size, location, strategic focus, customer base, geographic footprint), economic and regulatory conditions that may affect currency circulation and any required BSA reporting obligations (CTRs, CMIRs, etc.).
- Identify the characteristics of acceptable and unacceptable transactions, including circumstances when the bank does or does not accept bulk currency shipments.
- Assess the risks posed by a prospective shipping relationship using consistent, well-documented risk-rating methodologies.
- Incorporate risk assessments, as appropriate, into the bank's customer due diligence, EDD, and suspicious activity monitoring systems.
- Require adequate and ongoing due diligence once the relationship is established, which, as appropriate, may include periodic visits to the shipper and to shipping-preparation sites. As necessary, scrutinize the root source of cash shipments for reasonableness and legitimacy using risk-based processes.
- Ensure that appropriate due diligence standards are applied to relationships determined to be higher risk.
- Include procedures for processing shipments, including employee responsibilities, controls, reconciliation and documentation requirements, and employee/management authorizations.
- Establish a process for escalating suspicious information on potential and existing currency originator and intermediary relationships and transactions to an appropriate management level for review.
- Refuse shipments having questionable or suspicious origins.
- Ensure that shipping relationships and comparisons of expected vs. actual shipping volumes are included, as appropriate, within the U.S. bank's systems for monitoring and reporting suspicious activity.
- Establish criteria for terminating a shipping relationship.
- Ensure that shipments involving the foreign correspondent relationships are covered by the bank's due diligence program for correspondent accounts for foreign financial institutions.

As a sound practice, U.S. banks should inform currency originators, shippers, and intermediaries of the BSA/AML-related requirements and expectations that apply to U.S. banks.

U.S. banks also should understand the BSA/AML controls that apply to, or are otherwise adopted by, the currency originator, shipper, or intermediary, including any customer due diligence and recordkeeping requirements or practices.

Other bank controls may also prove useful in protecting banks against illicit bulk shipments of currency. These may include effective controls over foreign correspondent banking activity, pouch activity, funds transfers, international Automated Clearing House transactions, and remote deposit capture.

Contractual Agreements

U.S. banks should establish agreements or contracts with currency originators, shippers, intermediaries, and/or established common carriers such as the ones that are allowed to deliver directly to the bank's vault. The agreement or contract should describe each party's responsibilities and other relevant details of the relationship. The agreement or contract should reflect and be consistent with any BSA/AML considerations that apply to the bank, the common carrier, currency originator or intermediary, and their customers. The agreement or contract should also address expectations about due diligence and permitted use of the shipper's services by third parties. While agreements and contracts should also provide for respective BSA/AML controls, obligations, and considerations, U.S. banks cannot shift their BSA/AML responsibilities to others.

Examination Procedures - Bulk Shipments of Currency

Objective. ***Assess the adequacy of the U.S. bank's systems to manage the risks associated with receiving and sending bulk shipments of currency, and management's ability to implement effective due diligence, monitoring, and reporting systems.***

1. Determine whether the bank receives or distributes shipments of bulk currency.

2. Review the policies, procedures, and processes related to receiving shipments of bulk currency for adequacy, given the activity and the risks presented.

3. Review the list of currency originators, shippers, and intermediaries that send bulk currency shipments to the bank.

4. Determine whether management has assessed the risks associated with receiving bulk currency shipments from particular currency originators, shippers, and intermediaries. Consider the source of the currency originator, shipper, or intermediary's currency and the reasonableness of transaction volumes. Assess the adequacy of the risk-assessment methodology.

5. From a review of MIS and internal risk-rating factors, determine whether the bank effectively identifies and monitors relationships with currency originators and intermediaries, particularly those that pose a higher risk for money laundering or terrorist financing.

6. If the bank has a standardized agreement or contract with currency originators, shippers, intermediaries, and/or established common carriers, review a sample agreement or contract to

determine whether each party's responsibilities, products, and services provided, and allowable use of the relationship by third-parties , including the parties' BSA/AML responsibilities, are covered. If the bank does not have a standardized agreement or contract, refer to the transaction testing examination procedures below.

7. Determine whether the bank files required BSA reports (e.g., CTRs or CMIRs), if applicable.

8. Determine whether the bank's system for monitoring and reporting suspicious activities related to shipping relationships and transactions is adequate given the bank's size, complexity, location, and types of customer relationships.

9. Determine whether the bank is monitoring for expected versus actual shipping volumes and taking action in response to unusual or inordinate increase in volumes or patterns.

Transaction Testing

10. Based on the bank's risk assessment of its relationships with currency originators, shippers, and intermediaries, as well as prior examination and audit reports, select a sample of currency originators, shippers, or intermediaries and recent bulk currency shipments. The sample should include relationships with currency originators, shippers, and intermediaries located in or shipping from, jurisdictions that may pose a higher risk for money laundering and terrorist financing, or that participate in businesses that may pose a higher risk for money laundering and terrorist financing.

11. Preferably on an unannounced basis and over a period of several days, observe the process for accepting shipments of bulk currency. Review the records and the shipments for irregularities. From the samples selected, perform the following examination procedures:

    - Review for completeness a relationship agreement or contract that delineates each party's responsibilities and the products and services provided.
    - Review U.S. bank statements of accounts and, as necessary, specific transaction details.
    - Review vault control records for bulk currency shipment transactions (in and out) to identify large denomination activity as a result of small denomination exchanges.
    - Assess the reasonableness of customer due diligence and EDD information pertaining to the sampled currency originators, shippers, and intermediaries.
    - Determine whether the nature, volume, and frequency of activity are consistent with the expectations associated with the currency originator, shipper, and intermediary. Discuss any inconsistencies identified with bank management. As necessary, obtain and review copies of credit or debit advices, general ledger tickets, and other supporting documentation.
    - Review unusual transactions and customer due diligence information to determine if transactions are potentially suspicious.
    - Discuss preliminary findings and conclusions with bank management.

12. If the currency originator, shipper, or intermediary, or the referral agent who works for the currency originator, shipper, or intermediary has an account with the bank, review a sample of account activity.

13. Based on the examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with the bulk shipment of currency.

U.S. Dollar Drafts - Overview

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

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

Risk Factors

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

Risk Mitigation

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

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

Examination Procedures - U.S. Dollar Drafts

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

1. Review the policies, procedures, and processes related to U.S. dollar drafts. Evaluate the adequacy of the policies, procedures, and processes given the bank's U.S. dollar draft activities and the risks they present. Assess whether the controls are adequate to reasonably protect the

bank from money laundering and terrorist financing. Determine whether policies address the following:

- Criteria for allowing a foreign financial institution or entity to issue the U.S. bank's dollar drafts (e.g., jurisdiction; products, services, and target markets; purpose of account and anticipated activity; customer history; and other available information).
- Identification of unusual transactions (e.g., structuring transactions or the purchase of multiple sequentially numbered U.S. dollar drafts to the same payee).
- Criteria for ceasing U.S. dollar draft issuance through a foreign financial institution or entity.

2. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors higher-risk U.S. dollar draft accounts.

3. Determine whether the bank's system for monitoring U.S. dollar draft accounts for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

4. Obtain a list of foreign bank correspondent accounts in which U.S. dollar drafts are offered. Review the volume, by number and dollar amount, of monthly transactions for each account. Determine whether management has appropriately assessed risk.

Transaction Testing

5. On the basis of the bank's risk assessment of its U.S. dollar draft activities, as well as prior examination and audit reports, select a sample of foreign correspondent bank accounts in which U.S. dollar drafts are processed. In the sample selected, include accounts with a high volume of U.S. dollar draft activity. From the sample selected, perform the following examination procedures:

   - Review transactions for sequentially numbered U.S. dollar drafts to the same payee or from the same remitter. Research any unusual or suspicious U.S. dollar draft transactions.
   - Review the bank's contracts and agreements with foreign correspondent banks. Determine whether contracts address procedures for processing and clearing U.S. dollar drafts.
   - Verify that the bank has obtained and reviewed information about the foreign financial institution's home country AML regulatory requirements (e.g., customer identification and suspicious activity reporting).

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

Payable Through Accounts - Overview

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

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

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

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

Risk Factors

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

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

serious financial losses in criminal and civil fines and penalties, seizure or forfeiture of collateral, and reputation damage.

Risk Mitigation

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

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

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

- Roles and responsibilities of each party.
- Limits or restrictions on transaction types and amounts (e.g., currency deposits, funds transfers, check cashing).
- Restrictions on types of sub-accountholders (e.g., casas de cambio, finance companies, funds remitters, or other nonbank financial institutions).
- Prohibitions or restrictions on multi-tier subaccountholders.
- Access to the foreign financial institution's internal documents and audits that pertain to its PTA activity.
- U.S. banks should consider closing the PTA in the following circumstances:
  - Insufficient information on the ultimate PTA users.
  - Evidence of substantive or ongoing suspicious activity.
  - Inability to ensure that the PTAs are not being used for money laundering or other illicit purposes.

Examination Procedures - Payable Through Accounts

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

1. Review the policies, procedures, and processes related to PTAs. Evaluate the adequacy of the policies, procedures, and processes given the bank's PTA activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. Determine whether:

   - Criteria for opening PTA relationships with a foreign financial institution are adequate. Examples of factors that may be used include: jurisdiction; bank secrecy or money

laundering haven; products, services, and markets; purpose; anticipated activity; customer history; ownership; senior management; certificate of incorporation; banking license; certificate of good standing; and demonstration of the foreign financial institution's operational capability to monitor account activity.
- Appropriate information has been obtained and validated from the foreign financial institution concerning the identity of any persons having authority to direct transactions through the PTA.
- Information and EDD have been obtained from the foreign financial institution concerning the source and beneficial ownership of funds of persons who have authority to direct transactions through the PTA (e.g., name, address, expected activity level, place of employment, description of business, related accounts, identification of foreign politically exposed persons, source of funds, and articles of incorporation).
- Subaccounts are not opened before the U.S. bank has reviewed and approved the customer information.
- Master or subaccounts can be closed if the information provided to the bank has been materially inaccurate or incomplete.
- The bank can identify all signers on each subaccount.

2. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors PTAs.

3. Determine whether the bank's system for monitoring PTAs for suspicious activities, and reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

4. To assess the volume of risk and determine whether adequate resources are allocated to the oversight and monitoring activity, obtain a list of foreign correspondent bank accounts in which PTAs are offered and request MIS reports that show:

   - The number of subaccounts within each PTA.
   - The volume and dollar amount of monthly transactions for each subaccount.

5. Verify that the bank has obtained and reviewed information concerning the foreign financial institution's home country AML regulatory requirements (e.g., customer identification requirements and suspicious activity reporting) and considered these requirements when reviewing PTAs. Determine whether the bank has ensured that subaccount agreements comply with any AML statutory and regulatory requirements existing in the foreign financial institution's home country.

6. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

7. On the basis of the bank's risk assessment of its PTA activities, as well as prior examination and audit reports, select a sample of PTAs. From the sample, review the contracts or agreements with the foreign financial institution. Determine whether the contracts or agreements:

- Clearly outline the contractual responsibilities of both the U.S. bank and the foreign financial institution.
- Define PTA and subaccount opening procedures and require an independent review and approval process when opening the account.
- Require the foreign financial institution to comply with its local AML requirements.
- Restrict subaccounts from being opened by casas de cambio, finance companies, funds remitters, or other nonbank financial institutions.
- Prohibit multi-tier subaccountholders.
- Provide for proper controls over currency deposits and withdrawals by subaccountholders and ensure that CTRs have been appropriately filed.
- Provide for dollar limits on each subaccountholder's transactions that are consistent with expected account activity.
- Contain documentation requirements that are consistent with those used for opening domestic accounts at the U.S. bank.
- Provide the U.S. bank with the ability to review information concerning the identity of subaccountholders (e.g., directly or through a trusted third party).
- Require the foreign financial institution to monitor subaccount activities for unusual or suspicious activity and report findings to the U.S. bank.
- Allow the U.S. bank, as permitted by local laws, to audit the foreign financial institution's PTA operations and to access PTA documents.

8. Review PTA master-account bank statements. (The examiner should determine the time period based upon the size and complexity of the bank.) The statements chosen should include frequent transactions and those of large dollar amounts. Verify the statements to the general ledger and bank reconcilements. Note any currency shipments or deposits made at the U.S. bank on behalf of an individual subaccountholder for credit to the customer's subaccount.

9. From the sample selected, review each subaccountholder's identifying information and related transactions for a period of time as determined by the examiner. Evaluate PTA subaccountholders' transactions. Determine whether the transactions are consistent with expected transactions or warrant further research. (The sample should include subaccountholders with significant dollar activity.)

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

Pouch Activities - Overview

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

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

Increasingly, some banks are using Remote Deposit Capture (RDC) (a deposit transaction delivery system) to replace pouch activities. For additional information on RDC, refer to the expanded overview section on Electronic Banking.

Risk Factors

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

- The instruments were purchased on the same or consecutive days at different locations.
- They are numbered consecutively in amounts just under $3,000 or $10,000.
- The payee lines are left blank or made out to the same person (or to only a few people).
- They contain little or no purchaser information.
- They bear the same stamp, symbol, or initials.
- They are purchased in round denominations or repetitive amounts.
- The depositing of the instruments is followed soon after by a funds transfer out in the same dollar amount.

Risk Mitigation

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

- Outline criteria for opening a pouch relationship with an individual or a foreign financial institution (e.g., customer due diligence requirements, type of institution or person, acceptable purpose of the relationship).
- Detail acceptable and unacceptable transactions (e.g., monetary instruments with blank payees, unsigned monetary instruments, and a large number of consecutively numbered monetary instruments).
- Detail procedures for processing the pouch, including employee responsibilities, dual control, reconciliation and documentation requirements, and employee sign off.
- Detail procedures for reviewing for unusual or suspicious activity, including elevating

concerns to management. (Contents of pouches may be subject to CTR, Report of International Transportation of Currency or Monetary Instruments (CMIR), and SAR reporting requirements.)
- Discuss criteria for closing pouch relationships.

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

Examination Procedures - Pouch Activities

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

1. Determine whether the bank has incoming or outgoing pouch activity and whether the activity is via carrier or courier.

2. Review the policies, procedures, and processes, and any contractual agreements related to pouch activities. Evaluate the adequacy of the policies, procedures, and processes given the bank's pouch activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

3. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors pouch activities.

4. Determine whether the bank's system for monitoring pouch activities for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

5. Review the list of bank customers permitted to use pouch services (incoming and outgoing). Determine whether management has assessed the risk of the customers permitted to use this service.

6. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

7. On the basis of the bank's risk assessment of its pouch activities, as well as prior examination and audit reports, and recent activity records, select a sample of daily pouches for review. Preferably on an unannounced basis and over a period of several days, not necessarily consecutive, observe the pouch opening and the data capture process for items contained in a sample of incoming pouches, and observe the preparation of outgoing pouches. Review the records and the pouch contents for currency, monetary instruments,[196] bearer securities, prepaid cards, gems, art, illegal substances or contraband, or other items that should not ordinarily appear in a bank's pouch.

8. If the courier, or the referral agent who works for the courier, have an account with the bank, review an appropriate sample of their account activity.

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

Electronic Banking - Overview

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with electronic banking (e-banking) customers, including Remote Deposit Capture (RDC) activity, and management's ability to implement effective monitoring and reporting systems.***

E-banking systems, which provide electronic delivery of banking products to customers, include automated teller machine (ATM) transactions; online account opening; Internet banking transactions; and telephone banking. For example, credit cards, deposit accounts, mortgage loans, and funds transfers can all be initiated online, without face-to-face contact.

Management needs to recognize this as a potentially higher-risk area and develop adequate policies, procedures, and processes for customer identification and monitoring for specific areas of banking. Refer to the core examination procedures, "Customer Identification Program" (CIP) for further guidance. Additional information on e-banking is available in the FFIEC Information Technology Examination Handbook.

Risk Factors

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

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

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

Risk Mitigation

Banks should establish BSA/AML monitoring, identification, and reporting for unusual and suspicious activities occurring through e-banking systems. Useful MIS for detecting unusual activity in higher-risk accounts include ATM activity reports, funds transfer reports, new account activity reports, change of Internet address reports, Internet Protocol (IP) address reports, and reports to identify related or linked accounts (e.g., common addresses, phone numbers, e-mail addresses, and taxpayer identification numbers). In determining the level of monitoring required for an account, banks should include how the account was opened as a factor. Banks engaging in transactional Internet banking should have effective and reliable methods to authenticate a customer's identity when opening accounts online and should establish policies for when a customer should be required to open accounts on a face-to-face basis. Banks may also institute other controls, such as establishing transaction dollar limits for large items that require manual

intervention to exceed the preset limit.

Remote Deposit Capture

Remote Deposit Capture (RDC) is a deposit transaction delivery system that has made check and monetary instrument processing (e.g., traveler's checks or money orders) more efficient.

In broad terms, RDC allows a bank's customers to scan a check or monetary instrument, and then transmit the scanned or digitized image to the institution. Scanning and transmission activities occur at remote locations that include the bank's branches, ATMs, domestic and foreign correspondents, and locations owned or controlled by commercial or retail customers.

By eliminating face-to-face transactions, RDC decreases the cost and volume of paper associated with physically mailing or depositing items. RDC also supports new and existing banking products and improves customers' access to their deposits.

On January 14, 2009, the FFIEC published guidance titled, "Risk Management of Remote Deposit Capture." The guidance addresses the essential components of RDC risk management: the identification, assessment, and mitigation of risk. It includes a comprehensive discussion of RDC risk factors and mitigants. Refer to the FFIEC Web site.

Risk Factors

RDC may expose banks to various risks, including money laundering, fraud, and information security. Fraudulent, sequentially numbered, or physically altered documents, particularly money orders and traveler's checks, may be more difficult to detect when submitted by RDC and not inspected by a qualified person. Banks may face challenges in controlling or knowing the location of RDC equipment, because the equipment can be readily transported from one jurisdiction to another. This challenge is increased as foreign correspondents and foreign money services businesses are increasingly using RDC services to replace pouch and certain instrument processing and clearing activities. Inadequate controls could result in intentional or unintentional alterations to deposit item data, resubmission of a data file, or duplicate presentment of checks and images at one or multiple financial institutions. In addition, original deposit items are not typically forwarded to banks, but instead the customer or the customer's service provider retains them. As a result, record keeping, data safety, and integrity issues may increase.

Higher-risk customers may be defined by industry, incidence of fraud, or other criteria. Examples of higher-risk parties include online payment processors, certain credit-repair services, certain mail order and telephone order companies, online gambling operations, businesses located offshore, and adult entertainment businesses.

Risk Mitigation

Management should develop appropriate policies, procedures, and processes to mitigate the risks associated with RDC services and to effectively monitor for unusual or suspicious activity. Examples of risk mitigants include:

- Comprehensively identifying and assessing RDC risk prior to implementation. Senior management should identify BSA/AML, operational, information security, compliance
- legal, and reputation risks. Depending on the bank's size and complexity, this comprehensive risk assessment process should include staff from BSA/AML, information technology and security, deposit operations, treasury or cash management sales, business continuity, audit, compliance, accounting and legal.
- Conducting appropriate customer CDD and EDD.
- Creating risk-based parameters that can be used to conduct RDC customer suitability reviews. Parameters may include a list of acceptable industries, standardized underwriting criteria (e.g., credit history, financial statements, and ownership structure of business), and other risk factors (customer's risk management processes, geographic location, and customer base). When the level of risk warrants, bank staff should consider visiting the customer's physical location as part of the suitability review. During these visits, the customer's operational controls and risk management processes should be evaluated.
- Conducting vendor due diligence when banks use a service provider for RDC activities.
- Management should ensure implementation of sound vendor management processes.
- Obtaining expected account activity from the RDC customer, such as the anticipated RDC transaction volume, dollar volume, and type (e.g., payroll checks, third-party checks, or traveler's checks), comparing it to actual activity, and resolving significant deviations. Comparing expected activity to business type to ensure they are reasonable and consistent.
- Establishing or modifying customer RDC transaction limits.
- Developing well-constructed contracts that clearly identify each party's role, responsibilities, and liabilities, and that detail record-retention procedures for RDC data. These procedures should include physical and logical security expectations for access, transmission, storage, and ultimate disposal of original documents. The contract should also address the customer's responsibility for properly securing RDC equipment and preventing inappropriate use, including establishing effective equipment security controls (e.g., passwords, dual control access). In addition, contracts should detail the RDC customer's obligation to provide original documents to the bank in order to facilitate investigations related to unusual transactions or poor quality transmissions, or to resolve disputes. Contracts should clearly detail the authority of the bank to mandate specific internal controls, conduct audits, or terminate the RDC relationship.
- Implementing additional monitoring or review when significant changes occur in the type or volume of transactions, or when significant changes occur in the underwriting criteria, customer base, customer risk management processes, or geographic location that the bank relied on when establishing RDC services.
- Ensuring that RDC customers receive adequate training. The training should include documentation that addresses issues such as routine operations and procedures, duplicate presentment, and problem resolution.
- Using improved aggregation and monitoring capabilities as facilitated by the digitized data.
- As appropriate, using technology to minimize errors (e.g., the use of franking to stamp or identify a deposit as being processed).

