Bank Secrecy Act/ Anti-Money Laundering Examination Manual

Federal Financial Institutions Examination Council
Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation,
National Credit Union Administration, Office of the Comptroller of the Currency,
Office of Thrift Supervision, and State Liaison Committee

2010

TABLE OF CONTENTS

The sections of the FFIEC *BSA/AML Examination Manual* that have been added or significantly modified from the previous edition are reflected by date.

INTRODUCTION *5*

CORE EXAMINATION OVERVIEW AND PROCEDURES FOR ASSESSING THE BSA/AML COMPLIANCE PROGRAM *15*

Scoping and Planning — Overview (2010) 15
Examination Procedures 19
BSA/AML Risk Assessment — Overview (2010) 22
Examination Procedures 31
BSA/AML Compliance Program — Overview (2010) 32
Examination Procedures 38
Developing Conclusions and Finalizing the Examination — Overview (2010) 44
Examination Procedures 48

CORE EXAMINATION OVERVIEW AND PROCEDURES FOR REGULATORY REQUIREMENTS AND RELATED TOPICS *52*

Customer Identification Program — Overview 52
Examination Procedures 59
Customer Due Diligence — Overview 63
Examination Procedures 66
Suspicious Activity Reporting — Overview (2010) 67
Examination Procedures 81
Currency Transaction Reporting — Overview 86
Examination Procedures 88
Currency Transaction Reporting Exemptions — Overview (2010) 90
Examination Procedures 95
Information Sharing — Overview 97
Examination Procedures 103
Purchase and Sale of Monetary Instruments Recordkeeping — Overview 106
Examination Procedures 109
Funds Transfers Recordkeeping — Overview 110
Examination Procedures 116
Foreign Correspondent Account Recordkeeping and Due Diligence — Overview 117
Examination Procedures 125
Private Banking Due Diligence Program (Non-U.S. Persons) — Overview 130
Examination Procedures 135
Special Measures — Overview 138
Examination Procedures 141
Foreign Bank and Financial Accounts Reporting — Overview (2010) 142
Examination Procedures 143
International Transportation of Currency or Monetary Instruments Reporting — Overview 144
Examination Procedures 146

Office of Foreign Assets Control — Overview (2010) 147
Examination Procedures 157

EXPANDED EXAMINATION OVERVIEW AND PROCEDURES FOR CONSOLIDATED AND OTHER TYPES OF BSA/AML COMPLIANCE PROGRAM STRUCTURES *160*
BSA/AML Compliance Program Structures — Overview (2010) 160
Examination Procedures 166
Foreign Branches and Offices of U.S. Banks — Overview 169
Examination Procedures 173
Parallel Banking — Overview 175
Examination Procedures 176

EXPANDED EXAMINATION OVERVIEW AND PROCEDURES FOR PRODUCTS AND SERVICES *178*
Correspondent Accounts (Domestic) — Overview 178
Examination Procedures 181
Correspondent Accounts (Foreign) — Overview 183
Examination Procedures 186
Bulk Shipments of Currency — Overview (2010) 188
Examination Procedures 193
U.S. Dollar Drafts — Overview 195
Examination Procedures 196
Payable Through Accounts — Overview 198
Examination Procedures 201
Pouch Activities — Overview 204
Examination Procedures 206
Electronic Banking — Overview (2010) 208
Examination Procedures 212
Funds Transfers — Overview (2010) 213
Examination Procedures 221
Automated Clearing House Transactions — Overview (2010) 224
Examination Procedures 232
Electronic Cash — Overview (2010) 234
Examination Procedures 238
Third-Party Payment Processors — Overview (2010) 239
Examination Procedures 242
Purchase and Sale of Monetary Instruments — Overview 243
Examination Procedures 244
Brokered Deposits — Overview 246
Examination Procedures 248
Privately Owned Automated Teller Machines — Overview 250
Examination Procedures 253
Nondeposit Investment Products — Overview 255
Examination Procedures 260
Insurance — Overview 262
Examination Procedures 265
Concentration Accounts — Overview 267

Examination Procedures 269
Lending Activities — Overview 270
Examination Procedures 272
Trade Finance Activities — Overview (2010) 273
Examination Procedures 278
Private Banking — Overview (2010) 279
Examination Procedures 284
Trust and Asset Management Services — Overview 286
Examination Procedures 291

EXPANDED EXAMINATION OVERVIEW AND PROCEDURES FOR PERSONS AND ENTITIES *293*

Nonresident Aliens and Foreign Individuals — Overview 293
Examination Procedures 295
Politically Exposed Persons — Overview (2010) 297
Examination Procedures 301
Embassy and Foreign Consulate Accounts — Overview 303
Examination Procedures 305
Nonbank Financial Institutions — Overview 307
Examination Procedures 314
Professional Service Providers — Overview 316
Examination Procedures 318
Nongovernmental Organizations and Charities — Overview 320
Examination Procedures 322
Business Entities (Domestic and Foreign) — Overview 323
Examination Procedures 329
Cash-Intensive Businesses — Overview 331
Examination Procedures 333
Appendix A: BSA Laws and Regulations A–1
Appendix B: BSA/AML Directives (2010) B–1
Appendix C: BSA/AML References (2010) C–1
Appendix D: Statutory Definition of Financial Institution D–1
Appendix E: International Organizations E–1
Appendix F: Money Laundering and Terrorist Financing "Red Flags" (2010) F–1
Appendix G: Structuring G–1
Appendix H: Request Letter Items (Core and Expanded) (2010) H–1
Appendix I: Risk Assessment Link to the BSA/AML Compliance Program I–1
Appendix J: Quantity of Risk Matrix J–1
Appendix K: Customer Risk Versus Due Diligence and Suspicious Activity Monitoring K–1
Appendix L: SAR Quality Guidance L–1
Appendix M: Quantity of Risk Matrix — OFAC Procedures M–1
Appendix N: Private Banking — Common Structure N–1
Appendix O: Examiner Tools for Transaction Testing O–1
Appendix P: BSA Record Retention Requirements P–1
Appendix Q: Acronyms (2010) Q–1
Appendix R: Enforcement Guidance R–1

Appendix S: Key Suspicious Activity Monitoring Components (2010) S–1
Index Index–1

INTRODUCTION

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

Structure of Manual

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

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

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

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

The core and expanded overview sections provide narrative guidance and background information on each topic; each overview is followed by examination procedures. The "Core Examination Overview and Procedures for Assessing the BSA/AML Compliance Program" and the "Core Examination Overview and Procedures for Regulatory Requirements and Related Topics" (core) sections serve as a platform for the BSA/AML examination and, for the most part, address legal and regulatory requirements of the BSA/AML compliance program. The "Scoping and Planning" and the "BSA/AML Risk Assessment" sections help the examiner develop an appropriate examination plan based on the risk profile of the bank. There may be instances where a topic is covered in both the core and expanded sections (e.g., funds transfers and foreign correspondent banking). In such instances, the core overview and examination procedures address the BSA requirements while the expanded overview and examination procedures address the AML risks of the specific activity.

At a minimum, examiners should use the following examination procedures included within the "Core Examination Overview and Procedures for Assessing the BSA/AML Compliance Program" section of this manual to ensure that the bank has an adequate BSA/AML compliance program commensurate with its risk profile:

- Scoping and Planning (refer to pages 19 to 21).
- BSA/AML Risk Assessment (refer to page 31).
- BSA/AML Compliance Program (refer to pages 38 to 43).
- Developing Conclusions and Finalizing the Examination (refer to pages 48 to 51).

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

The expanded sections address specific lines of business, products, customers, or entities that may present unique challenges and exposures for which banks should institute appropriate policies, procedures, and processes. Absent appropriate controls, these lines of business, products, customers, or entities could elevate BSA/AML risks. In addition, the expanded section provides guidance on BSA/AML compliance program structures and management.

Not all of the core and expanded examination procedures will likely be applicable to every banking organization. The specific examination procedures that will need to be performed depend on the BSA/AML risk profile of the banking organization, the quality

and quantity of independent testing, the financial institution's history of BSA/AML compliance, and other relevant factors.

Background

In 1970, Congress passed the Currency and Foreign Transactions Reporting Act commonly known as the "Bank Secrecy Act,"[2] which established requirements for recordkeeping and reporting by private individuals, banks,[3] and other financial institutions. The BSA was designed to help identify the source, volume, and movement of currency and other monetary instruments transported or transmitted into or out of the United States or deposited in financial institutions. The statute sought to achieve that objective by requiring individuals, banks, and other financial institutions to file currency reports with the U.S. Department of the Treasury (U.S. Treasury), properly identify persons conducting transactions, and maintain a paper trail by keeping appropriate records of financial transactions. These records enable law enforcement and regulatory agencies to pursue investigations of criminal, tax, and regulatory violations, if warranted, and provide evidence useful in prosecuting money laundering and other financial crimes.

The Money Laundering Control Act of 1986 augmented the BSA's effectiveness by adding the interrelated sections 8(s) and 21 to the Federal Deposit Insurance Act (FDIA) and section 206(q) of the Federal Credit Union Act (FCUA), which sections apply equally to banks of all charters.[4] The Money Laundering Control Act of 1986 precludes circumvention of the BSA requirements by imposing criminal liability on a person or financial institution that knowingly assists in the laundering of money, or that structures transactions to avoid reporting them. The 1986 statute directed banks to establish and maintain procedures reasonably designed to ensure and monitor compliance with the reporting and recordkeeping requirements of the BSA. As a result, on January 27, 1987, all federal banking agencies issued essentially similar regulations requiring banks to develop programs for BSA compliance.

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

In April 1996, a Suspicious Activity Report (SAR) was developed to be used by all banking organizations in the United States. A banking organization is required to file a

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

[3] Under the BSA, as implemented by 31 CFR 103.11, the term "bank" includes each agent, agency, branch or office within the United States of commercial banks, savings and loan associations, thrift institutions, credit unions, and foreign banks. The term "bank" is used throughout the manual generically to refer to the financial institution being examined.