Exam Procedures - Electronic Banking

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with electronic banking (e-banking) customers, including Remote Deposit Capture (RDC) activity, and management's ability to implement effective monitoring and reporting systems.***

1. Review the policies, procedures, and processes related to e-banking, including RDC activity as appropriate. Evaluate the adequacy of the policies, procedures, and processes given the bank's e-banking activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors higher-risk e-banking activities.

3. Determine whether the bank's system for monitoring e-banking, including RDC activity as appropriate, for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

4. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

5. On the basis of the bank's risk assessment of its e-banking activities, as well as prior examination and audit reports, select a sample of e-banking accounts. From the sample selected, perform the following procedures:

    - Review account opening documentation, including CIP, ongoing CDD, and transaction history.
    - Compare expected activity with actual activity.
    - Determine whether the activity is consistent with the nature of the customer's business. Identify any unusual or 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 e-banking relationships.

Funds Transfers - Overview

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

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

Funds Transfer Services

The vast majority of the value of U.S. dollar payments, or transfers, in the United States is ultimately processed through wholesale payment systems, which generally handle large value transactions between banks. Banks conduct these transfers on their own behalf as well as for the benefit of other financial service providers and bank customers, both corporate and consumer.

Related retail transfer systems facilitate transactions such as automated clearing houses (ACH); automated teller machines (ATM); point-of-sales (POS); telephone bill paying; home banking systems; and credit, debit, and prepaid cards. Most of these retail transactions are initiated by customers rather than by banks or corporate users. These individual transactions may then be batched in order to form larger wholesale transfers, which are the focus of this section.

The two primary domestic wholesale payment systems for interbank funds transfers are the Fedwire Funds Service (Fedwire®) and the Clearing House Interbank Payments System (CHIPS). The bulk of the dollar value of these payments is originated electronically to make large value, time-critical payments, such as the settlement of interbank purchases and sales of federal funds, settlement of foreign exchange transactions, disbursement or repayment of loans; settlement of real estate transactions or other financial market transactions; and purchasing, selling, or financing securities transactions. Fedwire and CHIPS participants facilitate these transactions on their behalf and on behalf of their customers, including nonbank financial institutions, commercial businesses, and correspondent banks that do not have direct access.

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

Fedwire

Fedwire is operated by the Federal Reserve Banks and allows a participant to transfer funds from its master account at the Federal Reserve Banks to the master account of any other bank.203 Payment over Fedwire is final and irrevocable when the Federal Reserve Bank either credits the amount of the payment order to the receiving bank's Federal Reserve Bank master account or sends notice to the receiving bank, whichever is earlier. Although there is no settlement risk to Fedwire participants, they may be exposed to other risks, such as errors, omissions, and fraud.

Participants may access Fedwire by three methods:

- Direct mainframe-to-mainframe (Fedline Direct).
- Internet access over a virtual private network to Web-based applications (FedLine Advantage).
- Off-line or telephone-based access to a Federal Reserve Bank operations site.

CHIPS

CHIPS is a privately operated, real-time, multilateral payments system typically used for large-dollar payments. CHIPS is owned by banks, and any banking organization with a regulated U.S. presence may become a participant in the system. Banks use CHIPS for the settlement of both interbank and customer transactions, including, for example, payments associated with commercial transactions, bank loans, and securities transactions. CHIPS also plays a large role in the settlement of USD payments related to international transactions, such as foreign exchange, international commercial transactions, and offshore investments. An entity eligible to maintain a master account at the Federal Reserve is generally eligible to participate in the Fedwire Funds Service. These participants include:

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

Continuous Linked Settlement (CLS) Bank

CLS Bank is a private-sector, special-purpose bank that settles simultaneously both payment obligations that arise from a single foreign exchange transaction. The CLS payment-versus payment settlement model ensures that one payment segment of a foreign exchange transaction is settled if and only if the corresponding payment segment is also settled, eliminating the foreign exchange settlement risk that arises when each segment of the foreign exchange transaction is settled separately. CLS is owned by global financial institutions through shareholdings in CLS Group Holdings AG, a Swiss company that is the ultimate holding company for CLS Bank. CLS Bank currently settles payment instructions for foreign exchange transactions in 17 currencies

and is expected to add more currencies over time.

SWIFT

The SWIFT network is a messaging infrastructure, not a payments system, which provides users with a private international communications link among themselves. The actual funds movements (payments) are completed through correspondent bank relationships, Fedwire, or CHIPS. Movement of payments denominated in different currencies occurs through correspondent bank relationships or over funds transfer systems in the relevant country. In addition to customer and bank funds transfers, SWIFT is used to transmit foreign exchange confirmations, debit and credit entry confirmations, statements, collections, and documentary credits.

Cover Payments

A typical funds transfer involves an originator instructing its bank (the originator's bank) to make payment to the account of a payee (the beneficiary) with the beneficiary's bank. A cover payment occurs when the originator's bank and the beneficiary's bank do not have a relationship that allows them to settle the payment directly. In that case, the originator's bank instructs the beneficiary's bank to effect the payment and advises that transmission of funds to "cover" the obligation created by the payment order has been arranged through correspondent accounts at one or more intermediary banks.

Cross-border cover payments usually involve multiple banks in multiple jurisdictions. For U.S. dollar transactions, the intermediary banks are generally U.S. banks that maintain correspondent banking relationships with non-U.S. originators' banks and beneficiaries' banks. In the past, SWIFT message protocols allowed cross-border cover payments to be effected by the use of separate, simultaneous message formats:

- The MT 103 — payment order from the originator's bank to the beneficiary's bank with information identifying the originator and the beneficiary; and
- The MT 202 — bank-to-bank payment orders directing the intermediary banks to "cover" the originator's bank's obligation to pay the beneficiary's bank.

To address transparency concerns, SWIFT adopted a new message format for cover payments (the MT 202 COV) that contains mandatory fields for originator and beneficiary information. Effective November 21, 2009, the MT 202 COV is required for any bank-to-bank payment for which there is an associated MT 103. The MT 202 COV provides intermediary banks with additional originator and beneficiary information to perform sanctions screening and suspicious activity monitoring. The introduction of the MT 202 COV does not alter a U.S. bank's OFAC or BSA/AML obligations.

The MT 202 format remains available for bank-to-bank funds transfers that have no associated MT 103 message. For additional detail about transparency in cover payments, refer to Transparency and Compliance for U.S. Banking Organizations Conducting Cross-Border Funds Transfers (December 18, 2009), which can be found at each federal banking agencies' Web site.

Informal Value Transfer Systems

An informal value transfer system (IVTS) (e.g., hawalas) is a term used to describe a currency or value transfer system that operates informally to transfer money as a business.

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

IVTS may legally operate in the United States as a Money Services Business, and specifically as a type of money transmitter, so long as they abide by applicable state and federal laws. This includes registering with FinCEN and complying with BSA/AML provisions applicable to all money transmitters. A more sophisticated form of IVTS operating in the United States often interacts with other financial institutions in storing currency, clearing checks, remitting and receiving funds, and obtaining other routine financial services, rather than acting independently of the formal financial system.

Payable Upon Proper Identification Transactions

One type of funds transfer transaction that carries particular risk is the payable upon proper identification (PUPID) service. PUPID transactions are funds transfers for which there is no specific account to deposit the funds into and the beneficiary of the funds is not a bank customer. For example, an individual may transfer funds to a relative or an individual who does not have an account relationship with the bank that receives the funds transfer. In this case, the beneficiary bank may place the incoming funds into a suspense account and ultimately release the funds when the individual provides proof of identity. In some cases, banks permit noncustomers to initiate PUPID transactions. These transactions are considered extremely high risk and require strong controls. Sources of information on IVTS include:

- FinCEN Advisory FIN-2010-A011, Informal Value Transfer Systems, September 2010
- FinCEN Advisory 33, Informal Value Transfer Systems, March 2003.
- U.S. Treasury Informal Value Transfer Systems Report to the Congress in Accordance with Section 359 of the Patriot Act, November 2002.
- Financial Action Task Force on Money Laundering (FATF), Interpretative Note to Special Recommendation VI: Alternative Remittance, June 2003.
- FATF, Combating the Abuse of Alternative Remittance Systems, International Best Practices, October 2002.

Risk Factors

Funds transfers may present a heightened degree of risk, depending on such factors as the number and dollar volume of transactions, geographic location of originators and beneficiaries, and whether the originator or beneficiary is a bank customer. The size and complexity of a bank's operation and the origin and destination of the funds being transferred determine which type of funds transfer system the bank uses. The vast majority of funds transfer instructions are conducted electronically; however, examiners need to be mindful that physical instructions may be transmitted by other informal methods, as described earlier.

Cover payments effected through SWIFT pose additional risks for an intermediary bank that does not receive either a MT 103 or an adequately completed MT 202 COV that identifies the originator and beneficiary of the funds transfer. Without this data, the intermediary bank is unable to monitor or filter payment information. This lack of transparency limits the U.S. intermediary bank's ability to appropriately assess and manage the risk associated with correspondent and clearing operations, monitor for suspicious activity, and screen for OFAC compliance.

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

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

Risk Mitigation

Funds transfers can be used in the placement, layering, and integration stages of money laundering. Funds transfers purchased with currency are an example of the placement stage.

Detecting unusual activity in the layering and integration stages is more difficult for a bank because transactions may appear legitimate. In many cases, a bank may not be involved in the placement of the funds or in the final integration, only the layering of transactions. Banks should consider all three stages of money laundering when evaluating or assessing funds transfer risks.

Banks need to have sound policies, procedures, and processes to manage the BSA/AML risks of its funds transfer activities. Such policies may encompass more than regulatory recordkeeping minimums and be expanded to cover OFAC obligations. Funds transfer policies, procedures, and processes should address all foreign correspondent banking activities, including transactions in which U.S. branches and agencies of foreign banks are intermediaries for their head offices.

Obtaining CDD information is an important risk mitigation step in providing funds transfer services. Because of the nature of funds transfers, adequate and effective CDD policies, procedures, and processes are critical in detecting unusual and suspicious activities. An effective risk-based suspicious activity monitoring and reporting system is equally important.

Whether this monitoring and reporting system is automated or manual, it should be sufficient to detect suspicious trends and patterns typically associated with money laundering. Institutions should have processes for managing correspondent banking relationships in accordance with section 312 of the USA PATRIOT Act and corresponding regulations (31 CFR 1010.610). Correspondent bank due diligence should take into account the correspondent's practices with regard to funds transfers effected through the U.S. bank.

U.S. banks can mitigate risk associated with cover payments by managing correspondent banking relationships, by observing The Clearing House Payments Co., LLC and the Wolfsberg Group's best practices (discussed below) and the SWIFT standards when sending messages, and by conducting appropriate transaction screening and monitoring.

In May 2009, the Basel Committee on Banking Supervision issued a paper on cross-border cover payment messages (BIS Cover Payments Paper).205 The BIS Cover Payments Paper supported increased transparency and encouraged all banks involved in international payments transactions to adhere to the message standards developed by The Clearing House Payments Co., LLC and the Wolfsberg Group in 2007. These are:

- Financial institutions should not omit, delete, or alter information in payment messages or orders for the purpose of avoiding detection of that information by any other financial institution in the payment process;
- Financial institutions should not use any particular payment message for the purpose of avoiding detection of information by any other financial institution in the payment process;
- Subject to all applicable laws, financial institutions should cooperate as fully as practicable with other financial institutions in the payment process when requested to provide information about the parties involved; and
- Financial institutions should strongly encourage their correspondent banks to observe these principles.

In addition, effective monitoring processes for cover payments include:

- Monitoring funds transfers processed through automated systems in order to identify suspicious activity. This monitoring may be conducted after the transfers are processed on an automated basis, and may use a risk-based approach. The MT 202 COV provides intermediary banks with useful information, which can be filtered using risk factors developed by the intermediary bank. The monitoring process may be similar to that for MT 103 payments.
- Given the volume of messages and data for large U.S. intermediary banks, a manual review of every payment order may not be feasible or effective. However, intermediary banks should have, as part of their monitoring processes, a risk-based method to identify incomplete fields or fields with meaningless data. U.S. banks engaged in processing cover payments should have policies to address such circumstances, including those that involve systems other than SWIFT.

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

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

- Identifying disbursement method (i.e., by currency or official check) for proceeds from a beneficiary bank.

Examination Procedures - Funds Transfers

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

1. Review the policies, procedures, and processes related to funds transfers. Evaluate the adequacy of the policies, procedures, and processes given the bank's funds transfer activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. Review MIS and internal risk rating factors, and determine whether the bank effectively identifies and monitors funds transfer activities.

3. Evaluate the bank's risks related to funds transfer activities by analyzing the frequency and dollar volume of funds transfers, jurisdictions, and the bank's role in the funds transfer process (e.g., whether it is the originator's bank, intermediary bank, or beneficiary's bank). These factors should be evaluated in relation to the bank's size, its location, and the nature of its customer and correspondent account relationships.

4. Determine whether an audit trail of funds transfer activities exists. Determine whether an adequate separation of duties or other compensating controls are in place to ensure proper authorization for sending and receiving funds transfers and for correcting postings to accounts.

5. Determine whether the bank's system for monitoring funds transfers and for reporting suspicious activities is adequate given the bank's size, complexity, location, and types of customer relationships. Determine whether suspicious activity monitoring and reporting systems include:

   - Funds transfers purchased with currency.
   - Transactions in which the bank is acting as an intermediary.
   - All SWIFT message formats, including MT 103, MT 202, and MT 202 COV.
   - Transactions in which the bank is originating or receiving funds transfers from foreign financial institutions, particularly to or from jurisdictions with strict privacy and secrecy laws or those identified as higher risk.
   - Frequent currency deposits or funds transfers and then subsequent transfers, particularly to a larger institution or out of the country.

6. Review the bank's procedures for cross-border funds transfers:

   - Determine whether the bank's processes for foreign correspondent bank due diligence, as required under section 312 of the USA PATRIOT Act and corresponding regulations include the review and evaluation of the transparency practices of the bank's

correspondents who are involved in cross-border funds transfers through the bank (for example, whether correspondents are appropriately utilizing the MT 202 COV message format).
- As applicable and if not already performed, review the bank's procedures to ensure compliance with the Travel Rule, including appropriate use of the MT 202 COV format.
- Assess the bank's policies for cooperating with its correspondents when they request the bank to provide information about parties involved in funds transfers.
- Assess the adequacy of the bank's procedures for addressing isolated as well as, repeated instances where payment information received from a correspondent is missing, manifestly meaningless or incomplete, or suspicious.

7. Determine the bank's procedures for payable upon proper identification (PUPID) transactions.

- Beneficiary bank — determine how the bank disburses the proceeds (i.e., by currency or official check).
- Originating bank — determine whether the bank allows PUPID funds transfers for noncustomers. If so, determine the type of funds accepted (i.e., by currency or official check).

8. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

9. On the basis of the bank's risk assessment of funds transfer activities, as well as prior examination and audit reports, select a sample of higher-risk funds transfer activities, which may include the following:

- Funds transfers purchased with currency.
- Transactions in which the bank is acting as an intermediary, such as cover payments.
- Transactions in which the bank is originating or receiving funds transfers from foreign financial institutions, particularly to or from jurisdictions with strict privacy and secrecy laws or those identified as higher risk.
- PUPID transactions.

10. From the sample selected, analyze funds transfers to determine whether the amounts, frequency, and jurisdictions of origin or destination are consistent with the nature of the business or occupation of the customer.

11. In addition, for funds transfers processed using the MT 202 and MT 202 COV message formats, review the sample of messages to determine whether the bank has used the appropriate message formats and has included complete originator and beneficiary information (e.g., no missing or meaningless information).

12. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with funds transfer activity.

Automated Clearing House Transactions - Overview

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with automated clearing house (ACH) and international ACH transactions (IAT) and management's ability to implement effective monitoring and reporting systems.***

The use of the ACH has grown markedly over the last several years due to the increased volume of electronic check conversion and one-time ACH debits, reflecting the lower cost of ACH processing relative to check processing. Check conversion transactions, as well as one-time ACH debits, are primarily low-dollar value, consumer transactions for the purchases of goods and services or the payment of consumer bills. ACH is primarily used for domestic payments, but the Federal Reserve Banks' FedGlobal system can currently accommodate cross-border payments to several countries around the world.

In September 2006, the Office of the Comptroller of the Currency issued guidance titled Automated Clearinghouse Activities — Risk Management Guidance. The document provides guidance on managing the risks of ACH activity. Banks may be exposed to a variety of risks when originating, receiving, or processing ACH transactions, or outsourcing these activities to a third party.

ACH Payment Systems

Traditionally, the ACH system has been used for the direct deposit of payroll and government benefit payments and for the direct payment of mortgages and loans. As noted earlier, the ACH has been expanding to include one-time debits and check conversion. ACH transactions are payment instructions to either credit or debit a deposit account. Examples of credit payment transactions include payroll direct deposit, Social Security, dividends, and interest payments. Examples of debit transactions include mortgage, loan, insurance premium, and a variety of other consumer payments initiated through merchants or businesses.

In general, an ACH transaction is a batch-processed, value-dated, electronic funds transfer between an originating and a receiving bank. An ACH credit transaction is originated by the accountholder sending funds (payer), while an ACH debit transaction is originated by the electronic check conversion process, merchants that receive a check for payment do not collect the check through the check collection system, either electronically or in paper form. Instead, merchants use the information on the check to initiate a type of electronic funds transfer known as an ACH debit to the check writer's account. The check is used to obtain the bank routing number, account number, check serial number, and dollar amount for the transaction, and the check itself is not sent through the check collection system in any form as a payment instrument. Merchants use electronic check conversion because it can be a more efficient way for them to obtain payment than collecting the accountholder receiving funds (payee). Within the ACH system, these participants and usersare known by the following terms:

- Originator. An organization or person that initiates an ACH transaction to an account either as a debit or credit.
- Originating Depository Financial Institution (ODFI). The Originator's depository financial institution that forwards the ACH transaction into the national ACH network through an ACH Operator.
- ACH Operator. An ACH Operator processes all ACH transactions that flow between

different depository financial institutions. An ACH Operator serves as a central clearing facility that receives entries from the ODFIs and distributes the entries to the appropriate Receiving Depository Financial Institution. There are currently two ACH Operators: FedACH and Electronic Payments Network (EPN).

- Receiving Depository Financial Institution (RDFI). The Receiver's depository institution that receives the ACH transaction from the ACH Operators and credits or debits funds from their receivers' accounts.
- Receiver. An organization or person that authorizes the Originator to initiate an ACH transaction, either as a debit or credit to an account.
- Gateway. A financial institution, ACH Operator, or ODFI that acts as an entry or exit point to or from the United States. A formal declaration of status as a Gateway is not required. ACH operators and ODFIs acting in the role of Gateways have specific warranties and obligations related to certain international entries. A financial institution acting as a Gateway generally may process inbound and outbound debit and credit transactions. ACH Operators acting as Gateways may process outbound debit and credit entries, but can limit inbound entries to credit entries only and reversals.

International ACH Payments

NACHA —The Electronic Payments Association (NACHA) issued International ACH Transaction (IAT) operating rules and formats that became effective on September 18, 2009. NACHA has since issued a number of modifications and refinements to their IAT operating rules. The IAT is a Standard Entry Class code for ACH payments that enables financial institutions to identify and monitor international ACH payments, and perform screening to ensure compliance with OFAC requirements. The rules require Gateways to classify payments that are transmitted to or received from a financial agency outside the territorial jurisdiction of the United States as IATs. The classification depends on where the financial agency that handles the payment transaction (movement of funds) is located and not the location of any other party to the transaction (e.g., the Originator or Receiver).

Under NACHA operating rules, all U.S. financial institutions that participate in the ACH Network must be able to utilize the IAT format.

Definition of IAT

An IAT is an ACH entry that is part of a payment transaction involving a financial agency's office that is not located in the territorial jurisdiction of the United States. An office of a financial agency is involved in the payment transaction if one or more of the following conditions are met:

- Holds an account that is credited or debited as part of a payment transaction; or
- Receives funds directly from a person or makes payment directly to a person as part of a payment transaction; or
- Serves as an intermediary in the settlement of any part of a payment transaction.

IAT Defined Terms

An "inbound entry" originates in another country and is transmitted to the United States. For

example, an inbound entry could be a customer's on-line purchase from an overseas vendor. An inbound entry could also be funding for a company payroll. Each subsequent IAT used for direct deposit would be an inbound IAT entry.

An "outbound entry" originates in the United States and is transmitted to another country. For example, IAT pension payments going from a U.S. ODFI to a U.S. RDFI in which the funds are then transferred to an account in another country would be outbound IAT entries.

Payment Transaction Guidance

A payment transaction is:

- An instruction of a sender to a bank to pay, or to obtain payment of, or to cause another bank to pay or to obtain payment of, a fixed or determinate amount of money that is to be paid to, or obtained from, a Receiver, and
- Any and all settlements, accounting entries, or disbursements that are necessary or appropriate to carry out the instruction.

Identification of IAT Parties

The NACHA operating rules define parties as part of an IAT entry:

- Foreign Correspondent Bank: A participating depository financial institution (DFI) that holds deposits owned by other financial institutions and provides payment and other services to those financial institutions.
- Foreign Gateway: A Gateway that acts as an entry point to or exit point from a foreign country.

Information Available Under the IAT Format

Data available to banks under the IAT format may assist banks in their OFAC, anti-money laundering, and monitoring efforts. Originator and receiver information available to banks under the IAT format include:

- Originator name and address.
- Receiver name and address.
- Originator and Receiver account numbers.
- ODFI name (inbound IAT, foreign DFI), identification number, and branch country code.
- RDFI name (outbound IAT, foreign DFI), identification number, and branch country code.
- Country code.
- Currency code.
- Foreign Exchange indicator.

Effective March 14, 2014, a Gateway must identify within an inbound IAT entry:

- The ultimate foreign beneficiary of the funds transfer when the proceeds from a debit inbound IAT entry are "for further credit to" an ultimate foreign beneficiary that is ther

than the Originator of the debit IAT entry, or
- The foreign party funding a credit inbound IAT entry when that party is not the Originator of the credit IAT entry.

Refer to www.nacha.org/c/IATIndustryInformation.cfmfor more information on additional data available to banks under the new IAT format.

Third-Party Service Providers

A third-party service provider (TPSP) is an entity other than an Originator, ODFI, or RDFI that performs any functions on behalf of the Originator, the ODFI, or the RDFI with respect to the processing of ACH entries. For example, a bank may hire a TPSP to conduct ACH activities on behalf of the bank.213 NACHA operating rules define TPSPs and relevant subsets of TPSPs that include "Third-Party Senders" and "Sending Points." A third-party sender is a type of service provider that acts on behalf of an Originator (i.e., an intermediary between the Originator and the ODFI). For example, a third-party sender may be a customer of the bank processing ACH transactions on behalf of an Originator. In a third-party sender arrangement, there is no contractual agreement between the ODFI and the Originator. A sending point is defined as an entity that transmits entries to an ACH Operator on behalf of an ODFI.

The functions of these TPSPs can include, but are not limited to, the creation of ACH files on behalf of the Originator or ODFI, or acting as a sending point of an ODFI (or receiving point on behalf of an RDFI).

Risk Factors

The ACH system was designed to transfer a high volume of low-dollar domestic transactions, which pose lower BSA/AML risks. Nevertheless, the ability to send high-dollar and international transactions through the ACH may expose banks to higher BSA/AML risks.

Banks without a robust BSA/AML monitoring system may be exposed to additional risk particularly when accounts are opened over the Internet without face-to-face contact.

ACH transactions that are originated through a TPSP (that is, when the Originator is not a direct customer of the ODFI) may increase BSA/AML risks, therefore, making it difficult for an ODFI to underwrite and review Originator transactions for compliance with BSA/AML rules. Risks are heightened when neither the TPSP nor the ODFI performs due diligence on the companies for whom they are originating payments.

Certain ACH transactions, such as those originated through the Internet or the telephone, may be susceptible to manipulation and fraudulent use. Certain practices associated with how the banking industry processes ACH transactions may expose banks to BSA/AML risks.

These practices include:

- An ODFI authorizing a TPSP to send ACH files directly to an ACH Operator, in essence bypassing the ODFI.
- ODFIs and RDFIs relying on each other to perform adequate due diligence on their

customers.
- Batch processing that obscures the identities of originators.
- Lack of sharing of information on or about originators and receivers inhibits a bank's ability to appropriately assess and manage the risk associated with correspondent and ACH processing operations, monitor for suspicious activity, and screen for OFAC compliance.

Risk Mitigation

The BSA requires banks to have BSA/AML compliance programs and appropriate policies, procedures, and processes in place to monitor and identify unusual activity, including ACH transactions. Obtaining CDD information in all operations is an important mitigant of BSA/AML risk in ACH transactions. Because of the nature of ACH transactions and the reliance that ODFIs and RDFIs place on each other for OFAC reviews and other necessary due diligence information, it is essential that all parties have a strong CDD program for regular ACH customers. For relationships with TPSPs, CDD on the TPSP can be supplemented with due diligence on the principals associated with the TPSP and, as necessary, on the originators. Adequate and effective CDD policies, procedures, and processes are critical in detecting a pattern of unusual and suspicious activities because the individual ACH transactions are typically not reviewed. Equally important is an effective risk-based suspicious activity monitoring and reporting system. In cases where a bank is heavily reliant upon the TPSP, a bank may want to review the TPSP's suspicious activity monitoring and reporting program, either through its own or an independent inspection.

The ODFI may establish an agreement with the TPSP, which delineates general TPSP guidelines, such as compliance with ACH operating requirements and responsibilities and meeting other applicable state and federal regulations. Banks may need to consider controls to restrict or refuse ACH services to potential originators and receivers engaged in questionable or deceptive business practices. ACH transactions can be used in the layering and integration stages of money laundering.

Detecting unusual activity in the layering and integration stages can be a difficult task, because ACH may be used to legitimize frequent and recurring transactions. Banks should consider the layering and integration stages of money laundering when evaluating or assessing the ACH transaction risks of a particular customer.

The ODFI should be aware of IAT activity and evaluate the activity using a risk-based approach in order to ensure that suspicious activity is identified and monitored. The ODFI, if frequently involved in IATs, may develop a separate process, which may be automated, for reviewing IATs that minimizes disruption to general ACH processing, reconcilement, and settlement.

The potentially higher risk inherent in IATs should be considered in the bank's ACH policies, procedures, and processes. The bank should consider its current and potential roles and responsibilities when developing internal controls to monitor and mitigate the risk associated with IATs and to comply with the bank's suspicious activity reporting obligations.

In processing IATs, banks should consider the following:
- Customers and transactions types and volume.
- Third-party payment processor relationships.

- Responsibilities, obligations, and risks of becoming a Gateway.
- CIP, CDD, and EDD standards and practices.
- Suspicious activity monitoring and reporting.
- Appropriate MIS, including the potential necessity for systems upgrades or changes.
- Processing procedures (e.g., identifying and handling IATs, resolving OFAC hits, and handling noncompliant and rejected messages).
- Training programs for appropriate bank personnel (e.g., ACH personnel, operations, compliance audit, customer service, etc.).
- Legal agreements, including those with customers, third-party processors, and vendors, and whether those agreements need to be upgraded or modified.

OFAC Screening

ACH transactions may involve persons or parties that are subject to the sanctions programs administered by OFAC. (Refer to core overview section, "Office of Foreign Assets Control," for additional guidance.) OFAC has clarified its interpretation of the application of its rules for domestic and cross-border ACH transactions and provided more detailed guidance on cross-border ACH.

With respect to domestic ACH transactions, the 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 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 purpose of compliance with 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 TPSP should assess the nature of 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 screening obligations hold for IATs. 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 sanctions. For outbound IATs, the ODFI should not 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 core overview section, "Office of Foreign Asset Control," for additional guidance.

In guidance issued on March 10, 2009, OFAC authorized institutions in the United States when they are acting as an ODFI/Gateway for inbound IAT debits to reject transactions that appear to involve blockable property or property interests. The guidance further stated that to the extent that an ODFI/Gateway 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/Gateway determines that the transaction does appear to violate OFAC regulations, the ODFI/Gateway 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 payments. Additional information on the types of retail payment systems (ACH payment systems) is available in the FFIEC Information Technology Examination Handbook's Retail Payment Systems booklet.

Examination Procedures - Automated Clearing House Transactions

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with automated clearing house (ACH) and international ACH transactions (IAT) and management's ability to implement effective monitoring and reporting systems.***

1. Review the policies, procedures, and processes related to ACH transactions, including IATs. Evaluate the adequacy of the policies, procedures, and processes given the bank's ACH transactions, including IATs, and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. From review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors higher-risk customers using ACH transactions, including IATs.

3. Evaluate the bank's risks related to ACH transactions, including IATs, by analyzing the frequency and dollar volume and types of ACH transactions in relation to the bank's size, its location, the nature of its customer account relationships, and the location of the origin or destination of IATs relative to the bank's location.

4. Determine whether the bank's system for monitoring customers, including third-party service providers (TPSP), using ACH transactions and IATs for suspicious activities, and for reporting of suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. Determine whether internal control systems include:

   - Identifying customers with frequent and large ACH transactions or IATs.
   - Monitoring ACH detail activity when the batch-processed transactions are separated for other purposes (e.g., processing errors).
   - As appropriate, identifying and applying increased due diligence to higher-risk customers who originate or receive IATs, particularly when a party to the transaction is located in a higher-risk geographic location.

- Using methods to track, review, and investigate customer complaints or unauthorized returns regarding possible fraudulent or duplicate ACH transactions, including IATs.

5. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

6. On the basis of the bank's risk assessment of customers with ACH transactions as well as prior examination and audit reports, select a sample of higher-risk customers, including TPSPs, with ACH transactions or IATs, which may include the following:

   - Customers initiating ACH transactions, including IATs, from the Internet or via telephone, particularly from an account opened on the Internet or via the telephone without face-to-face interaction.
   - Customers whose business or occupation does not warrant the volume or nature of ACH or IAT activity.
   - Customers who have been involved in the origination or receipt of duplicate or fraudulent ACH transactions or IATs.
   - Customers or originators (clients of customers) that are generating a high rate or high volume of invalid account returns, consumer unauthorized returns, or other unauthorized transactions.

7. From the sample selected, analyze ACH transactions, including IATs, to determine whether the amounts, frequency, and jurisdictions of origin or destination are consistent with the nature of the business or occupation of the customer. A review of the account opening documentation, including CIP documentation, may be necessary in making these determinations. Identify any suspicious or unusual activity.

8. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with ACH transactions and IATs.

Prepaid Access - Overview

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with prepaid access products, and management's ability to implement effective monitoring and reporting systems.***

Prepaid access is defined as access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number or personal identification number.

Banks often rely on multiple third parties to accomplish the design, implementation, and maintenance of their prepaid access programs. These third parties may include program managers, distributors, marketers, merchants, and processors. Some banks that offer prepaid access products do so as the issuing bank. In addition to issuing prepaid access, banks may participate in other aspects of a prepaid program such as marketing and distributing products issued by another financial institution. FinCEN regulations define certain non-bank providers and sellers of prepaid access as money services businesses (MSBs).

Prepaid access can be issued in an electronic or physical form and linked to funds held in a pooled account. Consumers use both electronic and physical prepaid products to access funds held by banks in pooled accounts that are linked to subaccounts.

The growth of prepaid access as a financial tool continues to flourish. While prepaid cards are the most well-known and popular products used by consumers at this time, prepaid access products are continuing to evolve. This section is intended to address prepaid card relationships as well as other types of prepaid access. Guidance on risk factors and risk mitigation for prepaid cards is based on current practice and is not intended to exclude other types of prepaid access.

Prepaid Cards

Prepaid access can cover a variety of products, functionalities, and technologies. Physical access, issued in the form of prepaid cards, is currently the most popular form and is widely used for payments by governments, businesses and consumers. Most payment networks require that their branded prepaid cards be issued by a bank that is a member of that payment network. Prepaid cards operate within either an "open" or "closed" loop system. Open loop prepaid cards can be used for purchases at any merchant that accepts cards issued for use on the payment network associated with the card and to access cash at any automated teller machine (ATM) that connects to the affiliated ATM network. Examples of open loop prepaid cards include payroll cards, general purpose reloadable (GPR) cards, and certain gift cards. Some prepaid cards may be reloaded, allowing the cardholder or other person (such as an employer) to add value. Closed loop prepaid cards generally can only be used to buy goods or services from the merchant issuing the card or a select group of merchants or service providers that participate in a specific network. Examples of closed loop prepaid cards include merchant-specific retail gift cards, mall cards, and mass transit system cards.

Closed loop prepaid cards generally do not allow for cash access, although they can often be resold through third-party Web sites in exchange for other closed loop cards or payment via check, ACH or other method.

Prepaid cards are highly flexible and can be customized to meet the needs of the specific program. Some prepaid card programs are designed for specific limited-use purposes, such as flexible spending account (FSA) or health savings account (HSA) cards that can be used to purchase specific health-related services. Some prepaid card programs are used by state and federal government agencies to disburse government benefits (e.g., disability, unemployment, etc.) or provide income tax refunds, or by employers to deliver wage and salary payments.

Like debit cards, prepaid cards provide a compact and transportable way to maintain and access funds. Consumers use prepaid cards in a variety of ways, such as purchasing products, making transfers to other cardholders within the prepaid program, and paying bills.

They also offer individuals an alternative to cash and money orders. As an alternate method of cross-border funds transmittal, a small number of prepaid card programs may issue multiple cards per account, so that persons in another country or jurisdiction can access the funds loaded by the original cardholder via ATM withdrawals of cash or merchant purchases.

For such programs, risk-based customer due diligence should be conducted on the original cardholder and transactions should be subjected to risk-based monitoring.

Prepaid Access Participants

Prepaid access programs often rely on multiple third parties to accomplish the design, implementation, and maintenance of their programs. Within a prepaid access program, these parties are known by the following terms:

- Program Manager. Runs the program's day-to-day operations. This entity may or may not also be the entity that creates the program and designs the features and characteristics of the prepaid product. May be a provider of prepaid access (Money Services Business (MSB)) under FinCEN's rule.
- Network. Any of the payment networks that clear, settle, and process transactions.
- Distributor. An organization that markets and distributes prepaid products.
- Provider of Prepaid Access. A participant within a prepaid program that agrees to serve as the principal conduit for access to information from its fellow program participants. The provider must register with FinCEN as an MSB and identify each prepaid program for which it is the provider of prepaid access. As an MSB, providers of prepaid access are subject to certain BSA/AML responsibilities. A bank that serves as a provider of prepaid access has no requirement to register with FinCEN.
- Payment Processor. The entity that tracks and manages transactions and may be responsible for account set-up and activation; adding value to products; and fraud control and reporting.
- Issuing Bank. A bank that offers network branded prepaid products to consumers and may serve as the holder of funds that have been prepaid and are awaiting instructions to be disbursed.
- Seller or Retailer. A convenience store, drugstore, supermarket, or location where a consumer can buy a prepaid product.

Contractual Agreements

Each relationship that a U.S. bank has with another financial institution or third party as part of a prepaid access program should be governed by an agreement or a contract describing each party's responsibilities and other relationship details, such as the products and services provided. The agreement or contract should also consider each party's BSA/AML and OFAC compliance requirements, customer base, due diligence procedures, and any payment network obligations. The issuing bank maintains ultimate responsibility for BSA/AML compliance whether or not a contractual agreement has been established.

Risk Factors

As with other payment instruments, money laundering, terrorist financing, and other criminal activity may occur through prepaid access and prepaid card programs if effective controls are not in place. For example, law enforcement investigations have found that some prepaid holders have used false identification and funded their initial loads with stolen credit cards, or have purchased multiple prepaid cards under aliases. In the placement phase of money laundering, because many domestic and offshore banks offer prepaid access products or services with currency access through ATMs internationally, criminals may load cash from illicit sources onto prepaid access products and send them to accomplices inside or outside the United States. Generally, domestically issued prepaid cards can only be loaded in the United States. Investigations have disclosed that both open and closed loop prepaid cards have been used in conjunction with, or as a replacement to, bulk cash smuggling. Although prepaid access is increasingly regulated and is issued by highly regulated banks, some third parties involved in marketing or distributing prepaid access programs may or may not be subject to regulatory requirements, oversight, and supervision. In addition, these requirements may vary by party.

Prepaid access programs are extremely diverse in the range of products and services offered and the customer bases they serve. In evaluating the risk profile of a prepaid access program, banks should consider the program's specific features and functionalities. Higher potential money laundering risk associated with prepaid access would result if the holder is anonymous, or if the holder or purchaser provides fictitious holder/purchaser information.

Higher risk is also associated with cash access (especially internationally), and the volume and velocity of funds that can be loaded or transacted. Other risk factors include type and frequency of loads and transactions, geographic location where the transaction activity occurs, the relationships between the bank and parties associated with the program, value limits, distribution channels, and the nature of funding sources. Transactions using prepaid access may pose the following unique risks to the bank:

- Funds may be transferred to or from an unknown third party.
- Verification of cardholder identity may be done entirely remotely, relying on third-party program managers, processors or distributors.
- As with other modes of electronic payments (e.g., ACH, wire transfer, credit and debit cards), holders may be able to use prepaid access products internationally, thus avoiding border restrictions and reporting requirements applicable to cash and monetary instruments.
- Transactions may be credited or debited to the user's payment product immediately, although there may be a lag in delivery of funds to the issuing bank, creating a load timing

risk for the bank (also referred to as a "funds in flight" risk).
- Specific holder activity may be difficult to determine by reviewing activity through a pooled account.
- Data in underlying pooled accounts may be held or managed by third parties, separate from the issuing bank.
- Marketing of payment products, customer service, and onboarding of new customers (both consumer and business customers) may be handled primarily by third parties separate from the issuing bank.
- The customer may perceive the transactions as less transparent.
- Source of payroll funding may come through an intermediary bank and may not be transparent.

Risk Mitigation

Banks that offer prepaid access or otherwise participate in prepaid access programs should have policies, procedures, and processes sufficient to manage the related BSA/AML risks as required under the BSA and implementing regulations, as well as under payment network rules. Guidance provided by the Network Branded Prepaid Card Association is an additional resource for banks that provide prepaid card services.

BSA/AML risk mitigation is an important factor for prepaid access programs, involving several key components:

- Conducting appropriate due diligence on any third-party service provider.
- Conducting a risk assessment of the prepaid access product itself including product features and how it is distributed and loaded.
- Monitoring transactions conducted or attempted by, at or through the bank for unusual or suspicious activity.
- Product features and limits on usage.

Third-Party Service Providers

A bank's Customer Due Diligence (CDD) program should provide for a risk assessment of all third parties involved in offering, managing, distributing, processing, or otherwise implementing the prepaid access program, considering all relevant factors, including, as appropriate:

- A review of such party's BSA/AML compliance program.
- Systems integrity and BSA/AML monitoring capabilities.
- The policies on outsourcing should include processes for (1) documenting in writing the roles and responsibilities of the parties, (2) maintaining the confidentiality of customer information, and (3) maintaining the necessary access to information. The policies should include the right to audit the third party to monitor its performance.
- The BSA/AML and OFAC obligations of third parties.
- On-site audits.
- Corporate documentation, licenses, references (including independent reporting services), and, if appropriate, documentation on principal owners.
- An understanding of the third party's overall compliance culture.

Product Features and Distribution

Product features can provide important mitigation to the BSA/AML risks inherent in prepaid access and prepaid card relationships and transactions and may include:

- Limits or prohibitions on cash loads, access, or redemption, particularly where holder information is not on file.
- Limits or prohibitions on amounts of loads and number of loads/reloads within a specific time frame (load velocity limits).
- Controls on the number of cards purchased by one individual or the number of cards that can access the same card account.
- Controls on the ability to transfer or co-mingle funds.
- Maximum dollar thresholds on ATM withdrawals and on the number of withdrawals within a specific time frame (ATM velocity limits).
- Maximum dollar thresholds on Point of Sale (POS) transactions for individuals and transactions within a preset time period (i.e., daily or monthly); and on the number of withdrawals within a specific time frame (POS velocity limits).
- Limits or prohibitions on certain usage (e.g., merchant type) and on geographic usage, such as outside the United States.
- The ability to reverse transactions.
- Limits on aggregate card values.

Other features that mitigate risks in this area include:

- The identity and location of all third parties involved in selling or distributing the prepaid access program, including any subagents.
- The type, purpose, and anticipated activity of the prepaid access program.