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

SAR whenever it detects a known or suspected criminal violation of federal law or a suspicious transaction related to money laundering activity or a violation of the BSA.

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

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

Role of Government Agencies in the BSA

Certain government agencies play a critical role in implementing BSA regulations, developing examination guidance, ensuring compliance with the BSA, and enforcing the BSA. These agencies include the U.S. Treasury, FinCEN, and the federal banking agencies (Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision). Internationally there are various multilateral

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

government bodies that support the fight against money laundering and terrorist financing. Refer to Appendix E ("International Organizations") for additional information.

U.S. Treasury

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

FinCEN

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

Federal Banking Agencies

The federal banking agencies are responsible for the oversight of the various banking entities operating in the United States, including foreign branch offices of U.S. banks. The federal banking agencies are charged with chartering (National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision), insuring (Federal Deposit Insurance Corporation and National Credit Union Administration), regulating, and supervising banks.[6] 12 USC 1818(s)(2) and 1786(q) require that the appropriate federal banking agency include a review of the BSA compliance program at each examination of an insured depository institution. The federal banking agencies may use their authority, as granted under section 8 of the FDI Act, to enforce compliance with appropriate banking rules and regulations, including compliance with the BSA.

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

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

Banks should take reasonable and prudent steps to combat money laundering and terrorist financing and to minimize their vulnerability to the risk associated with such activities. Some banking organizations have damaged their reputations and have been required to pay civil money penalties for failing to implement adequate controls within their organization resulting in noncompliance with the BSA. In addition, due to the AML assessment required as part of the application process, BSA/AML concerns can have an impact on the bank's strategic plan. For this reason, the federal banking agencies' and FinCEN's commitment to provide guidance that assists banks in complying with the BSA remains a high supervisory priority.

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

As part of a strong BSA/AML compliance program, the federal banking agencies seek to ensure that a bank has policies, procedures, and processes to identify and report suspicious transactions to law enforcement. The agencies' supervisory processes assess whether banks have established the appropriate policies, procedures, and processes based on their BSA/AML risk to identify and report suspicious activity and that they provide

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

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

sufficient detail in reports to law enforcement agencies to make the reports useful for investigating suspicious transactions that are reported. Refer to Appendices B ("BSA/AML Directives") and C ("BSA/AML References") for guidance.

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

OFAC

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

OFAC requirements are separate and distinct from the BSA, but both OFAC and the BSA share a common national security goal. For this reason, many financial institutions view compliance with OFAC sanctions as related to BSA compliance obligations; supervisory examination for BSA compliance is logically connected to the examination of a financial institution's compliance with OFAC sanctions. Refer to the core overview and examination procedures, "Office of Foreign Assets Control," pages 147 to 156 and 157 to 159, respectively, for guidance.

Money Laundering and Terrorist Financing

The BSA is intended to safeguard the U.S. financial system and the financial institutions that make up that system from the abuses of financial crime, including money laundering, terrorist financing, and other illicit financial transactions. Money laundering and terrorist financing are financial crimes with potentially devastating social and financial effects. From the profits of the narcotics trafficker to the assets looted from government coffers by dishonest foreign officials, criminal proceeds have the power to corrupt and ultimately destabilize communities or entire economies. Terrorist networks are able to facilitate their activities if they have financial means and access to the financial system. In both money laundering and terrorist financing, criminals can exploit loopholes and other weaknesses in the legitimate financial system to launder criminal proceeds, finance terrorism, or conduct other illegal activities, and, ultimately, hide the actual purpose of their activity.

[9] Refer to Appendix R for additional information.

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

Money Laundering

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

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

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

Integration. The ultimate goal of the money laundering process is integration. Once the funds are in the financial system and insulated through the layering stage, the integration stage is used to create the appearance of legality through additional transactions. These transactions further shield the criminal from a recorded connection to the funds by providing a plausible explanation for the source of the funds. Examples include the purchase and resale of real estate, investment securities, foreign trusts, or other assets.

Terrorist Financing

The motivation behind terrorist financing is ideological as opposed to profit-seeking, which is generally the motivation for most crimes associated with money laundering. Terrorism is intended to intimidate a population or to compel a government or an international organization to do or abstain from doing any specific act through the threat of violence. An effective financial infrastructure is critical to terrorist operations.

Terrorist groups develop sources of funding that are relatively mobile to ensure that funds can be used to obtain material and other logistical items needed to commit terrorist acts. Thus, money laundering is often a vital component of terrorist financing.

Terrorists generally finance their activities through both unlawful and legitimate sources. Unlawful activities, such as extortion, kidnapping, and narcotics trafficking, have been found to be a major source of funding. Other observed activities include smuggling, fraud, theft, robbery, identity theft, use of conflict diamonds,[10] and improper use of charitable or relief funds. In the last case, donors may have no knowledge that their donations have been diverted to support terrorist causes.

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

Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to those methods used by other criminals that launder funds. For example, terrorist financiers use currency smuggling, structured deposits or withdrawals from bank accounts; purchases of various types of monetary instruments; credit, debit, or prepaid cards; and funds transfers. There is also evidence that some forms of informal banking (e.g., "hawala"[11]) have played a role in moving terrorist funds. Transactions through hawalas are difficult to detect given the lack of documentation, their size, and the nature of the transactions involved. Funding for terrorist attacks does not always require large sums of money, and the associated transactions may not be complex.

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

Penalties for money laundering and terrorist financing can be severe. A person convicted of money laundering can face up to 20 years in prison and a fine of up to $500,000.[12] Any property involved in a transaction or traceable to the proceeds of the criminal activity,

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

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

[12] 18 USC 1956.

including property such as loan collateral, personal property, and, under certain conditions, entire bank accounts (even if some of the money in the account is legitimate), may be subject to forfeiture. Pursuant to various statutes, banks and individuals may incur criminal and civil liability for violating AML and terrorist financing laws. For instance, pursuant to 18 USC 1956 and 1957, the U.S. Department of Justice may bring criminal actions for money laundering that may include criminal fines, imprisonment, and forfeiture actions.[13] In addition, banks risk losing their charters, and bank employees risk being removed and barred from banking.

Moreover, there are criminal penalties for willful violations of the BSA and its implementing regulations under 31 USC 5322 and for structuring transactions to evade BSA reporting requirements under 31 USC 5324(d). For example, a person, including a bank employee, willfully violating the BSA or its implementing regulations is subject to a criminal fine of up to $250,000 or five years in prison, or both.[14] A person who commits such a violation while violating another U.S. law, or engaging in a pattern of criminal activity, is subject to a fine of up to $500,000 or ten years in prison, or both.[15] A bank that violates certain BSA provisions, including 31 USC 5318(i) or (j), or special measures imposed under 31 USC 5318A, faces criminal money penalties up to the greater of $1 million or twice the value of the transaction.[16]

Civil Penalties for Violations of the BSA

Pursuant to 12 USC 1818(i) and 1786(k), and 31 USC 5321, the federal banking agencies and FinCEN, respectively, can bring civil money penalty actions for violations of the BSA. Moreover, in addition to criminal and civil money penalty actions taken against them, individuals may be removed from banking pursuant to 12 USC 1818(e)(2) for a violation of the AML laws under Title 31 of the U.S. Code, as long as the violation was not inadvertent or unintentional. All of these actions are publicly available.

---

[13] 18 USC 981 and 982.

[14] 31 USC 5322(a).

[15] *Id.*

[16] *Id.*

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

Scoping and Planning — Overview

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

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

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

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

Review of the Bank's BSA/AML Risk Assessment

The scoping and planning process should be guided by the examiner's review of the bank's BSA/AML risk assessment. Information gained from the examiner's review of the risk assessment will assist the scoping and planning process as well as the evaluation of the adequacy of the BSA/AML compliance program. If the bank has not developed a risk assessment, this fact should be discussed with management. For the purposes of the examination, whenever the bank has not completed a risk assessment, or the risk assessment is inadequate, the examiner must complete a risk assessment. Refer to the core overview section, "BSA/AML Risk Assessment," pages 22 to 30, for guidance on

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

Independent Testing

As part of the scoping and planning process, examiners should obtain and evaluate the supporting documents of the independent testing (audit)[17] of the bank's BSA/AML compliance program. The scope and quality of the audit may provide examiners with a sense of particular risks in the bank, how these risks are being managed and controlled, and the status of compliance with the BSA. The independent testing scope and workpapers can assist examiners in understanding the audit coverage and the quality and quantity of transaction testing. This knowledge will assist the examiner in determining the examination scope, identifying areas requiring greater (or lesser) scrutiny, and identifying when expanded examination procedures may be necessary.

Examination Plan

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

- Scoping and Planning (refer to pages 19 to 21).
- BSA/AML Risk Assessment (refer to page 31).
- BSA/AML Compliance Program (refer to pages 38 to 43).
- Developing Conclusions and Finalizing the Examination (refer to pages 48 to 51).

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

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

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

Transaction Testing

Examiners perform transaction testing to evaluate the adequacy of the bank's compliance with regulatory requirements, determine the effectiveness of its policies, procedures, and processes, and evaluate suspicious activity monitoring systems. Transaction testing is an important factor in forming conclusions about the integrity of the bank's overall controls and risk management processes. Transaction testing must be performed at each examination and should be risk-based. Transaction testing can be performed either through conducting the transaction testing procedures within the independent testing (audit) section (refer to the core examination procedures, "BSA/AML Compliance Program," pages 38 to 43, for further guidance) or completing the transaction testing procedures contained elsewhere within the core or expanded sections.

The extent of transaction testing and activities conducted is based on various factors including the examiner's judgment of risks, controls, and the adequacy of the independent testing. Once on site, the scope of the transaction testing can be expanded to address any issues or concerns identified during the examination. Examiners should document their decision regarding the extent of transaction testing to conduct, the activities for which it is to be performed, and the rationale for any changes to the scope of transaction testing that occur during the examination.

Information Available From BSA-Reporting Database

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

another bank, the examiner should obtain SARs, CTRs, and CTR exemptions data on the acquired bank, as well.

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

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

Examination Procedures

Scoping and Planning

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

BSA/AML Risk Assessment — Overview

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

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

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

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

The development of the BSA/AML risk assessment generally involves two steps: first, identify the specific risk categories (i.e., products, services, customers, entities, transactions, and geographic locations) unique to the bank; and second, conduct a more detailed analysis of the data identified to better assess the risk within these categories. In reviewing the risk assessment during the scoping and planning process, the examiner should determine whether management has considered all products, services, customers, entities, transactions, and geographic locations, and whether management's detailed analysis within these specific risk categories was adequate. If the bank has not developed a risk assessment, this fact should be discussed with management. For the purposes of the examination, whenever the bank has not completed a risk assessment, or the risk assessment is inadequate, the examiner must complete a risk assessment based on available information.[18]

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

Evaluating the Bank's BSA/AML Risk Assessment

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

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

Identification of Specific Risk Categories

The first step of the risk assessment process is to identify the specific products, services, customers, entities, and geographic locations unique to the bank. Although attempts to launder money, finance terrorism, or conduct other illegal activities through a bank can emanate from many different sources, certain products, services, customers, entities, and geographic locations may be more vulnerable or have been historically abused by money launderers and criminals. Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same. Various factors, such as the number and volume of transactions, geographic locations, and nature of the customer relationships, should be considered when the bank prepares its risk assessment. The differences in the way a bank interacts with the customer (face-to-face contact versus electronic banking) also should be considered. Because of these factors, risks will vary from one bank to another. In reviewing the bank's risk assessment, examiners should determine whether management has developed an accurate risk assessment that identifies the significant risks to the bank.

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

Products and Services

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

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

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

Customers and Entities

Although any type of account is potentially vulnerable to money laundering or terrorist financing, by the nature of their business, occupation, or anticipated transaction activity, certain customers and entities may pose specific risks. At this stage of the risk assessment process, it is essential that banks exercise judgment and neither define nor

[19] Monetary instruments in this context include official bank checks, cashier's checks, money orders, and traveler's checks. Refer to the expanded overview section, "Purchase and Sale of Monetary Instruments," pages 243 to 245, for further discussion on risk factors and risk mitigation regarding monetary instruments.

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

- Foreign financial institutions, including banks and foreign money services providers (e.g., casas de cambio, currency exchanges, and money transmitters).
- Nonbank financial institutions (e.g., money services businesses; casinos and card clubs; brokers/dealers in securities; and dealers in precious metals, stones, or jewels).
- Senior foreign political figures and their immediate family members and close associates (collectively known as politically exposed persons (PEP)).[20]
- Nonresident alien (NRA)[21] and accounts of foreign individuals.
- Foreign corporations and domestic business entities, particularly offshore corporations (such as domestic shell companies and Private Investment Companies (PIC) and international business corporations (IBC))[22] located in higher-risk geographic locations.
- Deposit brokers, particularly foreign deposit brokers.
- Cash-intensive businesses (e.g., convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATMs, vending machine operators, and parking garages).
- Nongovernmental organizations and charities (foreign and domestic).
- Professional service providers (e.g., attorneys, accountants, doctors, or real estate brokers).

Geographic Locations

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

---

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

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

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

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

- Countries subject to OFAC sanctions, including state sponsors of terrorism.[23]
- Countries identified as supporting international terrorism under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State.[24]
- Jurisdictions determined to be "of primary money laundering concern" by the Secretary of the Treasury, and jurisdictions subject to special measures imposed by the Secretary of the Treasury, through FinCEN, pursuant to section 311 of the USA PATRIOT Act.[25]
- Jurisdictions or countries monitored for deficiencies in their regimes to combat money laundering and terrorist financing by international entities such as the Financial Action Task Force (FATF).
- Major money laundering countries and jurisdictions identified in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR), in particular, countries which are identified as jurisdictions of primary concern.[26]
- Offshore financial centers (OFC).[27]
- Other countries identified by the bank as higher-risk because of its prior experiences or other factors (e.g., legal considerations, or allegations of official corruption).
- Domestic higher-risk geographic locations may include, but are not limited to, banking offices doing business within, or having customers located within, a U.S. government-designated higher-risk geographic location. Domestic higher-risk geographic locations include:
    - High Intensity Drug Trafficking Areas (HIDTA).[28]

---

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

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

[25] Notices of proposed rulemaking and final rules accompanying the determination "of primary money laundering concern," and imposition of a special measure (or measures) pursuant to section 311 of the USA PATRIOT Act are available on the FinCEN Web site: www.fincen.gov/reg_section311.html.

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

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

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

Analysis of Specific Risk Categories

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

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

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

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

---

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

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

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

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

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

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

Consolidated BSA/AML Compliance Risk Assessment

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

Bank's Updating of the Risk Assessment

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

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

Examiner Development of a BSA/AML Risk Assessment

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

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

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

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

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

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

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

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

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

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

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

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

Examination Procedures

BSA/AML Risk Assessment

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

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

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

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

BSA/AML Compliance Program — Overview

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

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

The BSA/AML compliance program[30] must be written, approved by the board of directors,[31] and noted in the board minutes. A bank must have a BSA/AML compliance program commensurate with its respective BSA/AML risk profile. Refer to the core overview section, "BSA/AML Risk Assessment," pages 22 to 30, for additional guidance on developing a BSA/AML risk assessment. Refer to Appendix I ("Risk Assessment Link to the BSA/AML Compliance Program") for a chart depicting the risk assessment's link to the BSA/AML compliance program. Furthermore, the BSA/AML compliance program must be fully implemented and reasonably designed to meet the BSA requirements.[32] Policy statements alone are not sufficient; practices must coincide with the bank's written policies, procedures, and processes. The BSA/AML compliance program must provide for the following minimum requirements:

- A system of internal controls to ensure ongoing compliance.

---

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

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

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

- Independent testing of BSA/AML compliance.
- Designate an individual or individuals responsible for managing BSA compliance (BSA compliance officer).
- Training for appropriate personnel.

In addition, a CIP must be included as part of the BSA/AML compliance program. Refer to the core overview section, "Customer Identification Program," pages 52 to 58, for additional guidance.

Internal Controls

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

Internal controls should:

- Identify banking operations (i.e., products, services, customers, entities, and geographic locations) more vulnerable to abuse by money launderers and criminals; provide for periodic updates to the bank's risk profile; and provide for a BSA/AML compliance program tailored to manage risks.
- Inform the board of directors, or a committee thereof, and senior management, of compliance initiatives, identified compliance deficiencies, and corrective action taken, and notify directors and senior management of SARs filed.
- Identify a person or persons responsible for BSA/AML compliance.
- Provide for program continuity despite changes in management or employee composition or structure.
- Meet all regulatory recordkeeping and reporting requirements, meet recommendations for BSA/AML compliance, and provide for timely updates in response to changes in regulations.[33]

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

- Implement risk-based CDD policies, procedures, and processes.
- Identify reportable transactions and accurately file all required reports including SARs, CTRs, and CTR exemptions. (Banks should consider centralizing the review and report-filing functions within the banking organization.)
- Provide for dual controls and the segregation of duties to the extent possible. For example, employees that complete the reporting forms (such as SARs, CTRs, and CTR exemptions) generally should not also be responsible for the decision to file the reports or grant the exemptions.
- Provide sufficient controls and systems for filing CTRs and CTR exemptions.
- Provide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity.
- Provide for adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity covered by the BSA and its implementing regulations.
- Incorporate BSA compliance into the job descriptions and performance evaluations of bank personnel, as appropriate.
- Train employees to be aware of their responsibilities under the BSA regulations and internal policy guidelines.

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

Independent Testing

Independent testing (audit) should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties. While the frequency of audit is not specifically defined in any statute, a sound practice is for the bank to conduct independent testing generally every 12 to 18 months, commensurate with the BSA/AML risk profile of the bank. Banks that do not employ outside auditors or consultants or have internal audit departments may comply with this requirement by using qualified persons who are not involved in the function being tested. The persons conducting the BSA/AML testing should report directly to the board of directors or to a designated board committee comprised primarily or completely of outside directors.

Those persons responsible for conducting an objective independent evaluation of the written BSA/AML compliance program should perform testing for specific compliance with the BSA, and evaluate pertinent management information systems (MIS). The audit should be risk based and evaluate the quality of risk management for all banking operations, departments, and subsidiaries. Risk-based audit programs will vary depending on the bank's size, complexity, scope of activities, risk profile, quality of

control functions, geographic diversity, and use of technology. An effective risk-based auditing program will cover all of the bank's activities. The frequency and depth of each activity's audit will vary according to the activity's risk assessment. Risk-based auditing enables the board of directors and auditors to use the bank's risk assessment to focus the audit scope on the areas of greatest concern. The testing should assist the board of directors and management in identifying areas of weakness or areas where there is a need for enhancements or stronger controls.