Customers/Prepaid Users

Customer due diligence regarding the purchaser and/or the user(s) of the prepaid product can also be important BSA/AML risk mitigant and may include:

- Whether the source of funds is known and trusted (such as corporate or government loads, vs. loads by individuals).
- The nature of the third parties' businesses and the markets and customer bases served.
- The information collected to identify and verify the holders' identity.
- The nature and duration of the bank's relationship with third parties who are the source of funds in the prepaid access program.
- The company requesting payroll funding and the source of payroll funding.
- The ability to monitor and track loads, transactions and velocity.

As part of their system of internal controls, banks should establish a means for monitoring, identifying, and reporting suspicious activity related to prepaid access programs. This reporting obligation extends to all transactions by, at, or through the bank, including those in an aggregated form. Banks may need to establish protocols to regularly obtain transaction information from processors or other third parties. Monitoring systems should have the ability to identify foreign activity, bulk purchases made by one individual, and multiple purchases made by related parties. In addition, procedures should include monitoring for unusual activity patterns, such as:

- cash loads followed immediately by withdrawals of the full amount from another location, or
- multiple unrelated funds transfers onto the prepaid access product, such as in tax refund fraud situations where multiple tax refunds are loaded onto one card.

Various management information system reports (MIS) may be useful for detecting unusual activity on higher-risk accounts. Those reports include ATM activity reports (focusing on foreign transactions), funds transfer reports, new account activity reports, change of Internet address reports, Internet Protocol (IP) address reports, and reports to identify related or linked accounts (e.g., common addresses, phone numbers, e-mail addresses, and taxpayer identification numbers).

Examination Procedures - Prepaid Access

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with prepaid access, and management's ability to implement effective monitoring and reporting systems.***

1. Review the policies, procedures, and processes related to prepaid access. Evaluate the risks posed by the prepaid access products offered, and the adequacy of the policies, procedures, and processes given the risks such prepaid access products present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. Review the due diligence undertaken by the bank regarding third-party service providers such as program managers, processors, marketers, merchants and distributors. Assess whether existing onboarding and ongoing oversight programs are reasonably satisfactory to protect the bank.

3. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors higher-risk prepaid access transactions, such as transactions involving unknown sources of funds (as opposed to funds received from a long-term commercial customer or federal, state or local government entity) as well as transactions involving international cash access/ATM transactions (as opposed to domestic merchandise-only transactions).

4. Determine whether the bank's prepaid access program is governed by an agreement or a contract describing each party's responsibilities and other relationship details, such as the products and services provided. At a minimum, the contract should consider each party's:

   - BSA/AML and OFAC compliance requirements;
   - customer base;
   - due diligence procedures; and
   - network obligations.

5. Determine whether the bank's system for monitoring prepaid access transactions for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, customer profile, and types of prepaid access products offered.

6. If appropriate, refer to the core examination procedures, " Office of Foreign Assets Control"; "Third Party Payment Processors," and " Nonbank Financial Institutions," for guidance.

Transaction Testing

7. On the basis of the bank's risk assessment of its prepaid access activities, as well as prior examination and audit reports, select a sample of prepaid access transactions. From the sample selected perform the following examination procedures:

   - Review the prepaid access product configuration(s), including features, how it is distributed, source of funds, and what BSA/AML risk mitigants apply.
   - Review account opening documentation, including CIP, ongoing CDD, and transaction history.
   - Compare expected activity with actual activity.
   - Determine whether the activity is consistent with the nature of the prepaid access product, known sources of funds, and knowledge of the user's identity.
   - Identify any unusual or suspicious activity.

8. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with prepaid access relationships.

Third-Party Payment Processors - Overview

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

Nonbank or third-party payment processors (processors) are bank customers that provide payment-processing services to merchants and other business entities. Traditionally, processors contracted primarily with retailers that had physical locations in order to process the retailers' transactions. These merchant transactions primarily included credit card payments but also covered automated clearing house (ACH) transactions, remotely created checks (RCC), and debit and prepaid cards transactions. With the expansion of the Internet, retail borders have been eliminated. Processors now provide services to a variety of merchant accounts, including conventional retail and Internet-based establishments, prepaid travel, telemarketers, and Internet gaming enterprises.

Third-party payment processors often use their commercial bank accounts to conduct payment processing for their merchant clients. For example, the processor may deposit into its account RCCs generated on behalf of a merchant client, or process ACH transactions on behalf of a merchant client. In either case, the bank does not have a direct relationship with the merchant. The increased use of RCCs by processor customers also raises the risk of fraudulent payments being processed through the processor's bank account. The Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), and Financial Crimes Enforcement Network (FinCEN) have issued guidance regarding the risks, including the BSA/AML risks, associated with banking third-party processors.

Risk Factors

Processors generally are not subject to BSA/AML regulatory requirements. As a result, some processors may be vulnerable to money laundering, identity theft, fraud schemes, or other illicit transactions, including those prohibited by OFAC.

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

While payment processors generally affect legitimate payment transactions for reputable merchants, the risk profile of such entities can vary significantly depending on the make-up of their customer base. Banks with third-party payment processor customers should be aware of the heightened risk of returns and use of services by higher-risk merchants. Some higher risk merchants routinely use third parties to process their transactions because they do not have a direct bank relationship. Payment processors pose greater money laundering and fraud risk if they do not have an effective means of verifying their merchant clients' identities and business practices. Risks are heightened when the processor does not perform adequate due diligence on the merchants for which they are originating payments.

Risk Mitigation

Banks offering account services to processors should develop and maintain adequate policies, procedures, and processes to address risks related to these relationships. At a minimum, these policies should authenticate the processor's business operations and assess their risk level. A bank may assess the risks associated with payment processors by considering the following:

- Implementing a policy that requires an initial background check of the processor (using, for example, the Federal Trade Commission Web site, Better Business Bureau, Nationwide Multi-State Licensing System & Registry (NMLS), NACHA, state incorporation departments, Internet searches, and other investigative processes), its principal owners, and of the processor's underlying merchants, on a risk-adjusted basis in order to verify their creditworthiness and general business practices.
- Reviewing the processor's promotional materials, including its Web site, to determine the target clientele. A bank may develop policies, procedures, and processes that restrict the types of entities for which it allows processing services. These restrictions should be clearly communicated to the processor at account opening.
- Determining whether the processor re-sells its services to a third party who may be referred to as an "agent or provider of Independent Sales Organization (ISO) opportunities" or "gateway" arrangements.
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of its due diligence standards for new merchants.
- Requiring the processor to identify its major customers by providing information such as the merchant's name, principal business activity, geographic location, and transaction volume.
- Verifying directly, or through the processor, that the merchant is operating a legitimate business by comparing the merchant's identifying information against public record databases, and fraud and bank check databases.
- Reviewing corporate documentation including independent reporting services and, if applicable, documentation on principal owners.
- Visiting the processor's business operations center.
- Reviewing appropriate databases to ensure that the processor and its principal owners and operators have not been subject to law enforcement actions.

Banks that provide account services to third-party payment processors should monitor their processor relationships for any significant changes in the processor's business strategies that may affect their risk profile. Banks should periodically re-verify and update the processors' profiles to ensure the risk assessment is appropriate. Banks should ensure that their contractual agreements with payment processors provide them with access to necessary information in a timely manner. Banks should periodically audit their third-party payment processing relationships; including reviewing merchant client lists and confirming that the processor is fulfilling contractual obligations to verify the legitimacy of its merchant clients and their business practices.

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

- Merchant base.

- Merchant activities.
- Average dollar volume and number of transactions.
- "Swiping" versus "keying" volume for credit card transactions.
- Charge-back history, including rates of return for ACH debit transactions and RCCs.
- Consumer complaints or other documentation that suggest a payment processor's merchant clients are inappropriately obtaining personal account information and using it to create unauthorized RCCs or ACH debits.

With respect to account monitoring, a bank should thoroughly investigate high levels of returns and should not accept high levels of returns on the basis that the processor has provided collateral or other security to the bank. High levels of RCCs or ACH debits returned for insufficient funds or as unauthorized can be an indication of fraud or suspicious activity. Therefore, return rate monitoring should not be limited to only unauthorized transactions, but include returns for other reasons that may warrant further review, such as unusually high rates of return for insufficient funds or other administrative reasons.

Transactions should be monitored for patterns that may be indicative of attempts to evade NACHA limitations on returned entries. For example, resubmitting a transaction under a different name or for slightly modified dollar amounts can be an attempt to circumvent these limitations and are violations of the NACHA Rules.

A bank should implement appropriate policies, procedures, and processes that address compliance and fraud risks. Policies and procedures should outline the bank's thresholds for returns and establish processes to mitigate risk from payment processors, as well as possible actions that can be taken against the payment processors that exceed these standards.

If the bank determines a SAR is warranted, FinCEN has requested banks check the appropriate box on the SAR report to indicate the type of suspicious activity, and include the term "payment processor," in both the narrative and the subject occupation portions of the SAR.

Examination Procedures - Third-Party Payment Processors

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

1. Review the policies, procedures, and processes related to third-party payment processors (processors). Evaluate the adequacy of the policies, procedures, and processes given the bank's processor activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors processor relationships, particularly those that pose a higher risk for money laundering.

3. Determine whether the bank's system for monitoring processor accounts for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

4. If appropriate, refer to the core examination procedures, " Office of Foreign Assets Control," for guidance.

Transaction Testing

5. On the basis of the bank's risk assessment of its processor activities, as well as prior examination and audit reports, select a sample of higher-risk processor accounts. From the sample selected:

   - Review account opening documentation and ongoing due diligence information.
   - Review account statements and, as necessary, specific transaction details to determine how expected transactions compare with actual activity.
   - Determine whether actual activity is consistent with the nature of the processor's stated activity.
   - Assess the controls concerning identification of high rates of returns and the process in place to address compliance and fraud risks.
   - Identify any unusual or 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 processor accounts.

Purchase and Sale of Monetary Instruments — Overview

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

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

Risk Factors

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

Risk Mitigation

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

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

Examination Procedures - Purchase and Sale of Monetary Instruments

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

1. Review the policies, procedures, and processes related to the sale of monetary instruments. Evaluate the adequacy of the policies, procedures, and processes given the bank's monetary

instruments activities and the risks they present. Assess whether controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. From the volume of sales and the number of locations where monetary instruments are sold, determine whether the bank appropriately manages the risks associated with monetary instrument sales.

3. Determine whether the bank's system for monitoring monetary instruments for suspicious activities, and for reporting suspicious activities, is adequate given the bank's volume of monetary instrument sales, size, complexity, location, and types of customer relationships. Determine whether suspicious activity monitoring and reporting systems (either manual or automated) include a review of:

   - Sales of sequentially numbered monetary instruments from the same or different purchasers on the same day to the same payee.
   - Sales of monetary instruments to the same purchaser or sales of monetary instruments to different purchasers made payable to the same remitter.
   - Monetary instrument purchases by noncustomers.
   - Common purchasers, payees, addresses, sequentially numbered purchases, and unusual symbols.

4. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

5. On the basis of the bank's risk assessment, as well as prior examination and audit reports, select a sample of monetary instrument transactions for both customers and noncustomers from:

   - Monetary instrument sales records.
   - Copies of cleared monetary instruments purchased with currency.

6. From the sample selected, analyze transaction information to determine whether amounts, the frequency of purchases, and payees are consistent with expected activity for customers or noncustomers (e.g., payments to utilities or household purchases). Identify any suspicious or unusual activity.

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

Brokered Deposits - Overview

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

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

Deposit brokers provide intermediary services for banks and investors. This activity is considered higher risk because each deposit broker operates under its own guidelines for obtaining deposits. The level of regulatory oversight over deposit brokers varies, as does the applicability of BSA/AML requirements directly on the deposit broker. However, the deposit broker is subject to OFAC requirements regardless of its regulatory status.

Consequently, the deposit broker may not be performing adequate customer due diligence or OFAC screening. For additional information refer to the core overview section, "Office of Foreign Assets Control," or "Customer Identification Program" core examination procedures. The bank accepting brokered deposits depends on the deposit broker to sufficiently perform required account opening procedures and to follow applicable BSA/AML compliance program requirements.

Risk Factors

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

Risk Mitigation

Banks that accept deposit broker accounts or funds should develop appropriate policies, procedures, and processes that establish minimum CDD procedures for all deposit brokers providing deposits to the bank. The level of due diligence a bank performs should be commensurate with its knowledge of the deposit broker and the deposit broker's known business practices and customer base.

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

- Determine whether the deposit broker is a legitimate business in all operating locations where the business is conducted.
- Review the deposit broker's business strategies, including customer markets (e.g., foreign or domestic customers) and methods for soliciting clients.

- Determine whether the deposit broker is subject to regulatory oversight.
- Evaluate whether the deposit broker's BSA/AML and OFAC policies, procedures, and processes are adequate (e.g., ascertain whether the deposit broker performs sufficient CDD including CIP procedures).
- Determine whether the deposit broker screens clients for OFAC matches.
- Evaluate the adequacy of the deposit broker's BSA/AML and OFAC audits and ensure that they address compliance with applicable regulations and requirements.
- Banks should take particular care in their oversight of deposit brokers who are not regulated entities and:
  - Are unknown to the bank.
  - Conduct business or obtain deposits primarily in other jurisdictions.
  - Use unknown or hard-to-contact businesses and banks for references.
  - Provide other services that may be suspect, such as creating shell companies for foreign clients.
  - Refuse to provide requested audit and due diligence information or insist on placing deposits before providing this information.
  - Use technology that provides anonymity to customers.

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

Brokered Deposits

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

1. Review the policies, procedures, and processes related to deposit broker relationships. Evaluate the adequacy of the policies, procedures, and processes given the bank's deposit broker activities and the risks that they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors deposit broker relationships, particularly those that pose a higher risk for money laundering.

3. Determine whether the bank's system for monitoring deposit broker relationships for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

4. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

5. On the basis of the bank's risk assessment of its brokered deposit activities, as well as prior examination and audit reports, select a sample of higher-risk deposit broker accounts. When selecting a sample, examiners should consider the following:

   - New relationships with deposit brokers.
   - The method of generating funds (e.g., Internet brokers).
   - Types of customers (e.g., nonresident or offshore customers, politically exposed persons, or foreign shell banks).
   - A deposit broker that has appeared in the bank's SARs.
   - Subpoenas served on the bank for a particular deposit broker.
   - Foreign funds providers.
   - Unusual activity.

6. Review the customer due diligence information on the deposit broker. For deposit brokers who are considered higher risk (e.g., they solicit foreign funds, market via the Internet, or are independent brokers), assess whether the following information is available:

   - Background and references.
   - Business and marketing methods.
   - Client-acceptance and due diligence practices.
   - The method for or basis of the broker's compensation or bonus program.
   - The broker's source of funds.
   - Anticipated activity or transaction types and levels (e.g., funds transfers).

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

Privately Owned Automated Teller Machines - Overview

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

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

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

Sponsoring Bank

Some electronic funds transfers (EFT) or point-of-sale (POS) networks require an ISO to be sponsored by a member of the network (sponsoring bank). The sponsoring bank and the ISO are subject to all network rules. The sponsoring bank is also charged with ensuring the ISO abides by all network rules. Therefore, the sponsoring bank should conduct proper due diligence on the ISO and maintain adequate documentation to ensure that the sponsored ISO complies with all network rules.

Risk Factors

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

Due diligence becomes more of a challenge when ISOs sell ATMs to, or subcontract with, other companies (sub-ISOs) whose existence may be unknown to the sponsoring bank.

When an ISO contracts with or sells ATMs to sub-ISOs, the sponsoring bank may not know who actually owns the ATM. Accordingly, sub-ISOs may own and operate ATMs that remain

virtually invisible to the sponsoring bank.

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

Money laundering can occur through privately owned ATMs when an ATM is replenished with illicit currency that is subsequently withdrawn by legitimate customers. This process results in ACH deposits to the ISO's account that appear as legitimate business transactions.

Consequently, all three phases of money laundering (placement, layering, and integration) can occur simultaneously. Money launderers may also collude with merchants and previously legitimate ISOs to provide illicit currency to the ATMs at a discount.

Risk Mitigation

Banks should implement appropriate policies, procedures, and processes, including appropriate due diligence and suspicious activity monitoring, to address risks with ISO customers. At a minimum, these policies, procedures, and processes should include:

- Appropriate risk-based due diligence on the ISO, through a review of corporate documentation, licenses, permits, contracts, or references.
- Review of public databases to identify potential problems or concerns with the ISO or principal owners.
- Understanding the ISO's controls for currency servicing arrangements for privately owned ATMs, including source of replenishment currency.
- Documentation of the locations of privately owned ATMs and determination of the ISO's target geographic market.
- Expected account activity, including currency withdrawals.

Because of these risks, ISO due diligence beyond the minimum CIP requirements is important. Banks should also perform due diligence on ATM owners and sub-ISOs, as appropriate. This due diligence may include:

- Reviewing corporate documentation, licenses, permits, contracts, or references, including the ATM transaction provider contract.
- Reviewing public databases for information on the ATM owners.
- Obtaining the addresses of all ATM locations, ascertaining the types of businesses in which the ATMs are located, and identifying targeted demographics.
- Determining expected ATM activity levels, including currency withdrawals.
- Ascertaining the sources of currency for the ATMs by reviewing copies of armored car contracts, lending arrangements, or any other documentation, as appropriate.
- Obtaining information from the ISO regarding due diligence on its sub-ISO arrangements, such as the number and location of the ATMs, transaction volume, dollar volume, and source of replenishment currency.

Examination Procedures - Privately Owned Automated Teller Machines

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

1. Review the policies, procedures, and processes related to privately owned ATM accounts. Evaluate the adequacy of the policies, procedures, and processes given the bank's privately owned ATM and ISO relationships and the risk they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors privately owned ATM accounts.

3. Determine whether the bank's system for monitoring privately owned ATM accounts for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

4. Determine whether the bank sponsors network membership for ISOs. If the bank is a sponsoring bank, review contractual agreements with networks and the ISOs to determine whether due diligence procedures and controls are designed to ensure that ISOs are in compliance with network rules.

5. Determine whether the bank obtains information from the ISO regarding due diligence on its sub-ISO arrangements.

Transaction Testing

6. On the basis of the bank's risk assessment of its privately owned ATM and ISO relationships, as well as prior examination and audit reports, select a sample of privately owned ATM accounts. From the sample selected, perform the following examination procedures:

    - Review the bank's CDD information. Determine whether the information adequately verifies the ISO's identity and describes its:
        - Background.
        - Source of funds.
        - Anticipated activity or transaction types and levels (e.g., funds transfers).
        - ATMs (size and location).
        - Currency delivery arrangement, if applicable.
    - Review any MIS reports the bank uses to monitor ISO accounts. Determine whether the flow of funds or expected activity is consistent with the CDD information.

7. Determine whether a sponsored ISO uses third-party providers or servicers to load currency, maintain ATMs, or solicit merchant locations. If yes, review a sample of third-party service agreements for proper due diligence and control procedures.

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

Non-Deposit Investment Products - Overview

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

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

Networking Arrangements

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

Co-Branded Products

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

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

Dual-Employee Arrangements

In a dual-employee arrangement, the bank and the financial services corporation such as an insurance agency or a registered broker/dealer have a common (shared) employee. The shared employee may conduct banking business as well as sell NDIP, or sell NDIP full-time.

Because of this dual-employee arrangement, the bank retains responsibility over NDIP activities. Even if contractual agreements establish the financial services corporation as being responsible for BSA/AML, the bank needs to ensure proper oversight of its employees, including

dual employees, and their compliance with all regulatory requirements.

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

Third-Party Arrangements

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

In-House Sales and Proprietary Products

Unlike networking arrangements, the bank is fully responsible for in-house NDIP transactions completed on behalf of its customers, either with or without the benefit of an internal broker/dealer employee.234 In addition, the bank may also offer its own proprietary NDIPs, which can be created and offered by the bank, its subsidiary, or an affiliate.

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

Risk Factors

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

Risk Mitigation

Management should develop risk-based policies, procedures, and processes that enable the bank to identify unusual account relationships and circumstances, questionable assets and sources of funds, and other potential areas of risk (e.g., offshore accounts, agency accounts, and

unidentified beneficiaries). Management should be alert to situations that need additional review or research.

Networking Arrangements

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

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

Bank management should make reasonable efforts to update due diligence information on the broker/dealer. Such efforts may include a periodic review of information on the broker/dealer's compliance with its BSA/AML responsibilities, verification of the broker/dealer's record in meeting testing requirements, and a review of consumer complaints.

Bank management is also encouraged, when possible, to review BSA/AML reports generated by the broker/dealer. This review could include information on account openings, transactions, investment products sold, and suspicious activity monitoring and reporting.

In-House Sales and Proprietary Products

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

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

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

- Bank is entering into a relationship with a new customer.
- Nondiscretionary accounts have a large asset size or frequent transactions.