Independent testing should, at a minimum, include:

- An evaluation of the overall adequacy and effectiveness of the BSA/AML compliance program, including policies, procedures, and processes. Typically, this evaluation will include an explicit statement about the BSA/AML compliance program's overall adequacy and effectiveness and compliance with applicable regulatory requirements. At the very least, the audit should contain sufficient information for the reviewer (e.g., an examiner, review auditor, or BSA officer) to reach a conclusion about the overall quality of the BSA/AML compliance program.
- A review of the bank's risk assessment for reasonableness given the bank's risk profile (products, services, customers, entities, and geographic locations).
- Appropriate risk-based transaction testing to verify the bank's adherence to the BSA recordkeeping and reporting requirements (e.g., CIP, SARs, CTRs and CTR exemptions, and information sharing requests).
- An evaluation of management's efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations, including progress in addressing outstanding supervisory actions, if applicable.
- A review of staff training for adequacy, accuracy, and completeness.
- A review of the effectiveness of the suspicious activity monitoring systems (manual, automated, or a combination) used for BSA/AML compliance. Related reports may include, but are not limited to:
  - Suspicious activity monitoring reports.
  - Large currency aggregation reports.
  - Monetary instrument records.
  - Funds transfer records.
  - Nonsufficient funds (NSF) reports.
  - Large balance fluctuation reports.
  - Account relationship reports.

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

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

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

BSA Compliance Officer

The bank's board of directors must designate a qualified individual to serve as the BSA compliance officer.[34] The BSA compliance officer is responsible for coordinating and monitoring day-to-day BSA/AML compliance. The BSA compliance officer is also charged with managing all aspects of the BSA/AML compliance program and with managing the bank's adherence to the BSA and its implementing regulations; however, the board of directors is ultimately responsible for the bank's BSA/AML compliance.

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

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

---

[34] The bank must designate one or more persons to coordinate and monitor day-to-day compliance. This requirement is detailed in the federal banking agencies' BSA compliance program regulations: 12 CFR 208.63, 12 CFR 211.5(m), and 12 CFR 211.24(j) (Board of Governors of the Federal Reserve System); 12 CFR 326.8 (Federal Deposit Insurance Corporation); 12 CFR 748.2 (National Credit Union Administration); 12 CFR 21.21 (Office of the Comptroller of the Currency); and 12 CFR 563.177 (Office of Thrift Supervision).

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

Training

Banks must ensure that appropriate personnel are trained in applicable aspects of the BSA. Training should include regulatory requirements and the bank's internal BSA/AML policies, procedures, and processes. At a minimum, the bank's training program must provide training for all personnel whose duties require knowledge of the BSA. The training should be tailored to the person's specific responsibilities. In addition, an overview of the BSA/AML requirements typically should be given to new staff during employee orientation. Training should encompass information related to applicable business lines, such as trust services, international, and private banking. The BSA compliance officer should receive periodic training that is relevant and appropriate given changes to regulatory requirements as well as the activities and overall BSA/AML risk profile of the bank.

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

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

Examples of money laundering activity and suspicious activity monitoring and reporting can and should be tailored to each individual audience. For example, training for tellers should focus on examples involving large currency transactions or other suspicious activities; training for the loan department should provide examples involving money laundering through lending arrangements.

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

Examination Procedures

BSA/AML Compliance Program

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

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

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

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

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

---

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

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

Risk Assessment Link to the BSA/AML Compliance Program

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

Internal Controls

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

   - Identify higher-risk banking operations (products, services, customers, entities, and geographic locations); provide for periodic updates to the bank's risk profile; and provide for a BSA/AML compliance program tailored to manage risks.
   - Inform the board of directors, or a committee thereof, and senior management, of compliance initiatives, identified compliance deficiencies, SARs filed, and corrective action taken.
   - Identify a person or persons responsible for BSA/AML compliance.
   - Provide for program continuity despite changes in management or employee composition or structure.
   - Meet all regulatory requirements, meet recommendations for BSA/AML compliance, and provide for timely updates to implement changes in regulations.
   - Implement risk-based CDD policies, procedures, and processes.
   - Identify reportable transactions and accurately file all required reports, including SARs, CTRs, and CTR exemptions. (Banks should consider centralizing the review and report-filing functions within the banking organization.)
   - Provide for dual controls and the segregation of duties to the extent possible. For example, employees that complete the reporting forms (such as SARs, CTRs, and CTR exemptions) generally should not also be responsible for the decision to file the reports or grant the exemptions.
   - Provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity.
   - Provide for adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity covered by the BSA and its implementing regulations.

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

Independent Testing

5. Determine whether the BSA/AML testing (audit) is independent (i.e., performed by a person (or persons) not involved with the bank's BSA/AML compliance staff) and whether persons conducting the testing report directly to the board of directors or to a designated board committee comprised primarily or completely of outside directors.
6. Evaluate the qualifications of the person (or persons) performing the independent testing to assess whether the bank can rely upon the findings and conclusions.
7. Validate the auditor's reports and workpapers to determine whether the bank's independent testing is comprehensive, accurate, adequate, and timely. The independent test should address the following:
   - The overall adequacy and effectiveness of the BSA/AML compliance program, including policies, procedures, and processes. Typically, this evaluation will include an explicit statement about the BSA/AML compliance program's overall adequacy and effectiveness and compliance with applicable regulatory requirements. At the very least, the audit should contain sufficient information for the reviewer (e.g., an examiner, review auditor, or BSA officer) to reach a conclusion about the overall quality of the BSA/AML compliance program.
   - BSA/AML risk assessment.
   - BSA reporting and recordkeeping requirements.
   - CIP implementation.
   - CDD policies, procedures, and processes and whether they comply with internal requirements.
   - Personnel adherence to the bank's BSA/AML policies, procedures, and processes.
   - Appropriate transaction testing, with particular emphasis on higher-risk operations (products, services, customers, and geographic locations).
   - Training, including its comprehensiveness, accuracy of materials, the training schedule, and attendance tracking.
   - The integrity and accuracy of MIS used in the BSA/AML compliance program. MIS includes reports used to identify large currency transactions, aggregate daily currency transactions, funds transfer transactions, monetary instrument sales transactions, and analytical and trend reports.

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

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

BSA Compliance Officer

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

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

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

Training

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

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

Transaction Testing

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

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

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

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

Independent Testing

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

Preliminary Evaluation

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

Developing Conclusions and Finalizing the Examination — Overview

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

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

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

Systemic or Recurring Violations

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Isolated or Technical Violations

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

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

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

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

[39] Interagency Enforcement Statement, page 6.

- Failure to obtain or verify required customer identification information that is infrequent, not consistent, or nonrecurring.
- Failure to complete a 314(a) information request that is inadvertent or nonrecurring.

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

Examination Procedures

Developing Conclusions and Finalizing the Examination

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

Formulating Conclusions

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

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

   All relevant determinations should be documented and explained.

Determine the Underlying Cause

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

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

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

Discuss Findings With Examiner in Charge and Identify Necessary Action

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

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

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

Preparing the BSA/AML Comments for the Report of Examination

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

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

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

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

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

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

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

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

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

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

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

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

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

    .

CORE EXAMINATION OVERVIEW AND PROCEDURES FOR REGULATORY REQUIREMENTS AND RELATED TOPICS

Customer Identification Program — Overview

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

All banks must have a written CIP.[40] The CIP rule implements section 326 of the USA PATRIOT Act and requires each bank to implement a written CIP that is appropriate for its size and type of business and that includes certain minimum requirements. The CIP must be incorporated into the bank's BSA/AML compliance program, which is subject to approval by the bank's board of directors.[41] The implementation of a CIP by subsidiaries of banks is appropriate as a matter of safety and soundness and protection from reputational risks. Domestic subsidiaries (other than functionally regulated subsidiaries subject to separate CIP rules) of banks should comply with the CIP rule that applies to the parent bank when opening an account within the meaning of 31 CFR 103.121.[42]

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

- The types of accounts offered by the bank.

---

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

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

[42] *Frequently Asked Questions Related to Customer Identification Program Rules* issued by FinCEN, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision, April 28, 2005.

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

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

An account does not include:

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

The CIP rule applies to a "customer." A customer is a "person" (an individual, a corporation, partnership, a trust, an estate, or any other entity recognized as a legal person) who opens a new account, an individual who opens a new account for another individual who lacks legal capacity, and an individual who opens a new account for an entity that is not a legal person (e.g., a civic club). A customer does not include a person who does not receive banking services, such as a person whose loan application is denied.[43] The definition of "customer" also does not include an existing customer as long as the bank has a reasonable belief that it knows the customer's true identity.[44] Excluded from the definition of customer are federally regulated banks, banks regulated by a state bank regulator, governmental entities, and publicly traded companies (as described in 31 CFR 103.22(d)(2)(ii) through (iv)).

---

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

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

Customer Information Required

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

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

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

Customer Verification

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

---

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

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

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

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

Verification Through Documents

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

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

Verification Through Nondocumentary Methods

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

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

Additional Verification for Certain Customers

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

identity of a sole proprietor or the principals in a partnership when the bank cannot otherwise satisfactorily identify the sole proprietorship or the partnership.

Lack of Verification

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

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

Recordkeeping and Retention Requirements

A bank's CIP must include recordkeeping procedures. At a minimum, the bank must retain the identifying information (name, address, date of birth for an individual, TIN, and any other information required by the CIP) obtained at account opening for a period of five years after the account is closed.[49] For credit cards, the retention period is five years after the account closes or becomes dormant.

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

- Any document that was relied on to verify identity, noting the type of document, the identification number, the place of issuance, and, if any, the date of issuance and expiration date.

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

- The method and the results of any measures undertaken to verify identity.
- The results of any substantive discrepancy discovered when verifying identity.

Comparison With Government Lists

The CIP must include procedures for determining whether the customer appears on any federal government list of known or suspected terrorists or terrorist organizations.[50] Banks will be contacted by the U.S. Treasury in consultation with their federal banking agency when a list is issued. At such time, banks must compare customer names against the list within a reasonable time of account opening or earlier, if required by the government, and they must follow any directives that accompany the list.

Adequate Customer Notice

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

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

Reliance on Another Financial Institution

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

- The relied-upon financial institution is subject to a rule implementing the AML program requirements of 31 USC 5318(h) and is regulated by a federal functional regulator.[51]

---

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

[51] Federal functional regulator means: Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; National Credit Union Administration; Office of the Comptroller of the Currency;

- The customer has an account or is opening an account at the bank and at the other functionally regulated institution.
- Reliance is reasonable, under the circumstances.
- The other financial institution enters into a contract requiring it to certify annually to the bank that it has implemented its AML program, and that it will perform (or its agent will perform) the specified requirements of the bank's CIP.

Use of Third Parties

The CIP rule does not alter a bank's authority to use a third party, such as an agent or service provider, to perform services on its behalf. Therefore, a bank is permitted to arrange for a third party, such as a car dealer or mortgage broker, acting as its agent in connection with a loan, to verify the identity of its customer. The bank can also arrange for a third party to maintain its records. However, as with any other responsibility performed by a third party, the bank is ultimately responsible for that third party's compliance with the requirements of the bank's CIP. As a result, banks should establish adequate controls and review procedures for such relationships. This requirement contrasts with the reliance provision of the rule that permits the relied-upon party to take responsibility. Refer to "Reliance on Another Financial Institution," pages 57 to 58.

Other Legal Requirements

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

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

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

Examination Procedures

Customer Identification Program

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

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

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

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

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

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

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

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

Transaction Testing

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

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

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

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

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

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

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

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

Customer Due Diligence — Overview

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

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

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

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

Customer Due Diligence Guidance

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

- Are commensurate with the bank's BSA/AML risk profile, paying particular attention to higher-risk customers.
- Contain a clear statement of management's overall expectations and establish specific staff responsibilities, including who is responsible for reviewing or approving changes to a customer's risk rating or profile, as applicable.
- Ensure that the bank possesses sufficient customer information to implement an effective suspicious activity monitoring system.

- Provide guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.

- Ensure the bank maintains current customer information.

Customer Risk

Management should have a thorough understanding of the money laundering or terrorist financing risks of the bank's customer base. Under this approach, the bank should obtain information at account opening sufficient to develop an understanding of normal and expected activity for the customer's occupation or business operations. This understanding may be based on account type or customer classification. For additional guidance, refer to Appendix K ("Customer Risk versus Due Diligence and Suspicious Activity Monitoring").

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

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

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

Enhanced Due Diligence for Higher-Risk Customers

Customers that pose higher money laundering or terrorist financing risks present increased exposure to banks; due diligence policies, procedures, and processes should be enhanced as a result. Enhanced due diligence (EDD) for higher-risk customers is especially critical in understanding their anticipated transactions and implementing a suspicious activity monitoring system that reduces the bank's reputation, compliance, and transaction risks. Higher-risk customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the bank. Guidance for identifying higher-risk customers may be found in the core overview section, "BSA/AML Risk Assessment," pages 22 to 30.

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

transactions, including those transactions involving higher-risk jurisdictions. If so, the bank should consider obtaining, both at account opening and throughout the relationship, the following information on the customer:

- Purpose of the account.
- Source of funds and wealth.
- Individuals with ownership or control over the account, such as beneficial owners, signatories, or guarantors.
- Occupation or type of business (of customer or other individuals with ownership or control over the account).
- Financial statements.
- Banking references.
- Domicile (where the business is organized).
- Proximity of the customer's residence, place of employment, or place of business to the bank.
- Description of the customer's primary trade area and whether international transactions are expected to be routine.
- Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers.
- Explanations for changes in account activity.

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

Examination Procedures

Customer Due Diligence

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

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

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

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

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

Transaction Testing

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

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

Suspicious Activity Reporting — Overview

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

Suspicious activity reporting forms the cornerstone of the BSA reporting system. It is critical to the United States' ability to utilize financial information to combat terrorism, terrorist financing, money laundering, and other financial crimes. Examiners and banks should recognize that the quality of SAR content is critical to the adequacy and effectiveness of the suspicious activity reporting system.

Within this system, FinCEN and the federal banking agencies recognize that, as a practical matter, it is not possible for a bank to detect and report all potentially illicit transactions that flow through the bank. Examiners should focus on evaluating a bank's policies, procedures, and processes to identify, evaluate, and report suspicious activity. However, as part of the examination process, examiners should review individual SAR filing decisions to determine the effectiveness of the bank's suspicious activity identification, evaluation, and reporting process. Banks, bank holding companies, and their subsidiaries are required by federal regulations[53] to file a SAR with respect to:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating $5,000 or more when a suspect can be identified.
- Criminal violations aggregating $25,000 or more regardless of a potential suspect.
- Transactions conducted or attempted by, at, or through the bank (or an affiliate) and aggregating $5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect that the transaction:
  - May involve potential money laundering or other illegal activity (e.g., terrorism financing).
  - Is designed to evade the BSA or its implementing regulations.[54]
  - Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

[53] Refer to 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Board of Governors of the Federal Reserve System); 12 CFR 353 (Federal Deposit Insurance Corporation); 12 CFR 748 (National Credit Union Administration); 12 CFR 21.11 (Office of the Comptroller of the Currency); 12 CFR 563.180 (Office of Thrift Supervision) and 31 CFR 103.18 (FinCEN).

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

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

Safe Harbor for Banks From Civil Liability for Suspicious Activity Reporting

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

Systems to Identify, Research, and Report Suspicious Activity

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

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

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

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

Identification of Unusual Activity

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

Employee Identification

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

Law Enforcement Inquiries and Requests

Banks should establish policies, procedures, and processes for identifying subjects of law enforcement requests, monitoring the transaction activity of those subjects when appropriate, identifying unusual or potentially suspicious activity related to those subjects, and filing, as appropriate, SARs related to those subjects. Law enforcement

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

Mere receipt of any law enforcement inquiry does not, by itself, require the filing of a SAR by the bank. Nonetheless, a law enforcement inquiry may be relevant to a bank's overall risk assessment of its customers and accounts. For example, the receipt of a grand jury subpoena should cause a bank to review account activity for the relevant customer.[56] A bank should assess all of the information it knows about its customer, including the receipt of a law enforcement inquiry, in accordance with its risk-based BSA/AML compliance program.

The bank should determine whether a SAR should be filed based on all customer information available. Due to the confidentiality of grand jury proceedings, if a bank files a SAR after receiving a grand jury subpoena, law enforcement discourages banks from including any reference to the receipt or existence of the grand jury subpoena in the SAR. Rather, the SAR should reference only those facts and activities that support a finding of suspicious transactions identified by the bank.

National Security Letters

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

- Telephone and electronic communications records from telephone companies and Internet service providers.[57]
- Information from credit bureaus.[58]
- Financial records from financial institutions.[59]

NSLs are highly confidential documents; for that reason, examiners will not review or sample specific NSLs.[60] Pursuant to 12 USC 3414(a)(3) and (5)(D), no bank, or officer, employee or agent of the institution, can disclose to any person that a government authority or the FBI has sought or obtained access to records through a Right to Financial Privacy Act NSL. Banks that receive NSLs must take appropriate measures to ensure the

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

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

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

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

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

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

confidentiality of the letters and should have procedures in place for processing and maintaining the confidentiality of NSLs.

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

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

Transaction Monitoring (Manual Transaction Monitoring)

A transaction monitoring system, sometimes referred to as a manual transaction monitoring system, typically targets specific types of transactions (e.g., those involving large amounts of cash, those to or from foreign geographies) and includes a manual review of various reports generated by the bank's MIS or vendor systems in order to identify unusual activity. Examples of MIS reports include currency activity reports, funds transfer reports, monetary instrument sales reports, large item reports, significant balance change reports, and nonsufficient funds (NSF) reports. Many MIS or vendor systems include filtering models for identification of potentially unusual activity. The process may involve review of daily reports, reports that cover a period of time (e.g., rolling 30-day reports, monthly reports), or a combination of both types of reports. The type and frequency of reviews and resulting reports used should be commensurate with the bank's BSA/AML risk profile and appropriately cover its higher-risk products, services, customers, entities, and geographic locations.

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

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

- Currency activity including multiple transactions greater than $10,000.
- Currency activity (single and multiple transactions) below the $10,000 reporting requirement (e.g., between $7,000 and $10,000).

- Currency transactions involving multiple lower dollar transactions (e.g., $3,000) that over a period of time (e.g., 15 days) aggregate to a substantial sum of money (e.g., $30,000).

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

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

Funds transfer records. The BSA requires banks to maintain records of funds transfer in amounts of $3,000 and above. Periodic review of this information can assist banks in identifying patterns of unusual activity. A periodic review of the funds transfer records in banks with low funds transfer activity is usually sufficient to identify unusual activity. For banks with more significant funds transfer activity, use of spreadsheet or vendor software is an efficient way to review funds transfer activity for unusual patterns. Most vendor software systems include standard suspicious activity filter reports. These reports typically focus on identifying certain higher-risk geographic locations and larger dollar funds transfer transactions for individuals and businesses. Each bank should establish its own filtering criteria for both individuals and businesses. Noncustomer funds transfer transactions and payable upon proper identification (PUPID) transactions should be reviewed for unusual activity. Activities identified during these reviews should be subjected to additional research to ensure that identified activity is consistent with the stated account purpose and expected activity. When inconsistencies are identified, banks may need to conduct a global relationship review to determine if a SAR is warranted.

Monetary instrument records. Records for monetary instrument sales are required by the BSA. Such records can assist the bank in identifying possible currency structuring through the purchase of cashier's checks, official bank checks, money orders, or traveler's checks in amounts of $3,000 to $10,000. A periodic review of these records can also help identify frequent purchasers of monetary instruments and common payees. Reviews for suspicious activity should encompass activity for an extended period of time (30, 60, 90 days) and should focus on, among other things, identification of commonalities, such as common payees and purchasers, or consecutively numbered purchased monetary instruments.