- Customer resides in a foreign jurisdiction.
- Customer is a PIC or other corporate structure established in a higher-risk jurisdiction.
- Assets or transactions are atypical for the customer.
- Investment type, size, assets, or transactions are atypical for the bank.
- International funds transfers are conducted, particularly from offshore funding sources.
- The identities of the principals or beneficiaries in investments or relationships are unknown or cannot be easily determined.
- Politically exposed persons (PEP) are parties to any investments or transactions.

Examination Procedures - Nondeposit Investment Products

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

1. Review the policies, procedures, and processes related to NDIP. Evaluate the adequacy of the policies, procedures, and processes given the bank's NDIP activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. If applicable, review contractual arrangements with financial service providers. Determine the BSA/AML compliance responsibility of each party. Determine whether these arrangements provide for adequate BSA/AML oversight.

3. Determine from a review of MIS reports (e.g., exception reports, funds transfer reports, and activity monitoring reports) and internal risk rating factors, whether the bank effectively identifies and monitors NDIP, particularly those that pose a higher risk for money laundering.

4. Determine how the bank includes NDIP sales activities in its bank-wide or, if applicable, firm-wide BSA/AML aggregation systems.

5. Determine whether the bank's system for monitoring NDIP and for reporting suspicious activities is adequate given the bank's size, complexity, location, and types of customer relationships.

6. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control" for guidance.

Transaction Testing

If the bank or its majority-owned subsidiary is responsible for the sale or direct monitoring of NDIP, then examiners should perform the following transaction testing procedures on customer accounts established by the bank.

7. On the basis of the bank's risk assessment of its NDIP activities, as well as prior examination and audit reports, select a sample of higher risk NDIP. From the sample selected, perform the following examination procedures:

   - Review appropriate documentation, including CIP, to ensure that adequate due diligence has been performed and appropriate records are maintained.
   - Review account statements and, as necessary, specific transaction details for:
     - Expected transactions with actual activity.
     - Holdings in excess of the customer's net worth.
     - Irregular trading patterns (e.g., incoming funds transfers to purchase securities followed by delivery of securities to another custodian shortly thereafter).
   - Determine whether actual activity is consistent with the nature of the customer's business and the stated purpose of the account. Identify any unusual or suspicious activity.

8. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with NDIP sales activities.

Insurance - Overview

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with the sale of covered insurance products, and management's ability to implement effective monitoring and reporting systems.***

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

AML Compliance Programs and Suspicious Activity Reporting

Requirements for Insurance Companies

FinCEN regulations impose AML compliance program requirements and SAR obligations on insurance companies similar to those that apply to banks. The insurance regulations apply only to insurance companies; there are no independent obligations for brokers and agents.

However, the insurance company is responsible for the conduct and effectiveness of its AML compliance program, which includes agent and broker activities. The insurance regulations only apply to a limited range of products that may pose a higher risk of abuse by money launderers and terrorist financiers. A covered product, for the purposes of an AML compliance program, includes:

- A permanent life insurance policy, other than a group life insurance policy.
- Any annuity contract, other than a group annuity contract.
- Any other insurance product with features of cash value or investment.

When an insurance agent or broker already is required to establish a BSA/AML compliance program under a separate requirement under BSA regulations (e.g., bank or securities broker requirements), the insurance company generally may rely on that compliance program to address issues at the time of sale of the covered product. However, the bank may need to establish specific policies, procedures, and processes for its insurance sales in order to submit information to the insurance company for the insurance company's AML compliance.

Likewise, if a bank, as an agent of the insurance company, detects unusual or suspicious activity relating to insurance sales, it can file a joint SAR on the common activity with the insurance company.

In April 2008, FinCEN published a strategic analytical report that provides information regarding certain money laundering trends, patterns, and typologies in connection with insurance products. Refer to *Insurance Industry Suspicious Activity Reporting: An Assessment of Suspicious Activity Report Filings* on the FinCEN Web site.

Risk Factors

Insurance products can be used to facilitate money laundering. For example, currency can be used to purchase one or more life insurance policies, which may subsequently be quickly canceled by a policyholder (also known as "early surrender") for a penalty. The insurance company refunds the money to the purchaser in the form of a check. Insurance policies without cash value or investment features are lower risk, but can be used to launder money or finance terrorism through the submission by a policyholder of inflated or false claims to its insurance carrier, which if paid, would enable the insured to recover a part or all of the originally invested payments. Other ways insurance products can be used to launder money include:

- Borrowing against the cash surrender value of permanent life insurance policies.
- Selling units in investment-linked products (such as annuities).
- Using insurance proceeds from an early policy surrender to purchase other financial assets.
- Buying policies that allow the transfer of beneficial interests without the knowledge and consent of the issuer (e.g., secondhand endowment and bearer insurance policies).
- Purchasing insurance products through unusual methods such as currency or currency equivalents.
- Buying products with insurance termination features without concern for the product's investment performance.

Risk Mitigation

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

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

Examination Procedures - Insurance

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with the sale of covered insurance products, and management's ability to implement effective monitoring and reporting systems.***

1. Review the policies, procedures, and processes related to insurance sales. Evaluate the adequacy of the policies, procedures, and processes given the bank's insurance sales activities, its role in insurance sales, and the risks the insurance sales present. Assess whether the

controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. Review the contracts and agreements for the bank's networking arrangements with affiliates, operating subsidiaries, or other third-party insurance providers conducting sales activities on bank premises on behalf of the bank.

3. Depending on the bank's responsibilities as set forth in the contracts and agreements, review MIS reports (e.g., large transaction reports, single premium payments, early policy cancellation records, premium overpayments, and assignments of claims) and internal risk rating factors. Determine whether the bank effectively identifies and monitors covered insurance product sales.

4. Depending on the bank's responsibilities as set forth in the contracts and agreements, determine whether the bank's system for monitoring covered insurance products for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

5. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

If the bank or its majority-owned subsidiary is responsible for the sale or direct monitoring of insurance, then examiners should perform the following transaction testing procedures.

6. On the basis of the bank's risk assessment of its insurance sales activities, as well as prior examination and audit reports, select a sample of covered insurance products. From the sample selected, perform the following examination procedures:

   - Review account opening documentation and ongoing due diligence information.
   - Review account activity. Compare anticipated transactions with actual transactions.
   - Determine whether activity is unusual or suspicious.

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

Concentration Accounts - Overview

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

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

Risk Factors

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

Risk Mitigation

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

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

- Maintaining a comprehensive system that identifies, bank-wide, the general ledger accounts used as concentration accounts, as well as the departments and individuals authorized to use those accounts.
- Requiring dual signatures on general ledger tickets.
- Prohibiting direct customer access to concentration accounts.
- Capturing customer transactions in the customer's account statements.
- Prohibiting customer's knowledge of concentration accounts or their ability to direct employees to conduct transactions through the accounts.
- Retaining appropriate transaction and customer identifying information.
- Frequent reconciling of the accounts by an individual who is independent from the transactions.
- Establishing timely discrepancy resolution process.
- Identifying recurring customer names.

Examination Procedures - Concentration Accounts

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

1. Review the policies, procedures, and processes related to concentration accounts. Evaluate the adequacy of the policies, procedures, and processes in relation to the bank's concentration account activities and the risks they represent. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors concentration accounts.

3. Review the general ledger and identify any concentration accounts. After discussing concentration accounts with management and conducting any additional research needed, obtain and review a list of all concentration accounts and the bank's most recent reconcilements.

4. Determine whether the bank's system for monitoring concentration accounts for suspicious activities, and for reporting of suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

5. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

6. On the basis of the bank's risk assessment of its concentration accounts, as well as prior examination and audit reports, select a sample of concentration accounts. From the sample selected, perform the following examination procedures:

   - Obtain account activity reports for selected concentration accounts.
   - Evaluate the activity and select a sample of transactions passing through different concentration accounts for further review.
   - Focus on higher-risk activity (e.g., funds transfers or monetary instruments purchases) and transactions from higher-risk jurisdictions.

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

Lending Activities - Overview

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

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

Risk Factors

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

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

Risk Mitigation

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

The bank should have policies, procedures, and processes to monitor, identify, and report unusual and suspicious activities. The sophistication of the systems used to monitor lending account activity should conform to the size and complexity of the bank's lending business.

For example, the bank can review loan reports such as early payoffs, past dues, fraud, or cash-secured loans.

Examination Procedures - Lending Activities

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

1. Review the policies, procedures, and processes related to lending activities. Evaluate the adequacy of the policies, procedures, and processes given the bank's lending activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors high-risk loan accounts.

3. Determine whether the bank's system for monitoring loan accounts for suspicious activities and for reporting of suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

4. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

5. On the basis of the bank's risk assessment of its lending activities, as well as prior examination and audit reports, select a sample of higher-risk loan accounts. From the sample selected, perform the following examination procedures:

   - Review account opening documentation, including CIP, to ensure that adequate due diligence has been performed and that appropriate records are maintained.
   - Review, as necessary, loan history.
   - Compare expected transactions with actual activity.
   - Determine whether actual activity is consistent with the nature of the customer's business and the stated purpose of the loan. Identify any unusual or 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 lending relationships.

Trade Finance Activities - Overview

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

Trade finance typically involves short-term financing to facilitate the import and export of goods. These operations can involve payment if documentary requirements are met (e.g., letter of credit), or may instead involve payment if the original obligor defaults on the commercial terms of the transactions (e.g., guarantees or standby letters of credit). In both cases, a bank's involvement in trade finance minimizes payment risk to importers and exporters. The nature of trade finance activities, however, requires the active involvement of multiple parties on both sides of the transaction. In addition to the basic exporter or importer relationship at the center of any particular trade activity, relationships may exist between the exporter and its suppliers and between the importer and its customers.

Both the exporter and importer may also have other banking relationships. Furthermore, many other intermediary financial and nonfinancial institutions may provide conduits and services to expedite the underlying documents and payment flows associated with trade transactions. Banks can participate in trade financing by, among other things, providing pre-export financing, helping in the collection process, confirming or issuing letters of credit, discounting drafts and acceptances, or offering fee-based services such as providing credit and country information on buyers. Although most trade financing is short-term and self-liquidating in nature, medium-term loans (one to five years) or long-term loans (more than five years) may be used to finance the import and export of capital goods such as machinery and equipment.

In transactions that are covered by letters of credit, participants can take the following roles:

- Applicant. The buyer or party who requests the issuance of a letter of credit.
- Issuing Bank. The bank that issues the letter of credit on behalf of the Applicant and advises it to the Beneficiary either directly or through an Advising Bank. The Applicant is the Issuing Bank's customer.
- Confirming Bank. Typically in the home country of the Beneficiary, at the request of the Issuing Bank, the bank that adds its commitment to honor draws made by the Beneficiary, provided the terms and conditions of the letter of credit are met.
- Advising Bank. The bank that advises the credit at the request of the Issuing Bank. The Issuing Bank sends the original credit to the Advising Bank for forwarding to the Beneficiary. The Advising Bank authenticates the credit and advises it to the Beneficiary. There may be more than one Advising Bank in a letter of credit transaction. The Advising Bank may also be a Confirming Bank.
- Beneficiary. The seller or party to whom the letter of credit is addressed.
- Negotiation. The purchase by the nominated bank of drafts (drawn on a bank other than the nominated bank) or documents under a complying presentation, by advancing or agreeing to advance funds to the beneficiary on or before the banking day on which reimbursement is due to the nominated bank.
- Nominated Bank. The bank with which the credit is available or any bank in the case of a credit available with any bank.
- Accepting Bank. The bank that accepts a draft, providing a draft is called for by the credit. Drafts are drawn on the Accepting Bank that dates and signs the instrument.

- Discounting Bank. The bank that discounts a draft for the Beneficiary after it has been accepted by an Accepting Bank. The Discounting Bank is often the Accepting Bank.
- Reimbursing Bank. The bank authorized by the Issuing Bank to reimburse the Paying Bank submitting claims under the letter of credit.
- Paying Bank. The bank that makes payment to the Beneficiary of the letter of credit.
- As an example, in a letter of credit arrangement, a bank can serve as the Issuing Bank, allowing its customer (the buyer) to purchase goods locally or internationally, or the bank can act as an Advising Bank, enabling its customer (the exporter) to sell its goods locally or internationally. The relationship between any two banks may vary and could include any of the roles listed above.

Risk Factors

The international trade system is subject to a wide range of risks and vulnerabilities that provide criminal organizations with the opportunity to launder the proceeds of crime and move funds to terrorist organizations with a relatively low risk of detection. The involvement of multiple parties on both sides of any international trade transaction can make the process of due diligence more difficult. Also, because trade finance can be more document-based than other banking activities, it can be susceptible to documentary fraud, which can be linked to money laundering, terrorist financing, or the circumvention of OFAC sanctions or other restrictions (such as export prohibitions, licensing requirements, or controls).

While banks should be alert to transactions involving higher-risk goods (e.g., trade in weapons or nuclear equipment), they need to be aware that goods may be over- or undervalued in an effort to evade anti-money laundering or customs regulations, or to move funds or value across national borders. For example, an importer may pay a large sum of money from the proceeds of an illegal activity for goods that are essentially worthless and are subsequently discarded. Alternatively, trade documents, such as invoices, may be fraudulently altered to hide the scheme. Variations on this theme include inaccurate or double invoicing, partial shipment of goods (short shipping), and the use of fictitious goods.

Illegal proceeds transferred in such transactions thereby appear sanitized and enter the realm of legitimate commerce. Moreover, many suspect trade finance transactions also involve collusion between buyers and sellers.

The Applicant's true identity or ownership may be disguised by the use of certain corporate forms, such as shell companies or offshore front companies. The use of these types of entities results in a lack of transparency, effectively hiding the identity of the purchasing party, and thus increasing the risk of money laundering and terrorist financing.

Risk Mitigation

Sound CDD procedures are needed to gain a thorough understanding of the customer's underlying business and locations served. The banks in the letter of credit process need to undertake varying degrees of due diligence depending upon their role in the transaction. For example, Issuing Banks should conduct sufficient due diligence on a prospective customer before establishing the letter of credit. The due diligence should include gathering sufficient information on Applicants and Beneficiaries, including their identities, nature of business, and sources of

funding. This may require the use of background checks or investigations, particularly in higher-risk jurisdictions. As such, banks should conduct a thorough review and reasonably know their customers prior to facilitating trade-related activity and should have a thorough understanding of trade finance documentation. Refer to the core overview section, "Customer Due Diligence," for additional guidance.

Likewise, guidance provided by the Financial Action Task Force on Money Laundering (FATF) has helped set important industry standards and is a resource for banks that provide trade finance services. The Wolfsberg Group also has published suggested industry standards and guidance for banks that provide trade finance services.

Banks taking other roles in the letter of credit process should complete due diligence that is commensurate with their roles in each transaction. Banks need to be aware that because of the frequency of transactions in which multiple banks are involved, Issuing Banks may not always have correspondent relationships with the Advising or Confirming Bank.

To the extent feasible, banks should review documentation, not only for compliance with the terms of the letter of credit, but also for anomalies or red flags that could indicate unusual or suspicious activity. Reliable documentation is critical in identifying potentially suspicious activity. When analyzing trade transactions for unusual or suspicious activity, banks should consider obtaining copies of official U.S. or foreign government import and export forms to assess the reliability of documentation provided. These anomalies could appear in shipping documentation, obvious under- or over-invoicing, government licenses (when required), or discrepancies in the description of goods on various documents. Identification of these elements may not, in itself, require the filing of a SAR, but may suggest the need for further research and verification. In circumstances where a SAR is warranted, the bank is not expected to stop trade or discontinue processing the transaction. However, stopping the trade may be required to avoid a potential violation of an OFAC sanction.

Trade finance transactions frequently use Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages. U.S. banks must comply with OFAC regulations, and when necessary, licensing in advance of funding. Banks should monitor the names of the parties contained in these messages and compare the names against OFAC lists. Refer to overview section, "Office of Foreign Assets Control," for guidance. Banks with a high volume of SWIFT messages should determine whether their monitoring efforts are adequate to detect suspicious activity, particularly if the monitoring mechanism is not automated. Refer to core overview section "Suspicious Activity Reporting," and expanded overview section, "Funds Transfers," for additional guidance.

Policies, procedures, and processes should also require a thorough review of all applicable trade documentation (e.g., customs declarations, trade documents, invoices, etc.) to enable the bank to monitor and report unusual and suspicious activity, based on the role played by the bank in the letter of credit process. The sophistication of the documentation review process and MIS should be commensurate with the size and complexity of the bank's trade finance portfolio and its role in the letter of credit process. In addition to OFAC filtering, the monitoring process should give greater scrutiny to:

- Items shipped that are inconsistent with the nature of the customer's business (e.g., a steel company that starts dealing in paper products, or an information technology company that starts dealing in bulk pharmaceuticals).

- Customers conducting business in higher-risk jurisdictions.
- Customers shipping items through higher-risk jurisdictions, including transit through non-cooperative countries.
- Customers involved in potentially higher-risk activities, including activities that may be subject to export/import restrictions (e.g., equipment for military or police organizations of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials, precious gems, or certain natural resources such as metals, ore, and crude oil).
- Obvious over- or under-pricing of goods and services.
- Obvious misrepresentation of quantity or type of goods imported or exported.
- Transaction structures that appear unnecessarily complex and designed to obscure the true nature of the transaction.
- Customer directs payment of proceeds to an unrelated third party.
- Shipment locations or description of goods not consistent with letter of credit.
- Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment. Any changes in the names of parties also should prompt additional OFAC review.

On February 18, 2010, FinCEN issued an advisory to inform and assist the financial industry in reporting instances of suspected trade-based money laundering (TBML). The advisory contains examples of "red flags" based on activity reported in SARs that FinCEN and law enforcement believe may indicate trade-based money laundering. In order to assist law enforcement in its effort to target TBML and black market peso exchange (BMPE) activities,

FinCEN requested in the advisory that financial institutions check the appropriate box in Part II, Suspicious Activity Information section of the SAR and include the abbreviation TBML or BMPE in the narrative section of the SAR. The advisory can be found on the FinCEN Web site.

Unless customer behavior or transaction documentation appears unusual, the bank should not be expected to spend undue time or effort reviewing all information. The examples above, particularly for an Issuing Bank, may be included as part of its routine CDD process. Banks with robust CDD programs may find that less focus is needed on individual transactions as a result of their comprehensive knowledge of the customer's activities.

Examination Procedures - Trade Finance Activities

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

1. Review the policies, procedures, and processes related to trade finance activities. Evaluate the adequacy of the policies, procedures, and processes governing trade finance-related activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. Evaluate the adequacy of the due diligence information the bank obtains for the customer's files. Determine whether the bank has processes in place for obtaining information at account opening, in addition to ensuring current customer information is maintained.

3. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors the trade finance portfolio for suspicious or unusual activities, particularly those that pose a higher risk for money laundering.

4. Determine whether the bank's system for monitoring trade finance activities for suspicious activities, and for reporting of suspicious activities, is adequate, given the bank's size, complexity, location, and types of customer relationships.

5. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

6. On the basis of the bank's risk assessment of its trade finance portfolio, as well as prior examination and audit reports, select a sample of trade finance accounts. From the sample selected, review customer due diligence documentation to determine whether the information is commensurate with the customer's risk. Identify any unusual or suspicious activities.

7. Verify whether the bank monitors the trade finance portfolio for potential OFAC violations and unusual transactional patterns and conducts and records the results of any due diligence.

8. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with trade finance activities.

Private Banking - Overview

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

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

U.S. banks may manage private banking relationships for both domestic and international customers. Typically, thresholds of private banking service are based on the amount of assets under management and on the need for specific products or services (e.g., real estate management, closely held company oversight, money management). The fees charged are ordinarily based on asset thresholds and the use of specific products and services. Private banking arrangements are typically structured to have a central point of contact (i.e., relationship manager) that acts as a liaison between the client and the bank and facilitates the client's use of the bank's financial services and products. Appendix N ("Private Banking - Common Structure") provides an example of a typical private banking structure and illustrates the relationship between the client and the relationship manager. Typical products and services offered in a private banking relationship include:

- Cash management (e.g., checking accounts, overdraft privileges, cash sweeps, and bill paying services).
- Funds transfers.
- Asset management (e.g., trust, investment advisory, investment management, and custodial and brokerage services).
- The facilitation of shell companies and offshore entities (e.g., Private Investment Companies (PIC), international business corporations (IBC), and trusts).
- Lending services (e.g., mortgage loans, credit cards, personal loans, and letters of credit).
- Financial planning services including tax and estate planning.
- Custody services.
- Other services as requested (e.g., mail services).

Privacy and confidentiality are important elements of private banking relationships.