Surveillance Monitoring (Automated Account Monitoring)

A surveillance monitoring system, sometimes referred to as an automated account monitoring system, can cover multiple types of transactions and use various rules to identify potentially suspicious activity. In addition, many can adapt over time based on historical activity, trends, or internal peer comparison. These systems typically use computer programs, developed in-house or purchased from vendors, to identify individual transactions, patterns of unusual activity, or deviations from expected activity. These systems can capture a wide range of account activity, such as deposits, withdrawals, funds transfers, automated clearing house (ACH) transactions, and automated teller machine (ATM) transactions, directly from the bank's core data

processing system. Banks that are large, operate in many locations, or have a large volume of higher-risk customers typically use surveillance monitoring systems.

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

Intelligent systems are adaptive and can filter transactions, based on historical account activity or compare customer activity against a pre-established peer group or other relevant data. Intelligent systems review transactions in context with other transactions and the customer profile. In doing so, these systems increase their information database on the customer, account type, category, or business, as more transactions and data are stored in the system.

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

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

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

Managing Alerts

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

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

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

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

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

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

Identifying Underlying Crime

Banks are required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing,[61] and certain other crimes above prescribed dollar thresholds. However, banks are not obligated to investigate or confirm the underlying crime (e.g., terrorist financing, money laundering, tax evasion, identity theft, and various types of fraud). Investigation is the responsibility of law enforcement. When evaluating suspicious activity and completing the SAR, banks should, to the best of their ability, identify the characteristics of the suspicious activity. Part III, section 35, of the SAR provides 20 different characteristics of suspicious activity. Although an "Other" category is available, the use of this category should be limited to situations that cannot be broadly identified within the 20 characteristics provided.

SAR Decision Making

After thorough research and analysis has been completed, findings are typically forwarded to a final decision maker (individual or committee). The bank should have policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity. Within those procedures, management should establish a clear and defined escalation process from the point of initial detection to disposition of the investigation.

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

The decision to file a SAR is an inherently subjective judgment. Examiners should focus on whether the bank has an effective SAR decision-making process, not individual SAR

---

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

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

decisions. Examiners may review individual SAR decisions as a means to test the effectiveness of the SAR monitoring, reporting, and decision-making process. In those instances where the bank has an established SAR decision-making process, has followed existing policies, procedures, and processes, and has determined not to file a SAR, the bank should not be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.[63]

SAR Filing on Continuing Activity

One purpose of filing SARs is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. This objective is accomplished by the filing of a SAR that identifies the activity of concern. If this activity continues over a period of time, such information should be made known to law enforcement and the federal banking agencies. FinCEN's guidelines suggest that banks should report continuing suspicious activity by filing a report at least every 90 days.[64] This practice will notify law enforcement of the continuing nature of the activity in aggregate. In addition, this practice will remind the bank that it should continue to review the suspicious activity to determine whether other actions may be appropriate, such as bank management determining that it is necessary to terminate a relationship with the customer or employee that is the subject of the filing.

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

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

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

---

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

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

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

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

SAR Completion and Filing

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

Timing of a SAR Filing

The SAR rules require that a SAR be filed no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect can be identified, the time period for filing a SAR is extended to 60 days. Organizations may need to review transaction or account activity for a customer to determine whether to file a SAR. The need for a review of customer activity or transactions does not necessarily indicate a need to file a SAR. The time period for filing a SAR starts when the organization, during its review or because of other factors, knows or has reason to suspect that the activity or transactions under review meet one or more of the definitions of suspicious activity.[67]

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

Whenever possible, an expeditious review of the transaction or the account is recommended and can be of significant assistance to law enforcement. In any event, the

---

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

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

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

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

For situations requiring immediate attention, in addition to filing a timely SAR, a bank must immediately notify, by telephone, an "appropriate law enforcement authority" and, as necessary, the bank's primary regulator. For this initial notification, an "appropriate law enforcement authority" would generally be the local office of the IRS Criminal Investigation Division or the FBI. Notifying law enforcement of a suspicious activity does not relieve a bank of its obligation to file a SAR.[70]

SAR Quality

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

By their nature, SAR narratives are subjective, and examiners generally should not criticize the bank's interpretation of the facts. Nevertheless, banks should ensure that SAR narratives are complete, thoroughly describe the extent and nature of the suspicious activity, and are included within the SAR form (no attachments to the narrative section can be stored in the BSA-reporting database). More specific guidance is available in Appendix L ("SAR Quality Guidance") to assist banks in writing, and assist examiners in evaluating, SAR narratives. In addition, comprehensive guidance is available from FinCEN (e.g., "Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative," November 2003, and "Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting," October 2007) at www.fincen.gov/news_room/rp/sar_guidance.html.

---

[69] *Id*.

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

Notifying Board of Directors of SAR Filings

Banks are required by the SAR regulations of their federal banking agency to notify the board of directors or an appropriate board committee that SARs have been filed. However, the regulations do not mandate a particular notification format and banks should have flexibility in structuring their format. Therefore, banks may, but are not required to, provide actual copies of SARs to the board of directors or a board committee. Alternatively, banks may opt to provide summaries, tables of SARs filed for specific violation types, or other forms of notification. Regardless of the notification format used by the bank, management should provide sufficient information on its SAR filings to the board of directors or an appropriate committee in order to fulfill its fiduciary duties.[71]

SAR Record Retention and Supporting Documentation

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

Prohibition of SAR Disclosure

No bank, and no director, officer, employee, or agent of a bank that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. Thus, any person subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR, except when such disclosure is requested by FinCEN or an appropriate law enforcement[73] or federal banking agency, shall decline to produce

---

[71] As noted in the Bank Secrecy Act Advisory Group's *The SAR Activity Review — Trends, Tips & Issues*, Issue 2, June 2001, "In the rare instance when suspicious activity is related to an individual in the organization, such as the president or one of the members of the board of directors, the established policy that would require notification of a SAR filing to such an individual should not be followed. Deviations to established policies and procedures so as to avoid notification of a SAR filing to a subject of the SAR should be documented and appropriate uninvolved senior organizational personnel should be so advised." Refer to www.fincen.gov.

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

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

the SAR or to provide any information that would disclose that a SAR has been prepared or filed, citing 31 CFR 103.18(e) and 31 USC 5318(g)(2). FinCEN and the bank's federal banking agency should be notified of any such request and of the bank's response. Furthermore, FinCEN and the federal banking agencies take the position that banks' internal controls for the filing of SARs should minimize the risks of disclosure.

Sharing SARs With Head Offices and Controlling Companies

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

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

The guidance confirms that:

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

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

---

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

Examination Procedures

Suspicious Activity Reporting

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

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

Identification of Unusual Activity

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

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

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

Transaction (Manual Transaction) Monitoring

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

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

Surveillance (Automated Account) Monitoring

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

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

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

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

Managing Alerts

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

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

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

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

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

SAR Decision Making

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

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

SAR Completion and Filing

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

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

Transaction Testing

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

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

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

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

    - Suspicious activity monitoring reports.

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

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

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

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

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

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

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

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

Currency Transaction Reporting — Overview

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

A bank must file a Currency Transaction Report (CTR) (FinCEN Form 104) for each transaction in currency[76] (deposit, withdrawal, exchange, or other payment or transfer) of more than $10,000 by, through, or to the bank. Certain types of currency transactions need not be reported, such as those involving "exempt persons," a group which can include retail or commercial customers meeting specific criteria for exemption. Refer to the core overview section, "Currency Transaction Reporting Exemptions," pages 90 to 94, for further guidance.

Aggregation of Currency Transactions

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

Filing Time Frames and Record Retention Requirements

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

CTR Backfiling

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

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

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

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

Examination Procedures

Currency Transaction Reporting

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

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

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

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

Transaction Testing

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

   - CTRs are completed in accordance with FinCEN instructions.

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

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

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

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

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

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

Currency Transaction Reporting Exemptions — Overview

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

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

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

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

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

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

- A bank, to the extent of its domestic operations.
- A federal, state, or local government agency or department.
- Any entity exercising governmental authority within the United States.
- Any entity (other than a bank) whose common stock or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange or have been designated as a NASDAQ National Market Security listed on the NASDAQ Stock Market (with some exceptions).
- Any subsidiary (other than a bank) of any "listed entity" that is organized under U.S. law and at least 51 percent of whose common stock or analogous equity interest is owned by the listed entity.

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

Filing Time Frames

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

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

Annual Review

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

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

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

Non-Listed Businesses

A "non-listed business" is defined as a commercial enterprise to the extent of its domestic operations and only with respect to transactions conducted through its exemptible accounts and that: (i) has maintained a transaction account at the exempting bank for at least two months or prior to the passing of two months' time if the bank undertakes a risk-based analysis of that customer that allows it to form and document a reasonable belief that the customer has a legitimate business purpose for conducting frequent large currency transactions; (ii) frequently[79] engages in transactions in currency with the bank in excess of $10,000; and (iii) is incorporated or organized under the laws of the United

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

States or a state, or is registered as and eligible to do business within the United States or a state.

Ineligible Businesses

Certain businesses are ineligible for treatment as an exempt non-listed business (31 CFR 103.22(d)(5)(viii)). An ineligible business is defined as a business engaged primarily in one or more of the following specified activities:

- Serving as a financial institution or as agents for a financial institution of any type.
- Purchasing or selling motor vehicles of any kind, vessels, aircraft, farm equipment, or mobile homes.
- Practicing law, accounting, or medicine.
- Auctioning of goods.
- Chartering or operation of ships, buses, or aircraft.
- Operating a pawn brokerage.
- Engaging in gaming of any kind (other than licensed pari-mutuel betting at race tracks).
- Engaging in investment advisory services or investment banking services.
- Operating a real estate brokerage.
- Operating in title insurance activities and real estate closings.
- Engaging in trade union activities.
- Engaging in any other activity that may, from time to time, be specified by FinCEN.

A business that engages in multiple business activities may qualify for an exemption as a non-listed business as long as no more than 50 percent of its gross revenues per year[80] are derived from one or more of the ineligible business activities listed in the rule.

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

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

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

Payroll Customers

A "payroll customer" is defined solely with respect to withdrawals for payroll purposes from existing exemptible accounts and as a person who: (i) has maintained a transaction account at the bank for at least two months or prior to the passing of two months' time if the bank undertakes a risk-based analysis of that customer that allows it to form and document a reasonable belief that the customer has a legitimate business purpose for conducting frequent large currency transactions; (ii) operates a firm that regularly withdraws more than $10,000 in order to pay its U.S. employees in currency; and (iii) is incorporated or organized under the laws of the United States or a state, or is registered as and is eligible to do business within the United States or a state.

Filing Time Frames

After a bank has decided to exempt a Phase II customer, the bank must file a Designation of Exempt Person form with the IRS within 30 days after the first transaction in currency that the bank plans to exempt.

Annual Review

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

Safe Harbor for Failure to File CTRs

The rules (31 CFR 103.22(d)(7)) provide a safe harbor that a bank is not liable for the failure to file a CTR for a transaction in currency by an exempt person, unless the bank knowingly provides false or incomplete information or has reason to believe that the customer does not qualify as an exempt customer. In the absence of any specific knowledge or information indicating that a customer no longer meets the requirements of an exempt person, the bank is entitled to a safe harbor from civil penalties to the extent it

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

continues to treat that customer as an exempt customer until the date of the customer's annual review.

Effect on Other Regulatory Requirements

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

If a bank has improperly exempted accounts, it may formally revoke the exemption by filing FinCEN Form 110 and checking the "Exemption Revoked" box or informally revoke the exemption by filing CTRs on the customer. In either case, the bank should begin filing CTRs and should contact the IRS Enterprise Computing Center — Detroit (formerly the Detroit Computing Center)[82] to request a determination on whether the backfiling of unreported currency transactions is necessary.

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

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

Examination Procedures

Currency Transaction Reporting Exemptions

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

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

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

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

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

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

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

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

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

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

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

Transaction Testing

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

---

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

Information Sharing — Overview

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

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

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

A federal, state, local, or foreign[85] law enforcement agency investigating terrorist activity or money laundering may request that FinCEN solicit, on its behalf, certain information from a financial institution or a group of financial institutions. The law enforcement agency must provide a written certification to FinCEN attesting that there is credible evidence of engagement or reasonably suspected engagement in terrorist activity or money laundering for each individual, entity, or organization about which the law enforcement agency is seeking information. The law enforcement agency also must provide specific identifiers, such as a date of birth and address, which would permit a financial institution to differentiate among common or similar names. Upon receiving a completed written certification from a law enforcement agency, FinCEN may require a financial institution to search its records to determine whether it maintains or has maintained accounts for, or has engaged in transactions with, any specified individual, entity, or organization.

Search Requirements

Upon receiving an information request,[86] a financial institution must conduct a one-time search of its records to identify accounts or transactions of a named suspect. Unless otherwise instructed by an information request, financial institutions must search their records for current accounts, accounts maintained during the preceding 12 months, and transactions conducted outside of an account by or on behalf of a named suspect during the preceding six months. The financial institution must search its records and report any

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

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

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

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

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

FinCEN has provided financial institutions with General Instructions and Frequently Asked Questions (FAQ) relating to the section 314(a) process. Unless otherwise instructed by an information request, financial institutions must search the records specified in the General Instructions.[87] The General Instructions or FAQs are made available to the financial institutions on the SISS.[88]

If a financial institution identifies any account or transaction, it must report to FinCEN that it has a match. No details should be provided to FinCEN other than the fact that the financial institution has a match. A negative response is not required. A financial institution may provide the 314(a) subject lists to a third-party service provider or vendor to perform or facilitate record searches as long as the institution takes the necessary steps, through the use of an agreement or procedures, to ensure that the third party safeguards and maintains the confidentiality of the information.

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

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

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

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

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

Use Restrictions and Confidentiality

Financial institutions should develop and implement comprehensive policies, procedures, and processes for responding to section 314(a) requests. The regulation restricts the use of the information provided in a section 314(a) request (31 CFR 103.100(b)(2)(iv)). A financial institution may only use the information to report the required information to FinCEN, to determine whether to establish or maintain an account or engage in a transaction, or to assist in BSA/AML compliance. While the section 314(a) subject list could be used to determine whether to establish or maintain an account, FinCEN strongly discourages financial institutions from using this as the sole factor in reaching a decision to do so unless the request specifically states otherwise. Unlike the OFAC lists, section 314(a) subject lists are not permanent "watch lists." In fact, section 314(a) subject lists generally relate to one-time inquiries and are not updated or corrected if an investigation is dropped, a prosecution is declined, or a subject is exonerated. Further, the names do not correspond to convicted or indicted persons; rather a 314(a) subject need only be "reasonably suspected" based on credible evidence of engaging in terrorist acts or money laundering. Moreover, FinCEN advises that inclusion on a section 314(a) subject list should not be the sole factor used to determine whether to file a SAR. Financial institutions should establish a process for determining when and if a SAR should be filed. Refer to the core overview section, "Suspicious Activity Reporting," pages 67 to 80, for additional guidance.

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

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

---

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

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

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

Documentation

Additionally, documentation that all required searches were performed is essential. For those 314(a) subject lists received via facsimile prior to June 2, 2008, a bank may maintain copies of the cover page of the request with a financial institution sign-off that the records were checked, the date of the search, and search results (e.g., positive or negative). For positive matches with subject lists received via facsimile, copies of the form returned to FinCEN and the supporting documentation should be retained. For those institutions utilizing the Web-based 314(a) SISS, banks may print a search self-verification document for each 314(a) subject list transmission. Additionally, a Subject Response List can be printed for documentation purposes. The Subject Response List displays the total number of positive responses submitted to FinCEN for that transmission, the transmission date, the submitted date, and the tracking number and subject name that had the positive hit. If the financial institution elects to maintain copies of the section 314(a) requests, it should not be criticized for doing so, as long as it appropriately secures them and protects their confidentiality. Audits should include an evaluation of compliance with these guidelines within their scope.

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

---

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

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

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

Section 314(b) encourages financial institutions[92] and associations of financial institutions located in the United States to share information in order to identify and report activities that may involve terrorist activity or money laundering. Section 314(b) also provides specific protection from civil liability.[93] To avail itself of this statutory safe harbor from liability, a financial institution or an association must notify FinCEN of its intent to engage in information sharing and that it has established and will maintain adequate procedures to protect the security and confidentiality of the information. Failure to comply with the requirements of 31 CFR 103.110 will result in loss of safe harbor protection for information sharing and may result in a violation of privacy laws or other laws and regulations.

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

A notice to share information is effective for one year.[94] The financial institution should designate a point of contact for receiving and providing information. A financial institution should establish a process for sending and receiving information sharing requests. Additionally, a financial institution must take reasonable steps to verify that the other financial institution or association of financial institutions with which it intends to share information has also submitted the required notice to FinCEN. FinCEN provides participating financial institutions with access to a list of other participating financial institutions and their related contact information.

If a financial institution receives such information from another financial institution, it must also limit use of the information and maintain its security and confidentiality (31 CFR 103.110(b)(4)). Such information may be used only to identify and, where appropriate, report on money laundering and terrorist activities; to determine whether to establish or maintain an account; to engage in a transaction; or to assist in BSA

---

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

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

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

compliance. The procedures to ensure confidentiality will be considered adequate if the financial institution applies procedures similar to the ones it has established to comply with section 501 of the Gramm–Leach–Bliley Act (15 USC 6801) for the protection of its customers' nonpublic personal information. The safe harbor does not extend to sharing of information across international borders. In addition, section 314(b) does not authorize a financial institution to share a SAR, nor does it permit the financial institution to disclose the existence or nonexistence of a SAR. If a financial institution shares information under section 314(b) about the subject of a prepared or filed SAR, the information shared should be limited to underlying transaction and customer information. A financial institution may use information obtained under section 314(b) to determine whether to file a SAR, but the intention to prepare or file a SAR cannot be shared with another financial institution. Financial institutions should establish a process for determining when and if a SAR should be filed.

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

Examination Procedures

Information Sharing

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

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

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

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

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

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

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

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

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

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

Voluntary Information Sharing (Section 314(b))

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

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

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

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

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

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

Transaction Testing

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

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

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

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

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

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

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

Purchase and Sale of Monetary Instruments Recordkeeping — Overview

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

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

Purchaser Verification

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

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

Acceptable Identification

The U.S. Treasury's Administrative Ruling 92-1 provides guidance on how a bank can verify the identity of an elderly or disabled customer who does not possess the normally acceptable forms of identification. A bank may accept a Social Security, Medicare, or Medicaid card along with another form of documentation bearing the customer's name and address. Additional forms of documentation include a utility bill, a tax bill, or a voter registration card. The forms of alternate identification a bank decides to accept should be included in its formal policies, procedures, and processes.

Contemporaneous Purchases

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

Indirect Currency Purchases of Monetary Instruments

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

However, FinCEN takes the position[96] that when a customer purchases a monetary instrument in amounts between $3,000 and $10,000 using currency that the customer first deposits into the customer's account, the transaction is still subject to the recordkeeping requirements of 31 CFR 103.29. This requirement applies whether the transaction is conducted in accordance with a bank's established policy or at the request of the customer. Generally, when a bank sells monetary instruments to deposit accountholders, the bank will already maintain most of the information required by 31 CFR 103.29 in the normal course of its business.