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

Risk Factors

Private banking services can be vulnerable to money laundering schemes, and past money laundering prosecutions have demonstrated that vulnerability. The 1999 Permanent Subcommittee on Investigations' Report "Private Banking and Money Laundering: A Case Study

of Opportunities and Vulnerabilities"248 outlined, in part, the following vulnerabilities to money laundering:

- Private bankers as client advocates.
- Powerful clients including politically exposed persons (PEPs), industrialists, and entertainers.
- Culture of confidentiality and the use of secrecy jurisdictions or shell companies.
- Private banking culture of lax internal controls.
- Competitive nature of the business.
- Significant profit potential for the bank.

Risk Mitigation

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

Customer Risk Assessment

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

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

nature of this relationship and the risks involved.

Customer Due Diligence

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

For purposes of the CIP, the bank is not required to search the private banking account to verify the identities of beneficiaries, but instead is only required to verify the identity of the named accountholder. However, the CIP rule also provides that, based on the bank's risk assessment of a new account opened by a customer that is not an individual (e.g., private banking accounts opened for a PIC), the bank may need "to obtain information about" individuals with authority or control over such an account, including signatories, in order to verify the customer's identity and to determine whether the account is maintained for non-U.S. persons.

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

- Purpose of the account.
- Type of products and services to be used.
- Anticipated account activity.
- Description and history of the source of the client's wealth.
- Client's estimated net worth, including financial statements.
- Current source of funds for the account.
- References or other information to confirm the reputation of the client.

Bearer Shares

Some shell companies issue bearer shares (i.e., ownership is vested via bearer shares, which allows ownership of the corporation to be conveyed by simply transferring physical possession of the shares). Risk mitigation of shell companies that issue bearer shares may include maintaining control of the bearer shares, entrusting the shares with a reliable independent third party, or requiring periodic certification of ownership. Banks should assess the risks these relationships pose and determine the appropriate controls. For example, in most cases banks should choose to maintain (or have an independent third party maintain) bearer shares for customers. In rare cases involving lower-risk, well-known, longtime customers, banks may find that periodically re-certifying beneficial ownership is effective. A strong CDD program is an effecttive underlying control through which banks can determine the nature, purpose, and expected use of shell companies and apply appropriate monitoring and documentation standards.

Convertible Shares

Certain jurisdictions also allow for registered shares to be converted to bearer shares. These types of entities also carry the same type of risk as bearer shares, primarily centered on the lack of transparency regarding the potential transfer of ownership or control of those shares.

Risk mitigation for relationships belonging to corporate entities with a convertibility option is essentially the same as traditional bearer shares. Financial institutions should assess the risk posed by these relationships and implement appropriate and ongoing beneficial ownership certifications, establish prudent measures as necessary to restrict conversion to bearer share form without prior notification from the customer or require control of the shares by a reliable independent third party.

Board of Directors and Senior Management Oversight

The board of directors' and senior management's active oversight of private banking activities and the creation of an appropriate corporate oversight culture are crucial elements of a sound risk management and control environment. The purpose and objectives of the organization's private banking activities should be clearly identified and communicated by the board and senior management. Well-developed goals and objectives should describe the target client base in terms of minimum net worth, investable assets, and types of products and services sought. Goals and objectives should also specifically describe the types of clients the bank does and does not accept and should establish appropriate levels of authorization for new-client acceptance. Board and senior management should also be actively involved in establishing control and risk management goals for private banking activities, including effective audit and compliance reviews. Each bank should ensure that its policies, procedures, and processes for conducting private banking activities are evaluated and updated regularly and ensure that roles, responsibilities, and accountability are clearly delineated.

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

Given the sensitive nature of private banking and the potential liability associated with it, banks should thoroughly investigate the background of newly hired private banking relationship managers. During the course of employment, any indications of inappropriate activities should be promptly investigated by the bank.

Additionally, when private banking relationship managers change employers, their customers often move with them. Banks bear the same potential liability for the existing customers of newly hired officers as they do for any new, private banking relationship. Therefore, those accounts should be promptly reviewed using the bank's procedures for establishing new account relationships.

MIS and reports are also important in effectively supervising and managing private banking relationships and risks. Board and senior management should review relationship manager

compensation reports, budget or target comparison reports, and applicable risk management reports. Private banker MIS reports should enable the relationship manager to view and manage the whole client and any related client relationships.

Examination Procedures - Private Banking

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

1. Review the policies, procedures, and processes related to private banking activities. Evaluate the adequacy of the policies, procedures, and processes given the bank's private banking activities and the risks they represent. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. From a review of MIS reports (e.g., customer aggregation, policy exception and missing documentation, customer risk classification, unusual accounts activity, and client concentrations) and internal risk rating factors, determine whether the bank effectively identifies and monitors private banking relationships, particularly those that pose a higher risk for money laundering.

3. Determine whether the bank's system for monitoring private banking relationships for suspicious activities, and for reporting of suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

4. Review the private banking compensation program. Determine whether it includes qualitative measures that are provided to employees to comply with account opening and suspicious activity monitoring and reporting requirements.

5. Review the monitoring program the bank uses to oversee the private banking relationship manager's personal financial condition and to detect any inappropriate activities.

6. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control" for guidance.

Transaction Testing

7. On the basis of the bank's risk assessment of its private banking activities, as well as prior examination and audit reports, select a sample of private banking accounts. The sample should include the following types of accounts:

   - Politically exposed persons (PEP).
   - Private investment companies (PIC), international business corporations (IBC), and shell companies.

- Offshore entities.
- Cash-intensive businesses.
- Import or export companies.
- Customers from or doing business in a higher-risk geographic location.
- Customers listed on unusual activity monitoring reports.
- Customers who have large dollar transactions and frequent funds transfers.

8. From the sample selected, perform the following examination procedures:

   - Review account opening documentation and ongoing due diligence information.
   - Review account statements and, as necessary, specific transaction details.
   - Compare expected transactions with actual activity.
   - Determine whether actual activity is consistent with the nature of the customer's business.
   - Identify any unusual or suspicious activity.

9. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with private banking relationships.

Trust and Asset Management Services - Overview

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

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

Unlike trust arrangements, agency accounts are established by contract and governed by contract law. Assets are held under the terms of the contract, and legal title or ownership does not transfer to the bank as agent. Agency accounts include custody, escrow, investment management, and safekeeping relationships. Agency products and services may be offered in a traditional trust department or through other bank departments.

Customer Identification Program

CIP rules, which became effective October 1, 2003, apply to substantially all bank accounts opened after that date. The CIP rule defines an "account" to include cash management, safekeeping, custodian, and trust relationships. The definition of account in the CIP rule does not include an account for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974 (ERISA).

In the case of employee benefit plan accounts that are subject to ERISA that are established as trusts, the bank's customer is the employee benefit plan trust established by the employer to hold the assets of the employee benefit plan. Such plans often have individual participant or beneficiary accounts. For purposes of the CIP rule, a participant in or beneficiary of such an account is not be deemed to be the bank's "customer," as such a person has not initiated the relationship with the bank. The account is not be considered opened by the employee even if a subaccount is maintained in the employee's name, or the employee is able to contribute assets into the account, so long as the employee contribution is limited to rolling over assets from another plan, elective salary deferral contributions, purchasing securities or Asset management accounts can be trust or agency accounts and are managed by the bank.

For employee benefit plan accounts that are not subject to ERISA such as employee benefit plan accounts established by government entities, the bank's customer is the employer that contracts with the bank to establish the account. By contrast, where an *individual* opens an individual retirement account in a bank, the individual who opens the account is the bank's "customer."

For purposes of the CIP, the bank is not required to search the trust, escrow, or similar accounts to verify the identities of beneficiaries, but instead is only required to verify the identity of the named accountholder (the trust). In the case of a trust account, the customer is the trust whether or not the bank is the trustee for the trust. However, the CIP rule also provides that, based on the bank's risk assessment of a new account opened by a customer that is not an

individual, the bank may need "to obtain information about" individuals with authority or control over such an account, including signatories, in order to verify the customer's identity.259 For example, in certain circumstances involving revocable trusts, the bank may need to gather information about the settlor, grantor, trustee, or other persons with the authority to direct the trustee, and who thus have authority or control over the account, in order to establish the true identity of the customer.

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

Risk Factors

Trust and asset management accounts, including agency relationships, present BSA/AML concerns similar to those of deposit taking, lending, and other traditional banking activities.

Concerns are primarily due to the unique relationship structures involved when the bank handles trust and agency activities, such as:

- Personal and court-supervised accounts.
- Trust accounts formed in the private banking department.
- Asset management and investment advisory accounts.
- Global and domestic custody accounts.
- Securities lending.
- Employee benefit and retirement accounts.
- Corporate trust accounts.
- Transfer agent accounts.
- Other related business lines.

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

Risk Mitigation

Management should develop policies, procedures, and processes that enable the bank to identify unusual account relationships and circumstances, questionable assets and sources of assets, and other potential areas of risk (e.g., offshore accounts, PICs, asset protection trusts (APT),262 agency accounts, and unidentified beneficiaries). While the majority of traditional trust and asset management accounts do not need EDD, management should be alert to those situations that need additional review or research.

Customer Comparison Against Lists

The bank must maintain required CIP information and complete the required one-time check of trust account names against section 314(a) search requests. The bank should also be able to identify customers who may be politically exposed persons (PEP), doing business with or located in a jurisdiction designated as "primary money laundering concern" under section 311 of the USA PATRIOT Act, or match OFAC lists. As a sound practice, the bank should also determine the identity of other parties that may have control over the account, such as grantors or co-trustees. Refer to the core overview section, "Information Sharing,"

Circumstances Warranting Enhanced Due Diligence

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

- Type of trust or agency account and its size.
- Types and frequency of transactions.
- Country of residence of the principals or beneficiaries, or the country where established, or source of funds.
- Accounts and transactions that are not usual and customary for the customer or for the bank.
- Stringent documentation, verification, and transaction monitoring procedures should be established for accounts that management considers as higher risk. Typically, employee benefit accounts and court-supervised accounts are among the lowest BSA/AML risks.

The following are examples of situations in which EDD may be appropriate:

- Bank is entering into a relationship with a new customer.
- Account principals or beneficiaries reside in a foreign jurisdiction, or the trust or its funding mechanisms are established offshore.
- Assets or transactions are atypical for the type and character of the customer.
- Account type, size, assets, or transactions are atypical for the bank.
- International funds transfers are conducted, particularly through offshore funding sources.
- Accounts are funded with easily transportable assets such as gemstones, precious metals, coins, artwork, rare stamps, or negotiable instruments.
- Accounts or relationships are maintained in which the identities of the principals, or beneficiaries, or sources of funds are unknown or cannot easily be determined.
- Accounts benefit charitable organizations or other nongovernmental organizations (NGO) that may be used as a conduit for illegal activities.264

- Interest on lawyers' trust accounts (IOLTA) holding and processing significant dollar amounts.
- Account assets that include PICs.
- PEPs are parties to any accounts or transactions.

Examination Procedures - Trust and Asset Management Services

Objective. ***Assess the adequacy of the bank's policies, procedures, processes, and systems to manage the risks associated with trust and asset management[265] services, and management's ability to implement effective due diligence, monitoring, and reporting systems.***

If this is a standalone trust examination, refer to the core examination procedures, "Scoping and Planning," for comprehensive guidance on the BSA/AML examination scope. In such instances, the trust examination may need to cover additional areas, including training, the BSA compliance officer, independent review, and follow-up items.

1. Review the policies, procedures, and processes related to trust and asset management services. Evaluate the adequacy of the policies, procedures, and processes given the bank's trust and asset management activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. Review the bank's procedures for gathering additional identification information, when necessary, about the settlor, grantor, trustee, or other persons with authority to direct a trustee, and who thus have authority or control over the account, in order to establish a true identity of the customer.

3. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors trust and asset management relationships, particularly those that pose a higher risk for money laundering.

4. Determine how the bank includes trust and asset management relationships in a bank-wide or, if appropriate, firm-wide BSA/AML aggregation systems.

5. Determine whether the bank's system for monitoring trust and asset management relationships for suspicious activities, and for reporting of suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

6. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

7. On the basis of the bank's risk assessment of its trust and asset management relationships, as well as prior examination and audit reports, select a sample of higher-risk trust and asset management services relationships. Include relationships with grantors and co-trustees, if they have authority or control, as well as any higher-risk assets such as private investment

companies (PIC) or asset protection trusts. From the sample selected, perform the following examination procedures:

- Review account opening documentation, including the CIP, to ensure that adequate due diligence has been performed and that appropriate records are maintained.
- Review account statements and, as necessary, specific transaction details. Compare expected transactions with actual activity.
- Determine whether actual activity is consistent with the nature of the customer's business and the stated purpose of the account.
- Identify any unusual or suspicious activity.

8. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with trust and asset management relationships.

Section 25: Expanded Examination Overview and Procedures for Persons and Entities (revised 2014)

Nonresident Aliens and Foreign Individuals — Overview

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

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

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

Risk Factors

Banks may find it more difficult to verify and authenticate an NRA accountholder's identification, source of funds, and source of wealth, which may result in BSA/AML risks.

The NRA's home country may also heighten the account risk, depending on the secrecy laws of that country. Because the NRA is expected to reside outside of the United States, funds transfers or the use of foreign automated teller machines (ATM) may be more frequent. The BSA/AML risk may be further heightened if the NRA is a politically exposed person (PEP). Refer to the expanded examination procedures, "Politically Exposed Persons," for further information.

Risk Mitigation

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

- Accountholder's home country.
- Types of products and services used.
- Forms of identification.

- Source of wealth and funds.
- Unusual account activity.

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

The bank's CIP should detail the identification requirements for opening an account for a non-U.S. person, including an NRA. The program should include the use of documentary and nondocumentary methods to verify a customer. In addition, banks must maintain due diligence procedures for private banking accounts for non-U.S. persons, including those held for PEPs or senior foreign political figures. Refer to the core overview and examination procedures, "Private Banking Due Diligence Program (Non-U.S. Persons)," and the expanded overview and examination procedures, "Politically Exposed Persons."

Examination Procedures - Nonresident Aliens and Foreign Individuals

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

1. Review the bank's policies, procedures, and processes related to NRA and foreign individual accounts. Evaluate the adequacy of the policies, procedures, and processes given the bank's nonresident alien and foreign individual activities and the risks they represent. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors higher-risk NRA and foreign individual accounts.

3. Determine whether the bank's system of monitoring NRA and foreign individual accounts for suspicious activities, and for reporting of suspicious activities, is adequate based on the complexity of the bank's NRA and foreign individual relationships, the types of products used by NRAs and foreign individuals, the home countries of the NRAs, and the source of funds and wealth for NRAs and foreign individuals.

4. If appropriate, refer to core examination procedures, "Office of Foreign Assets Control," for further guidance.

Transaction Testing

5. On the basis of the bank's risk assessment of its NRA and foreign individual accounts, as well as prior examination and audit reports, select a sample of higher-risk NRA accounts. Include the following risk factors:

   - Account for resident or citizen of a higher-risk jurisdiction.
   - Account activity is substantially currency based.

- NRA or foreign individual who uses a wide range of bank services, particularly correspondent services.
- NRA or foreign individual for whom the bank has filed a SAR.

6. From the sample selected, perform the following examination procedures:

   - Review the customer due diligence information, including CIP information, if applicable.
   - Review account statements and, as necessary, transaction details to determine whether actual account activity is consistent with expected activity. Assess whether transactions appear unusual or suspicious.
   - For W-8 accounts, verify that appropriate forms have been completed and updated, as necessary. Review transaction activity and identify patterns that indicate U.S. resident status or indicate other unusual and suspicious activity.

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

Politically Exposed Persons - Overview

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with senior foreign political figures, often referred to as "politically exposed persons" (PEP), and management's ability to implement effective risk-based due diligence, monitoring, and reporting systems. If the relationship is a private banking account refer to core overview section, "Private Banking Due Diligence Program (Non-U.S. Persons)," for guidance.***

Banks should take all reasonable steps to ensure that they do not knowingly or unwittingly assist in hiding or moving the proceeds of corruption by senior foreign political figures, their families, and their associates. Because the risks presented by PEPs vary by customer, product/service, country, and industry, identifying, monitoring, and designing controls for these accounts and transactions should be risk-based.

The term "politically exposed person" generally includes a current or former senior foreign political figure, their immediate family, and their close associates. Interagency guidance issued in January 2001 offers banks resources that can help them to determine whether an individual is a PEP. More specifically:

- A "senior foreign political figure" is a senior official in the executive, legislative,
- administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned corporation. In addition, a senior foreign political figure includes any corporation, business, or other entity that has been formed by, or for the benefit of, a senior foreign political figure.
- The "immediate family" of a senior foreign political figure typically includes the figure's parents, siblings, spouse, children, and in-laws.
- A "close associate" of a senior foreign political figure is a person who is widely and publicly known to maintain an unusually close relationship with the senior foreign political figure, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the senior foreign political figure. The definition of senior official or executive must remain sufficiently flexible to capture the range of individuals who, by virtue of their office or position, potentially pose a risk that their funds may be the proceeds of foreign corruption. Titles alone may not provide sufficient information to determine if an individual is a PEP, because governments are organized differently from jurisdiction to jurisdiction. 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. Banks should establish risk-based controls and procedures that include reasonable steps to ascertain the status of an individual as a PEP and to conduct risk-based scrutiny of accounts held by these individuals. Risk varies depending on other factors, such as products and services used and size or complexity of the account relationship. Banks also should consider various factors when determining if an individual is a PEP including:
- Official responsibilities of the individual's office.
- Nature of the title (e.g., honorary or salaried).
- Level and nature of authority or influence over government activities or other officials.
- Access to significant government assets or funds.

In determining the acceptability of higher-risk accounts, a bank should be able to obtain sufficient information to determine whether an individual is or is not a PEP. For example, when conducting due diligence on a higher-risk account, it would be usual for a bank to review a customer's income sources, financial information, and professional background.

These factors would likely require some review of past and present employment as well as general references that may identify a customer's status as a PEP. Moreover, a bank should always keep in mind that identification of a customer's status as a PEP should not automatically result in a higher-risk determination; it is only one factor the bank should consider in assessing the risk of a relationship.

Ascertaining whether a customer has a close association with a senior foreign political figure can be difficult, although focusing on those relationships that are "widely and publicly known" provides a reasonable limitation on expectations to identify close associates as PEPs.

However, banks that have actual knowledge of a close association should consider their customer a PEP, even if such association is not otherwise widely or publicly known. Banks are expected to follow reasonable steps to ascertain the status of an individual, and the federal banking agencies and FinCEN recognize that these steps may not uncover all close associations.

Risk Factors

In high-profile cases over the past few years, PEPs have used banks as conduits for their illegal activities, including corruption, bribery, and money laundering. However, not all PEPs present the same level of risk. This risk varies depending on numerous factors, including the PEP's geographic location, industry, or sector, position, and level or nature of influence or authority. Risk may also vary depending on factors such as the purpose of the account, the actual or anticipated activity, products and services used, and size or complexity of the account relationship.

As a result of these factors, some PEPs may be lower risk and some may be higher risk for foreign corruption or money laundering. Banks that conduct business with dishonest PEPs face substantial reputational risk, additional regulatory scrutiny, and possible supervisory action. Red flags regarding transactions that may be related to the proceeds of foreign corruption are listed in the January 2001 interagency guidance. Banks also should be alert to a PEP's access to, and control or influence over, government or corporate accounts; the level of involvement of intermediaries, vendors, shippers, and agents in the industry or sector in which the PEP operates; and the improper use of corporate vehicles and other legal entities to obscure ownership.

Risk Mitigation

Banks should exercise reasonable judgment in designing and implementing policies, procedures, and processes regarding PEPs. Banks should obtain risk-based due diligence information on PEPs and establish policies, procedures, and processes that provide for appropriate scrutiny and monitoring. Having appropriate risk-based account opening procedures for large-dollar or higher-risk products and services is critical. The opening of an account is the prime opportunity for the bank to gather information for all customers, including PEPs. Commensurate with the identified level of risk, due diligence procedures should include, but are not necessarily

limited to, the following:

- Identify the accountholder and beneficial owner, including the nominal and beneficial owners of companies, trusts, partnerships, private investment companies, or other legal entities that are accountholders.
- Seek information directly from the account holder and beneficial owner regarding possible PEP status.
- Identify the accountholder's and beneficial owner's countr(ies) of residence and the level of risk for corruption and money laundering associated with these jurisdictions.
- Obtain information regarding employment, including industry and sector and the level of risk for corruption associated with the industries and sectors.
- Check references, as appropriate, to determine whether the account holder and beneficial owner is or has been a PEP.
- Identify the account holder's and beneficial owner's source of wealth and funds.
- Obtain information on immediate family members or close associates either having transaction authority over the account or benefiting from transactions conducted through the account.
- Determine the purpose of the account and the expected volume and nature of account activity.
- Make reasonable efforts to review public sources of information. These sources vary depending on each situation; however, banks should check the accountholder and any beneficial owners of legal entities against reasonably accessible public sources of information (e.g., government databases, major news publications, commercial databases and other databases available on the Internet, as appropriate).

PEP accounts are not limited to large or internationally focused banks. A PEP can open an account at any bank, regardless of its size or location. Banks should have risk-based procedures for identifying PEP accounts and assessing the degree of risks involved, which will vary. Management should be involved in the decision to accept a PEP account. If management determines after-the-fact that an account is a PEP account, it should evaluate the risks and take appropriate steps. The bank should exercise additional, reasonable due diligence with regard to such accounts. For example, the bank may increase reference inquiries, obtain additional background information on the PEP from branches or correspondents operating in the client's home country, and make reasonable efforts to consult publicly available information sources. Ongoing risk-based monitoring of PEP accounts is critical to ensuring that the accounts are being used as anticipated. Refer to core overview section, "Private Banking Due Diligence Program (Non-U.S. Persons)," for expectations regarding private banking relationships with PEPs.

Examination Procedures - Politically Exposed Persons

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with senior foreign political figures, often referred to as "politically exposed persons" (PEP), and management's ability to implement effective risk-based due diligence, monitoring, and reporting systems. If the relationship is a private banking account [273]refer to core overview section, "Private Banking Due Diligence Program (Non-U.S. Persons)," for guidance.***

1. Review the risk-based policies, procedures, and processes related to PEPs. Evaluate the adequacy of the policies, procedures, and processes given the bank's PEP accounts and the risks they present. Assess whether the risk-based controls are adequate to reasonably protect the bank from being used as a conduit for money laundering, corruption, and terrorist financing.

2. Review the procedures for opening PEP accounts. Identify management's role in the approval and ongoing risk-based monitoring of PEP accounts.

3. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors PEP relationships, particularly those that pose a higher risk for corruption, money laundering, and terrorist financing.

4. Determine whether the bank's system for monitoring PEPs for suspicious activities, and for reporting of suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

5. If appropriate, refer to core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

6. On the basis of the bank's risk assessment of its PEP relationships, as well as prior examination and audit reports, select a sample of PEP accounts. From the sample selected, perform the following examination procedures:

    - Determine compliance with regulatory requirements and with the bank's established policies, procedures, and processes related to PEPs.
    - Review transaction activity for accounts selected. If necessary, request and review specific transactions.
    - If the analysis of activity and customer due diligence information raises concerns, hold discussions with bank management.

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

Embassy, Foreign Consulate, and Foreign Mission Accounts - Overview

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

Embassies contain the offices of the foreign ambassador, the diplomatic representative, and their staff. The embassy, led by the ambassador, is a foreign government's official representation in the United States (or other country). Foreign consulate offices act as branches of the embassy and perform various administrative and governmental functions (e.g., issuing visas and handling immigration matters). Foreign consulate offices are typically located in major metropolitan areas. In addition, foreign ambassadors' diplomatic representatives, their families, and their associates may be considered politically exposed persons (PEP) in certain circumstances. Embassies and foreign consulates in the United States require access to the banking system to meet many of their day-to-day financial responsibilities. Such services can range from account relationships for operational expenses (e.g., payroll, rent, and utilities) to inter- and intragovernmental transactions (e.g., commercial and military purchases). In addition to official embassy accounts, some banks provide ancillary services or accounts to embassy staff, families, and current or prior foreign government officials. Each of these relationships poses different levels of risk to the bank.

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

In March 2011,the federal banking agencies and FinCEN issued joint interagency guidance on providing account services to foreign embassies, consulates and missions (foreign missions). This document supplements, but does not replace, guidance related to foreign governments and foreign political figures issued in June 2004.

Risk Factors

To provide embassy, foreign consulate, and foreign mission services, a U.S. bank may need to maintain a foreign correspondent relationship with the embassy's, foreign consulate's, or foreign mission's bank. Banks conducting business with foreign embassies, consulates, or missions should assess and understand the potential risks of these accounts and should develop appropriate policies, procedures, and processes. Embassy, foreign consulate, and foreign mission accounts may pose a higher risk in the following circumstances:

- Accounts are from countries that have been designated as higher risk.
- Substantial currency transactions take place in the accounts.
- Account activity is not consistent with the purpose of the account (e.g., pouch activity or payable upon proper identification transactions) or account transactions are in unusual amounts.
- Accounts directly fund personal expenses of foreign nationals, including but not limited to

expenses for college students.
- Official embassy business is conducted through personal accounts.

Risk Mitigation

Banks should obtain comprehensive due diligence information on embassy, foreign consulate, and foreign mission account relationships. For private banking accounts for non-U.S. persons specifically, banks must obtain due diligence information as required by 31 CFR 1010.620. The bank's due diligence related to embassy, foreign consulate, and foreign mission account relationships should be commensurate with the risk levels presented.

In addition, banks are expected to establish policies, procedures, and processes that provide for greater scrutiny and monitoring of all embassy, foreign consulate, and foreign mission account relationships. Management should fully understand the purpose of the account and the expected volume and nature of account activity. Ongoing monitoring of these account relationships is critical to ensuring that the account relationships are being used as anticipated.

Banks may also mitigate risk by entering into a written agreement that clearly defines the terms of use for the account(s), setting forth available services, acceptable transactions and access limitations. Written agreements to provide ancillary services or accounts to embassy, foreign consulate, and foreign mission personnel and their families may also assist in mitigating the varying degrees of risk.

Similarly, the bank could offer limited purpose accounts, such as those used to facilitate operational expense payments (e.g., payroll, rent and utilities, routine maintenance), which are generally considered lower risk and allow the implementation of customary functions in the United States. The type and volume of transactions should be commensurate with the purpose of the limited access account. Account monitoring to ensure compliance with account limitations and the terms of any service agreements is essential to mitigate risks associated with these accounts.

Examination Procedures - Embassy, Foreign Consulate, and Foreign Mission Accounts

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

1. Review the policies, procedures, and processes related to embassy, foreign consulate, and foreign mission accounts. Evaluate the adequacy of the policies, procedures, and processes given the bank's embassy, foreign consulate, and foreign mission accounts and the risks they present (e.g., number of accounts, volume of activity, and geographic locations). Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. Identify senior management's role in the approval and ongoing monitoring of embassy, foreign consulate, and foreign mission accounts. Determine whether the board is aware of these banking activities and whether it receives periodic reports on these activities.

3. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors embassy, foreign consulate, and foreign mission accounts, particularly those that pose a higher risk for money laundering.

4. Determine whether the bank's system for monitoring embassy, foreign consulate, and foreign mission accounts for suspicious activities, and for reporting of suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

5. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

6. On the basis of the bank's risk assessment of its embassy, foreign consulate, and foreign mission accounts, as well as prior examination and audit reports, select a sample of accounts. From the sample selected, perform the following examination procedures:

   - Determine compliance with regulatory requirements and with the bank's established policies, procedures, and processes.
   - Review the documentation authorizing the ambassador or the foreign consulate to conduct banking in the United States.
   - Review transaction activity for accounts selected. If necessary, request and review specific transactions.

7. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with embassy, foreign consulate, and foreign mission accounts.

Nonbank Financial Institutions - Overview

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with accounts of nonbank financial institutions (NBFI), and management's ability to implement effective monitoring and reporting systems.***

NBFIs are broadly defined as institutions other than banks that offer financial services. The USA PATRIOT Act has defined a variety of entities as financial institutions. Common examples of NBFIs include, but are not limited to:

- Casinos and card clubs.
- Securities and commodities firms (e.g., brokers/dealers, investment advisers, mutual funds, hedge funds, or commodity traders).
- Money services businesses (MSB).
- Insurance companies.
- Loan or finance companies.
- Operators of credit card systems.
- Other financial institutions (e.g., dealers in precious metals, stones, or jewels; pawnbrokers).

Some NBFIs are currently required to develop an AML program, comply with the reporting and recordkeeping requirements of the BSA, and report suspicious activity, as are banks.

NBFIs typically need access to banking services in order to operate. Although NBFIs maintain operating accounts at banks, the BSA does not require, and neither FinCEN nor the federal banking agencies expect, banks to serve as the *de facto* regulator of any NBFI industry or individual NBFI customer. Furthermore, while banks are expected to manage risk associated with all accounts, including NBFI accounts, banks are not held responsible for their customers' compliance with the BSA and other applicable federal and state laws and regulations.

Risk Factors

NBFI industries are extremely diverse, ranging from large multi-national corporations to small, independent businesses that offer financial services only as an ancillary component to their primary business (e.g., grocery store that offers check cashing). The range of products and services offered, and the customer bases served by NBFIs, are equally diverse. As a result of this diversity, some NBFIs may be lower risk and some may be higher risk for money laundering.

Banks that maintain account relationships with NBFIs may be exposed to a higher risk for potential money laundering activities because many NBFIs:

- Lack ongoing customer relationships and require minimal or no identification from customers.
- Maintain limited or inconsistent record keeping on customers and transactions.
- Engage in frequent currency transactions.
- Are subject to varying levels of regulatory requirements and oversight.
- Can quickly change their product mix or location and quickly enter or exit an operation.

- Sometimes operate without proper registration or licensing.

Risk Mitigation

Banks that maintain account relationships with NBFIs should develop policies, procedures, and processes to:

- Identify NBFI relationships.
- Assess the potential risks posed by the NBFI relationships.
- Conduct adequate and ongoing due diligence on the NBFI relationships when necessary.
- Ensure NBFI relationships are appropriately considered within the bank's suspicious activity monitoring and reporting systems.

Risk Assessment Factors

Banks should assess the risks posed by their NBFI customers and direct their resources most appropriately to those accounts that pose a more significant money laundering risk.

The following factors may be used to help identify the relative risks within the NBFI portfolio. Nevertheless, management should weigh and evaluate each risk assessment factor to arrive at a risk determination for each customer and to prioritize oversight resources.

Relevant risk factors include:

- Types of products and services offered by the NBFI.
- Locations and markets served by the NBFI.
- Anticipated account activity.
- Purpose of the account.

A bank's due diligence should be commensurate with the level of risk of the NBFI customer identified through its risk assessment. If a bank's risk assessment indicates potential for a heightened risk of money laundering or terrorist financing, the bank is expected to conduct further due diligence in a manner commensurate with the heightened risk.

Providing Banking Services to Money Services Businesses

FinCEN and the federal banking agencies issued interpretive guidance on April 26, 2005, to clarify the BSA requirements and supervisory expectations as applied to accounts opened or maintained for MSBs.281 With limited exceptions, many MSBs are subject to the full range of BSA regulatory requirements, including the anti-money laundering program rule, suspicious activity and currency transaction reporting rules, and various other identification and recordkeeping rules. Existing FinCEN regulations require certain MSBs to register with FinCEN. Finally, many states have established supervisory requirements, often including the requirement that an MSB be licensed with the state(s) in which it is incorporated or does business.

FinCEN defines MSBs as doing business in one or more of the following capacities:

- Dealer in foreign exchange
- Check casher
- Issuer or seller of traveler's checks or money orders
- Money transmitter
- Provider of prepaid access
- Seller of prepaid access
- U.S. Postal Service

There is a threshold requirement for dealers in foreign exchange, check cashers and issuers or sellers of traveler's checks or money orders. A business that engages in such transactions is not be considered an MSB if it does not engage in such transactions in an amount greater than $1,000 for any person on any day in one or more transactions (31 CFR 1010.100(ff)).

An entity that engages in money transmission in any amount is considered an MSB.

Thresholds for providers and sellers of prepaid access are discussed below.

Prepaid Access

FinCEN's regulation for MSBs excluded certain prepaid access arrangements from the definition of prepaid programs. Providers and sellers of prepaid access are not be considered MSBs if they engage in prepaid arrangements excluded from the definition of a prepaid program under 31 CFR 1010.100(ff)(4)(iii).284 The exclusions include arrangements that:

- Provide closed loop prepaid access to funds (e.g., such as store gift cards) in amounts not to exceed $2,000 maximum value per device on any day.
- Provide prepaid access solely to funds provided by a government agency.
- Provide prepaid access to funds for pre-tax flexible spending for health and dependent care, or from Health Reimbursement Arrangements for health care expenses.

There are two types of prepaid access arrangements that have a qualified exclusion:

- Open loop prepaid access that does not exceed $1,000 maximum value on any day.
- Prepaid access to employment benefits, incentives, wages or salaries (payroll).

These arrangements are not prepaid programs subject to BSA regulatory requirements unless they can:

- Be used internationally.
- Allow transfers of value from person to person within the arrangement, or
- Be reloaded from a non-depository source.

If any one of these features is part of the arrangement, it is a covered prepaid program under 31 CFR 1010.100.

Administrators and Exchangers of Virtual Currency

FinCEN's regulations define currency as "the coin and paper money of the United States or of any other country that is designated as legal tender; and that circulates; and is customarily used and accepted as a medium of exchange in the country of issuance." In contrast, "virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have legal tender status in any jurisdiction. Virtual currency must be converted into U.S. dollars through the services of an administrator or exchanger prior to deposit into the banking system. An administrator or exchanger of virtual currency is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. BSA requirements and supervisory expectations for providing banking services to administrators or exchangers of virtual currencies are the same as money transmitters.

Regulatory Expectations

The following regulatory expectations apply to banks with MSB customers:

- The BSA does not require, and neither FinCEN nor the federal banking agencies expect, banks to serve as the *de facto* regulator of any type of NBFI industry or individual NBFI customer, including MSBs.
- While banks are expected to manage risk associated with all accounts, including MSB accounts, banks are not be held responsible for the MSB's BSA/AML program.
- Not all MSBs pose the same level of risk, and not all MSBs require the same level of due diligence. Accordingly, if a bank's assessment of the risks of a particular MSB relationship indicates a lower risk of money laundering or other illicit activity, a bank is not routinely expected to perform further due diligence (such as reviewing information about an MSB's BSA/AML program) beyond the minimum due diligence expectations.

Unless indicated by the risk assessment of the MSB, banks are not expected to routinely review an MSB's BSA/AML program.

MSB Risk Assessment

An effective risk assessment should be a composite of multiple factors, and depending upon the circumstances, certain factors may be given more weight than others. The following factors may be used to help identify the level of risk presented by each MSB customer:

- Purpose of the account.
- Anticipated account activity (type and volume).
- Types of products and services offered by the MSB.
- Locations and markets served by the MSB.

Bank management may tailor these factors based on their customer base or the geographic locations in which the bank operates. Management should weigh and evaluate each risk assessment factor to arrive at a risk determination for each customer. A bank's due diligence should be commensurate with the level of risk assigned to the MSB customer, after consideration of these factors. If a bank's risk assessment indicates potential for a heightened risk of money laundering or terrorist financing, the bank is expected to conduct further due diligence in a

manner commensurate with the heightened risk.

MSB Risk Mitigation

A bank's policies, procedures, and processes should provide for sound due diligence and verification practices, adequate risk assessment of MSB accounts, and ongoing monitoring and reporting of unusual or suspicious activities. A bank that establishes and maintains accounts for MSBs should apply appropriate, specific, risk-based, and where necessary, EDD policies, procedures, and controls.

The factors below, while not all inclusive, may reduce or mitigate the risk in some MSB accounts:

- MSB is registered with FinCEN and licensed with the appropriate state(s), if required.
- MSB confirms it is subject to examination for AML compliance by the IRS or the state(s), if applicable.
- MSB affirms the existence of a written BSA/AML program and provides the BSA officer's name and contact information.
- MSB has an established banking relationship and/or account activity consistent with expectations.
- MSB is an established business with an operating history.
- MSB is a principal with one or a few agents, or is acting as an agent for one principal.
- MSB provides services only to local residents.
- Most of the MSB's customers conduct routine transactions in low dollar amounts.
- The expected (lower-risk) transaction activity for the MSB's business operations is consistent with information obtained by bank at account opening. Examples include the following:
  - Check cashing activity is limited to payroll or government checks (any dollar amount).
  - Check cashing service is not offered for third-party or out-of-state checks.
  - Money-transmitting activities are limited to domestic entities (e.g., domestic bill payments) or limited to lower dollar amounts (domestic or international).

MSB Due Diligence Expectations

Registration with FinCEN, if required, and compliance with any state-based licensing requirements represent the most basic of compliance obligations for MSBs. As a result, it is reasonable and appropriate for a bank to require an MSB to provide evidence of compliance with such requirements, or to demonstrate that it is not subject to such requirements due to the nature of its financial services or status exclusively as an agent of another MSB(s).

FinCEN issued a final rule clarifying that certain foreign-located persons engaging in MSB activities within the United States fall within FinCEN's definition of an MSB and are required to register with FinCEN.

Given the importance of licensing and registration requirements, a bank should file a SAR if it becomes aware that a customer is operating in violation of the registration or state licensing requirement. There is no requirement in the BSA regulations for a bank to close an account that

is the subject of a SAR. The decision to maintain or close an account should be made by bank management under standards and guidelines approved by its board of directors.

The extent to which the bank should perform further due diligence beyond the minimum due diligence obligations set forth below is dictated by the level of risk posed by the individual MSB customer. Because not all MSBs present the same level of risk, not all MSBs require further due diligence. For example, a local grocer that also cashes payroll checks for customers purchasing groceries may not present the same level of risk as a money transmitter specializing in cross-border funds transfers. Therefore, the customer due diligence requirements differ based on the risk posed by each MSB customer. Based on existing BSA requirements applicable to banks, the minimum due diligence expectations associated with opening and maintaining accounts for any MSB are:

- Apply the bank's CIP.
- Confirm FinCEN registration, if required. (Note: registration must be renewed every two years.)
- Confirm compliance with state or local licensing requirements, if applicable.
- Confirm agent status, if applicable.
- Conduct a basic BSA/AML risk assessment to determine the level of risk associated with the account and whether further due diligence is necessary.

If the bank determines that the MSB customer presents a higher level of money laundering or terrorist financing risk, EDD measures should be conducted in addition to the minimum due diligence procedures. Depending on the level of perceived risk, and the size and sophistication of the particular MSB, banking organizations may pursue some or all of the following actions as part of an appropriate EDD review:

- Review the MSB's BSA/AML program.
- Review results of the MSB's independent testing of its AML program.
- Review written procedures for the operation of the MSB.
- Conduct on-site visits.
- Review list of agents, including locations, within or outside the United States, which receive services directly or indirectly through the MSB account.
- Determine whether the MSB has performed due diligence on any third-party servicers or paying agents.
- Review written agent management and termination practices for the MSB.
- Review written employee screening practices for the MSB.

FinCEN and the federal banking agencies do not expect banks to uniformly require any or all of the actions identified above for all MSBs.

Examination Procedures - Nonbank Financial Institutions

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with accounts of nonbank financial institutions (NBFI), and management's ability to implement effective monitoring and reporting systems.***

1. Determine the extent of the bank's relationships with NBFIs and, for banks with significant relationships with NBFIs, review the bank's risk assessment of this activity.

2. Review the policies, procedures, and processes related to NBFI accounts. Evaluate the adequacy of the policies, procedures, and processes given the bank's NBFI activities and the risks they represent. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

3. From review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors NBFI accounts.

4. Determine whether the bank's system for monitoring NBFI accounts for suspicious activities, and for reporting of suspicious activities, is adequate given the nature of the bank's customer relationships.

Money Services Businesses

5. Consistent with the interagency guidance released on April 26, 2005, determine whether the bank has policies, procedures, and processes in place for accounts opened or maintained for money services businesses (MSB) to:

   - Apply the bank's CIP.[291]
   - Confirm FinCEN registration, if required. (Note: registration must be renewed every two years.)
   - Confirm state licensing, if applicable.
   - Confirm agent status, if applicable.
   - Conduct a risk assessment to determine the level of risk associated with each account and whether further due diligence is required.

6. Determine whether the bank's policies, procedures, and processes to assess risks posed by MSB customers effectively identify higher-risk accounts and the amount of further due diligence necessary.

10. Transaction Testing

7. On a basis of the bank's risk assessment of its NBFI accounts, as well as prior examination and audit reports, select a sample of higher-risk NBFI accounts. From the sample selected, perform the following examination procedures:

   - Review account opening documentation and ongoing due diligence information.
   - Review account statements and, as necessary, specific transaction details. Compare expected transactions with actual activity.
   - Determine whether actual activity is consistent with the nature of the customer's business and identify any unusual or suspicious activity.

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

Professional Service Providers - Overview

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with professional service provider relationships, and management's ability to implement effective due diligence, monitoring, and reporting systems.***

A professional service provider acts as an intermediary between its client and the bank. Professional service providers include lawyers, accountants, investment brokers, and other third parties that act as financial liaisons for their clients. These providers may conduct financial dealings for their clients. For example, an attorney may perform services for a client, or arrange for services to be performed on the client's behalf, such as settlement of real estate transactions, asset transfers, management of client monies, investment services, and trust arrangements.

A typical example is interest on lawyers' trust accounts (IOLTA). These accounts contain funds for a lawyer's various clients, and act as a standard bank account with one unique feature: The interest earned on the account is ceded to the state bar association or another entity for public interest and pro bono purposes.

Risk Factors

In contrast to escrow accounts that are set up to serve individual clients, professional service provider accounts allow for ongoing business transactions with multiple clients. Generally, a bank has no direct relationship with or knowledge of the beneficial owners of these accounts, who may be a constantly changing group of individuals and legal entities.

As with any account that presents third-party risk, the bank could be more vulnerable to potential money laundering abuse. Some potential examples of abuse could include:

- Laundering illicit currency.
- Structuring currency deposits and withdrawals.
- Opening any third-party account for the primary purpose of masking the underlying client's identity.

As such, the bank should establish an effective due diligence program for the professional service provider as summarized below.

Risk Mitigation

When establishing and maintaining relationships with professional service providers, banks should adequately assess account risk and monitor the relationship for suspicious or unusual activity. At account opening, the bank should have an understanding of the intended use of the account, including anticipated transaction volume, products and services used, and geographic locations involved in the relationship. As indicated in the core overview section, "Currency Transaction Reporting Exemptions," professional service providers cannot be exempted from currency transaction reporting requirements.

Examination Procedures - Professional Service Providers

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with professional service provider relationships, and management's ability to implement effective due diligence, monitoring, and reporting systems.***

1. Review the policies, procedures, and processes related to professional service provider relationships. Evaluate the adequacy of the policies, procedures, and processes given the bank's relationships with professional service providers and the risks these relationships represent. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors professional service provider relationships. MIS reports should include information about an entire relationship. For example, an interest on lawyers' trust account (IOLTA) may be in the name of the law firm instead of an individual. However, the bank's relationship report should include the law firm's account *and* the names and accounts of lawyers associated with the IOLTA.

3. Determine whether the bank's system for monitoring professional service provider relationship's suspicious activities, and for reporting of suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

4. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

5. On the basis of the bank's risk assessment of its relationships with professional service providers, as well as prior examination and audit reports, select a sample of higher-risk relationships. From the sample selected, perform the following examination procedures:

   - Review account opening documentation and a sample of transaction activity.
   - Determine whether actual account activity is consistent with anticipated (as documented) account activity. Look for trends in the nature, size, or scope of the transactions, paying particular attention to currency transactions.
   - Determine whether ongoing monitoring is sufficient to identify potentially 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 professional service provider relationships.

Nongovernmental Organizations and Charities - Overview

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with accounts of nongovernmental organizations (NGO) and charities, and management's ability to implement effective due diligence, monitoring, and reporting systems.***

NGOs are private nonprofit organizations that pursue activities intended to serve the public good. NGOs may provide basic social services, work to relieve suffering, promote the interests of the poor, bring citizen concerns to governments, encourage political participation, protect the environment, or undertake community development to serve the needs of citizens, organizations, or groups in one or more of the communities that the NGO operates. An NGO can be any nonprofit organization that is independent from government. NGOs can range from large regional, national, or international charities to community-based self-help groups. NGOs also include research institutes, churches, professional associations, and lobby groups. NGOs typically depend, in whole or in part, on charitable donations and voluntary service for support.

Risk Factors

Because NGOs can be used to obtain funds for charitable organizations, the flow of funds both into and out of the NGO can be complex, making them susceptible to abuse by money launderers and terrorists. The U.S. Treasury issued guidelines to assist charities in adopting practices to reduce the risk of terrorist financing or abuse.

Risk Mitigation

To assess the risk of NGO customers, a bank should conduct adequate due diligence on the organization. In addition to required CIP information, due diligence for NGOs should focus on other aspects of the organization, such as the following:

- Purpose and objectives of their stated activities.
- Geographic locations served (including headquarters and operational areas).
- Organizational structure.
- Donor and volunteer base.
- Funding and disbursement criteria (including basic beneficiary information).
- Recordkeeping requirements.
- Its affiliation with other NGOs, governments, or groups.
- Internal controls and audits.

For accounts that bank management considers to be higher risk, stringent documentation, verification, and transaction monitoring procedures should be established. NGO accounts that are at higher risk for BSA/AML concerns include those operating or providing services internationally, conducting unusual or suspicious activities, or lacking proper documentation.

EDD for these accounts should include:

- Evaluating the principals.
- Obtaining and reviewing the financial statements and audits.
- Verifying the source and use of funds.
- Evaluating large contributors or grantors of the NGO.

- Conducting reference checks.

Examination Procedures - Non-Governmental Organizations and Charities

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with accounts of nongovernmental organizations (NGO) and charities, and management's ability to implement effective due diligence, monitoring, and reporting systems.***

1. Review the policies, procedures, and processes related to NGOs. Evaluate the adequacy of the policies, procedures, and processes given the bank's NGO accounts and the risks they represent. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors higher-risk NGO accounts.

3. Determine whether the bank's system for monitoring NGO accounts for suspicious activities, and for reporting of suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

4. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

5. On the basis of the bank's risk assessment, its NGO and charity accounts, as well as prior examination and audit reports, select a sample of higher-risk NGO accounts. From the sample selected, perform the following examination procedures:

   - Review account opening documentation and ongoing due diligence information.
   - Review account statements and, as necessary, specific transaction details.
   - Compare expected transactions with actual activity.
   - Determine whether actual activity is consistent with the nature of the customer's business.
   - Identify any unusual or 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 NGO accounts.

Business Entities (Domestic and Foreign) - Overview

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with transactions involving domestic and foreign business entities, and management's ability to implement effective due diligence, monitoring, and reporting systems.***

The term "business entities" refers to limited liability companies, corporations, trusts, and other entities that may be used for many purposes, such as tax and estate planning. Business entities are relatively easy to establish. Individuals, partnerships, and existing corporations establish business entities for legitimate reasons, but the entities may be abused for money laundering and terrorist financing.

Domestic Business Entities

All states have statutes governing the organization and operation of business entities, including limited liability companies, corporations, general partnerships, limited partnerships, and trusts. Shell companies registered in the United States are a type of domestic business entity that may pose heightened risks. Shell companies can be used for money laundering and other crimes because they are easy and inexpensive to form and operate. In addition, ownership and transactional information can be concealed from regulatory agencies and law enforcement, in large part because most state laws require minimal disclosures of such information during the formation process. According to a report by the U.S. Government Accountability Office (GAO), law enforcement officials are concerned that criminals are increasingly using U.S. shell companies to conceal their identity and illicit activities.

Shell companies can be publicly traded or privately held. Although publicly traded shell companies can be used for illicit purposes, the vulnerability of the shell company is compounded when it is privately held and beneficial ownership can more easily be obscured or hidden. Lack of transparency of beneficial ownership can be a desirable characteristic for some legitimate uses of shell companies, but it is also a serious vulnerability that can make some shell companies ideal vehicles for money laundering and other illicit financial activity.

In some state jurisdictions, only minimal information is required to register articles of incorporation or to establish and maintain "good standing" for business entities – increasing the potential for their abuse by criminal and terrorist organizations.

Foreign Business Entities

Frequently used foreign entities include trusts, investment funds, and insurance companies. Two foreign entities that can pose particular money laundering risk are international business corporations (IBC) and Private Investment Companies (PIC) opened in offshore financial centers (OFC). Many OFCs have limited organizational disclosure and recordkeeping requirements for establishing foreign business entities, creating an opportune environment for money laundering.

International Business Corporations

IBCs are entities formed outside of a person's country of residence that can be used to maintain

confidentially or hide assets. IBC ownership can, based on jurisdiction, be conveyed through registered or bearer shares. There are a variety of advantages to using an IBC that include, but are not limited to, the following:

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

Through an IBC, an individual is able to conduct the following:

- Open and hold bank accounts.
- Hold and transfer funds.
- Engage in international business and other related transactions.
- Hold and manage offshore investments (e.g., stocks, bonds, mutual funds, and certificates of deposit), many of which may not be available to "individuals" depending on their location of residence.
- Hold corporate debit and credit cards, thereby allowing convenient access to funds.

Private Investment Companies

PICs are separate legal entities. They are essentially subsets of IBCs. Determining whether a foreign corporation is a PIC is based on identifying the purpose and use of the legal vehicle.

PICs are typically used to hold individual funds and investments, and ownership can be vested through bearer shares or registered shares. Like other IBCs, PICs can offer confidentiality of ownership, hold assets centrally, and may provide intermediaries between private banking customers and the potential beneficiaries of the PICs. Shares of a PIC may be held by a trust, which further obscures beneficial ownership of the underlying assets.

IBCs, including PICs, are frequently incorporated in countries that impose low or no taxes on company assets and operations or are bank secrecy havens.

Nominee Incorporation Services

Intermediaries, called nominee incorporation services (NIS), establish U.S. shell companies and bank accounts on behalf of foreign clients. NIS may be located in the United States or offshore. Corporate lawyers in the United States often use NIS to organize companies on behalf of their domestic and foreign clients because such services can efficiently organize legal entities in any state. NIS must comply with applicable state and federal procedures as well as any specific bank requirements. Those laws and procedures dictate what information NIS must share about the owners of a legal entity. Money launderers have also utilized NIS to hide their identities. By hiring a firm to serve as an intermediary between themselves, the licensing jurisdiction, and the bank, a company's beneficial owners may avoid disclosing their identities in state corporate filings and in corporate bank account opening documentation.

An NIS has the capability to form business entities, open full-service bank accounts for those entities, and act as the registered agent to accept service of legal process on behalf of those entities

in a jurisdiction in which the entities have no physical presence. Furthermore, an NIS can perform these services without ever having to identify beneficial ownership on company formation, registration, or bank account documents.

Several international NIS firms have formed partnerships or marketing alliances with U.S. banks to offer financial services such as Internet banking and funds transfer capabilities to shell companies and non-U.S. citizens. U.S. banks participating in these marketing alliances by opening accounts through intermediaries without requiring the actual accountholder's physical presence, accepting by mail copies of passport photos, utility bills, and other identifying information may be assuming increased levels of BSA/AML risk.

Risk Factors

Money laundering and terrorist financing risks arise because business entities can hide the true owner of assets or property derived from or associated with criminal activity. The privacy and confidentiality surrounding some business entities may be exploited by criminals, money launderers, and terrorists. Verifying the grantors and beneficial owner(s) of some business entities may be extremely difficult, as the characteristics of these entities shield the legal identity of the owner. Few public records disclose true ownership. Overall, the lack of ownership transparency; minimal or no recordkeeping requirements, financial disclosures, and supervision; and the range of permissible activities all increase money laundering risk.

While business entities can be established in most international jurisdictions, many are incorporated in OFCs that provide ownership privacy and impose few or no tax obligations.

To maintain anonymity, many business entities are formed with nominee directors, officeholders, and shareholders. In certain jurisdictions, business entities can also be established using bearer shares; ownership records are not maintained, rather ownership is based on physical possession of the stock certificates. Revocable trusts are another method used to insulate the grantor and beneficial owner and can be designed to own and manage the business entity, presenting significant barriers to law enforcement.

While the majority of U.S.-based shell companies serve legitimate purposes, some shell companies have been used as conduits for money laundering, to hide overseas transactions, or to layer domestic or foreign business entity structures. For example, regulators have identified shell companies registered in the United States conducting suspicious transactions with foreign-based counterparties. These transactions, primarily funds transfers circling in and out of the U.S. banking system, evidenced no apparent business purpose. Domestic business entities with bank-like names, but without regulatory authority to conduct banking, should be particularly suspect.

The following indicators of potentially suspicious activity may be commonly associated with shell company activity:

- Insufficient or no information available to positively identify originators or beneficiaries of funds transfers (using Internet, commercial database searches, or direct inquiries to a respondent bank).
- Payments have no stated purpose, do not reference goods or services, or identify only a contract or invoice number.
- Goods or services, if identified, do not match profile of company provided by respondent

bank or character of the financial activity; a company references remarkably dissimilar goods and services in related funds transfers; explanation given by foreign respondent bank is inconsistent with observed funds transfer activity.
- Transacting businesses share the same address, provide only a registered agent's address, or other address inconsistencies.
- Many or all of the funds transfers are sent in large, round dollar, hundred dollar, or thousand dollar amounts.
- Unusually large number and variety of beneficiaries receiving funds transfers from one company.
- Frequent involvement of multiple jurisdictions or beneficiaries located in higher-risk OFCs.
- A foreign correspondent bank exceeds the expected volume in its client profile for funds transfers, or an individual company exhibits a high volume and pattern of funds transfers that is inconsistent with its normal business activity.
- Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.
- Purpose of the shell company is unknown or unclear.

Risk Mitigation

Management should develop policies, procedures, and processes that enable the bank to identify account relationships, in particular deposit accounts, with business entities, and monitor the risks associated with these accounts in all the bank's departments. Business entity customers may open accounts within the private banking department, within the trust department, or at local branches. Management should establish appropriate due diligence at account opening and during the life of the relationship to manage risk in these accounts. The bank should gather sufficient information on the business entities and their beneficial owners to understand and assess the risks of the account relationship. Important information for determining the valid use of these entities includes the type of business, the purpose of the account, the source of funds, and the source of wealth of the owner or beneficial owner.

The bank's CIP should detail the identification requirements for opening an account for a business entity. When opening an account for a customer that is not an individual, banks are permitted by 31 CFR 1020.100 to obtain information about the individuals who have authority and control over such accounts in order to verify the customer's identity (the customer being the business entity). Required account opening information may include articles of incorporation, a corporate resolution by the directors authorizing the opening of the account, or the appointment of a person to act as a signatory for the entity on the account.

Particular attention should be paid to articles of association that allow for nominee shareholders, board members, and bearer shares.

If the bank, through its trust or private banking departments, is facilitating the establishment of a business entity for a new or existing customer, the money laundering risk to the bank is typically mitigated. Because the bank is aware of the parties (e.g., grantors, beneficiaries, and shareholders) involved in the business entity, initial due diligence and verification is easier to obtain. Furthermore, in such cases, the bank frequently has ongoing relationships with the customers initiating the establishment of a business entity.

Risk assessments may include a review of the domestic or international jurisdiction where the business entity was established, the type of account (or accounts) and expected versus actual transaction activities, the types of products used, and whether the business entity was created in-house or externally. If ownership is held in bearer share form, banks should assess the risks these relationships pose and determine the appropriate controls. For example, in most cases banks should choose to maintain (or have an independent third party maintain) bearer shares for customers. In rare cases involving lower-risk, well-known, established customers, banks may find that periodically recertifying beneficial ownership is effective.

The bank's risk assessment of a business entity customer becomes more important in complex corporate formations. For example, a foreign IBC may establish a layered series of business entities, with each entity naming its parent as its beneficiary.

Ongoing account monitoring is critical to ensure that the accounts are reviewed for unusual and suspicious activity. The bank should be aware of higher-risk transactions in these accounts, such as activity that has no business or apparent lawful purpose, funds transfer activity to and from higher-risk jurisdictions, currency intensive transactions, and frequent changes in the ownership or control of the nonpublic business entity.

Examination Procedures - Business Entities (Domestic and Foreign)

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with transactions involving domestic and foreign business entities, and management's ability to implement effective due diligence, monitoring, and reporting systems.***

1. Review the bank's policies, procedures, and processes related to business entities. Evaluate the adequacy of the policies, procedures, and processes given the bank's transactions with business entities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. Review the policies and processes for opening and monitoring accounts with business entities. Determine whether the policies adequately assess the risk between different account types.

3. Determine how the bank identifies and, as necessary, completes additional due diligence on business entities. Assess the level of due diligence the bank performs when conducting its risk assessment.

4. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors higher-risk business entity accounts.

5. Determine whether the bank's system for monitoring business entities for suspicious activities, and for reporting of suspicious activities, is adequate given the activities associated with business entities.

6. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

7. On the basis of the bank's risk assessment of its accounts with business entities, as well as prior examination and audit reports, select a sample of these accounts. Include the following risk factors:

   - An entity organized in a higher-risk jurisdiction.
   - Account activity that is substantially currency based.
   - An entity whose account activity consists primarily of circular-patterned funds transfers.
   - A business entity whose ownership is in bearer shares, especially bearer shares that are not under bank or trusted third-party control.
   - An entity that uses a wide range of bank services, particularly trust and correspondent services.
   - An entity owned or controlled by other nonpublic business entities.
   - Business entities for which the bank has filed SARs.

8. From the sample selected, obtain a relationship report for each selected account. It is critical that the full relationship, rather than only an individual account, be reviewed.

9. Review the due diligence information on the business entity. Assess the adequacy of that information.

10. Review account statements and, as necessary, specific transaction details. Compare expected transactions with actual activity. Determine whether actual activity is consistent with the nature and stated purpose of the account and whether transactions appear unusual or suspicious. Areas that may pose a higher risk, such as funds transfers, private banking, trust, and monetary instruments, should be a primary focus of the transaction review.

11. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with business entity relationships.

Cash-Intensive Businesses - Overview

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with cash-intensive businesses and entities, and management's ability to implement effective due diligence, monitoring, and reporting systems.***

Cash-intensive businesses and entities cover various industry sectors. Most of these businesses are conducting legitimate business; however, some aspects of these businesses may be susceptible to money laundering or terrorist financing. Common examples include, but are not limited to, the following:

- Convenience stores.
- Restaurants.
- Retail stores.
- Liquor stores.
- Cigarette distributors.
- Privately owned automated teller machines (ATM).
- Vending machine operators.
- Parking garages.

Risk Factors

Some businesses and entities may be misused by money launderers to legitimize their illicit proceeds. For example, a criminal may own a cash-intensive business, such as a restaurant, and use it to launder currency from illicit criminal activities. The restaurant's currency deposits with its bank do not, on the surface, appear unusual because the business is legitimately a cash-generating entity. However, the volume of currency in a restaurant used to launder money is most likely be higher in comparison with similar restaurants in the area.

The nature of cash-intensive businesses and the difficulty in identifying unusual activity may cause these businesses to be considered higher risk.

Risk Mitigation

When establishing and maintaining relationships with cash-intensive businesses, banks should establish policies, procedures, and processes to identify higher-risk relationships; assess AML risks; complete due diligence at account opening and periodically throughout the relationship; and include such relationships in appropriate monitoring for unusual or suspicious activity. At the time of account opening, the bank should have an understanding of the customer's business operations; the intended use of the account; including anticipated transaction volume, products, and services used; and the geographic locations involved in the relationship.

When conducting a risk assessment of cash-intensive businesses, banks should direct their resources to those accounts that pose the greatest risk of money laundering or terrorist financing. The following factors may be used to identify the risks:

- Purpose of the account.
- Volume, frequency, and nature of currency transactions.
- Customer history (e.g., length of relationship, CTR filings,300 and SAR filings).

- Primary business activity, products, and services offered.
- Business or business structure.
- Geographic locations and jurisdictions of operations.
- Availability of information and cooperation of the business in providing information.

For those customers deemed to be particularly higher risk, bank management may consider implementing sound practices, such as periodic on-site visits, interviews with the business's management, or closer reviews of transactional activity.

Examination Procedures - Cash-Intensive Businesses

Objective. ***Assess the adequacy of the bank's systems to manage the risks associated with cash-intensive businesses and entities, and management's ability to implement effective due diligence, monitoring, and reporting systems.***

1. Review the policies, procedures, and processes related to cash-intensive businesses. Evaluate the adequacy of policies, procedures, and processes given the bank's cash-intensive business activities in relation to the bank's cash-intensive business customers and the risks that they represent. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors cash-intensive businesses and entities.

3. Determine whether the bank's system for monitoring cash-intensive businesses for suspicious activities, and for reporting of suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

4. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," for guidance.

Transaction Testing

5. On the basis of the bank's risk assessment of its cash-intensive business and entity relationships, as well as prior examination and audit reports, select a sample of cash-intensive businesses. As an alternative, identify branches in the bank's highest-risk areas or branches that ship/receive the most cash and request the largest sources and users of cash at those locations. From the sample selected, perform the following examination procedures:

   - Review account opening documentation including CIP information, if applicable, and a sample of transaction activity.
   - Determine whether actual account activity is consistent with anticipated account activity.
   - Look for trends in the nature, size, or scope of the transactions, paying particular attention to currency transactions.
   - Determine whether ongoing monitoring is sufficient to identify potentially 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 cash-intensive businesses and entities.