Recordkeeping and Retention Requirements

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

- If the purchaser **has a deposit account** with the bank:
  - Name of the purchaser.
  - Date of purchase.
  - Types of instruments purchased.
  - Serial numbers of each of the instruments purchased.
  - Dollar amounts of each of the instruments purchased in currency.
  - Specific identifying information, if applicable.[97]

---

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

[97] The bank must verify that the person is a deposit accountholder or must verify the person's identity. Verification may be either through a signature card or other file or record at the bank, provided the deposit accountholder's name and address were verified previously and that information was recorded on the

- If the purchaser does not have a deposit account with the bank:
  - Name and address of the purchaser.
  - Social Security or alien identification number of the purchaser.
  - Date of birth of the purchaser.
  - Date of purchase.
  - Types of instruments purchased.
  - Serial numbers of each of the instruments purchased.
  - Dollar amounts of each of the instruments purchased.
  - Specific identifying information for verifying the purchaser's identity (e.g., state of issuance and number on driver's license).

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

---

signature card or other file or record, or by examination of a document that is normally acceptable within the banking community and that contains the name and address of the purchaser. If the deposit accountholder's identity has not been verified previously, the bank shall record the specific identifying information (e.g., state of issuance and number of driver's license) of the document examined.

Examination Procedures

Purchase and Sale of Monetary Instruments Recordkeeping

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

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

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

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

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

Transaction Testing

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

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

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

Funds Transfers Recordkeeping — Overview

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

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

In 1995, the U.S. Treasury and the Board of Governors of the Federal Reserve System issued a final rule on recordkeeping requirements concerning payment orders by banks (31 CFR 103.33).[98] The rule requires each bank involved in funds transfers[99] to collect and retain certain information in connection with funds transfers of $3,000 or more.[100] The information required to be collected and retained depends on the bank's role in the particular funds transfer (originator's bank, intermediary bank, or beneficiary's bank).[101] The requirements may also vary depending on whether an originator or beneficiary is an established customer of a bank and whether a payment order is made in person or otherwise.

Also in 1995, the U.S. Treasury issued a final rule that requires all financial institutions to include certain information in transmittal orders for funds transfers of $3,000 or more (31 CFR 103.33).[102] This requirement is commonly referred to as the "Travel Rule."

---

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

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

[100] 31 CFR 103.33(e)(6) provides exceptions to the funds transfer requirements. Funds transfers where both the originator and the beneficiary are the same person and the originator's bank and the beneficiary's bank are the same bank are not subject to the recordkeeping requirements for funds transfers. Additionally, exceptions are provided from the recordkeeping requirements for funds transfers where the originator and beneficiary are: a bank; a wholly owned domestic subsidiary of a bank chartered in the United States; a broker or dealer in securities; a wholly owned domestic subsidiary of a broker or dealer in securities; the United States; a state or local government; or a federal, state or local government agency or instrumentality.

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

[102] The rule applies to both banks and nonbanks (31 CFR 103.33(g)). Because it is broader in scope, the Travel Rule uses more expansive terms, such as "transmittal order" instead of "payment order" and

Responsibilities of Originator's Banks

Recordkeeping Requirements

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

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

Additional Recordkeeping Requirements for Nonestablished Customers

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

Payment Orders Made in Person

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

- Name and address of the person placing the order.
- Type of identification reviewed.
- Number of the identification document (e.g., driver's license).

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

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

Payment Orders Not Made in Person

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

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

Retrievability

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

Travel Rule Requirement

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

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

  - Name and address of the recipient.
  - Account number of the recipient.
  - Any other specific identifier of the recipient.
- Either the name and address or the numerical identifier of the transmittor's financial institution.

There are no recordkeeping requirements in the Travel Rule.

Responsibilities of Intermediary Institutions

Recordkeeping Requirements

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

Travel Rule Requirements

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

- Name and account number of the transmittor.
- Address of the transmittor.
- Amount of the transmittal order.
- Date of the transmittal order.
- Identity of the recipient's financial institution.
- As many of the following items as are received with the transmittal order:
  - Name and address of the recipient.
  - Account number of the recipient.
  - Any other specific identifier of the recipient.
- Either the name and address or the numerical identifier of the transmittor's financial institution.

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

Responsibilities of Beneficiary's Banks

Recordkeeping Requirements

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

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

Proceeds Delivered in Person

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

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

Proceeds Not Delivered in Person

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

Retrievability

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

There are no Travel Rule requirements for beneficiary banks.

Abbreviations and Addresses

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

("doing business as") or the names of unincorporated divisions or departments of the business.

Customer Address

The term "address," as used in 31 CFR 103.33(g), is not defined. Previously issued guidance from FinCEN had been interpreted as not allowing the use of mailing addresses in a transmittal order when a street address is known to the transmittor's financial institution. However, in the November 28, 2003, *Federal Register* notice,[103] FinCEN issued a regulatory interpretation that states the Travel Rule should allow the use of mailing addresses, including post office boxes, in the transmittor address field of transmittal orders in certain circumstances.

The regulatory interpretation states that, for purposes of 31 CFR 103.33(g), the term "address" means either the transmittor's street address or the transmittor's address maintained in the financial institution's automated CIF (such as a mailing address including a post office box) as long as the institution maintains the transmittor's address[104] on file and the address information is retrievable upon request by law enforcement.

---

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

[104] Consistent with 31 CFR 103.121, an "address" for purposes of the Travel Rule is as follows: for an individual, "address" is a residential or business street address, an Army Post Office Box or a Fleet Post Office Box, or the residential or business street address of next of kin or another contact person for persons who do not have a residential or business address. For a person other than an individual (such as a corporation, partnership, or trust), "address" is a principal place of business, local office, or other physical location. However, while 31 CFR 103.121 applies only to new customers opening accounts on or after October 1, 2003, and while the rule exempt funds transfers from the definition of "account," for banks, the Travel Rule applies to all transmittals of funds of $3,000 or more, whether or not the transmittor is a customer for purposes of 31 CFR 103.121.

Examination Procedures

Funds Transfers Recordkeeping

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

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

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

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

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

Transaction Testing

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

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

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

Foreign Correspondent Account Recordkeeping and Due Diligence — Overview

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

One of the central goals of the USA PATRIOT Act was to protect access to the U.S. financial system by requiring certain records and due diligence programs for foreign correspondent accounts. In addition, the USA PATRIOT Act prohibits accounts with foreign shell banks. Foreign correspondent accounts, as noted in past U.S. Senate investigative reports,[105] are a gateway into the U.S. financial system. This section of the manual covers the regulatory requirements established by sections 312, 313, and 319(b) of the USA PATRIOT Act and by the implementing regulations at 31 CFR 103.175, 103.176, 103.177, and 103.185. Additional discussions and procedures regarding specific money laundering risks for foreign correspondent banking activities, such as bulk shipments of currency, pouch activity, U.S. dollar drafts, and payable through accounts, are included in the expanded sections.

Foreign Shell Bank Prohibition and Foreign Correspondent Account Recordkeeping

For purposes of 31 CFR 103.177 and 103.185, a "correspondent account" is an account established by a bank for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of the foreign bank, or to handle other financial transactions related to the foreign bank. An "account" means any formal banking or business relationship established to provide regular services, dealings, and other financial transactions. It includes a demand deposit, savings deposit, or other transaction or asset account and a credit account or other extension of credit (31 CFR 103.175(d)). Accounts maintained by foreign banks for financial institutions covered by the rule are not "correspondent accounts" subject to this regulation.[106]

---

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

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

Under 31 CFR 103.177, a bank is prohibited from establishing, maintaining, administering, or managing a correspondent account in the United States for, or on behalf of, a foreign shell bank. A foreign shell bank is defined as a foreign bank without a physical presence in any country.[107] An exception, however, permits a bank to maintain a correspondent account for a foreign shell bank that is a regulated affiliate.[108] 31 CFR 103.177 also requires that a bank take reasonable steps to ensure that any correspondent account established, maintained, administered, or managed in the United States for a foreign bank is not being used by that foreign bank to provide banking services indirectly to foreign shell banks.

Certifications

A bank that maintains a correspondent account in the United States for a foreign bank must maintain records in the United States identifying the owners of each foreign bank.[109] A bank must also record the name and street address of a person who resides in the United States and who is authorized, and has agreed, to be an agent to accept service of legal process.[110] Under 31 CFR 103.185, a bank must produce these records within seven days upon receipt of a written request from a federal law enforcement officer.

---

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

[107] "Physical presence" means a place of business that:

- Is maintained by a foreign bank.
- Is located at a fixed address (other than solely an electronic address or a post office box) in a country in which the foreign financial institution is authorized to conduct banking activities, at which location the foreign financial institution:
- Employs one or more persons on a full-time basis.
- Maintains operating records related to its banking activities.
- Is subject to inspection by the banking authority that licensed the foreign financial institution to conduct banking activities.

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

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

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

The U.S. Treasury, working with the industry and federal banking and law enforcement agencies, developed a "certification process" to assist banks in complying with the recordkeeping provisions. This process includes certification and recertification forms. While banks are not required to use these forms, a bank will be "deemed to be in compliance" with the regulation if it obtains a completed certification form from the foreign bank and receives a recertification on or before the three-year anniversary of the execution of the initial or previous certification.[111]

Account Closure

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

Verification

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

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

Subpoenas

Under section 319(b) of the USA PATRIOT Act, the Secretary of the Treasury or the U.S. Attorney General may issue a subpoena or summons to any foreign bank that maintains a correspondent account in the United States to obtain records relating to that

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

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

Requests for AML Records by Federal Regulator

Also, upon request by its federal regulator, a bank must provide or make available records related to AML compliance of the bank or one of its customers, within 120 hours from the time of the request (31 USC 5318(k)(2)).

Special Due Diligence Program for Foreign Correspondent Accounts

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

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

General Due Diligence

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

---

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

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

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

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

Risk assessment of foreign financial institutions. A bank's general due diligence program must include policies, procedures, and processes to assess the risks posed by the bank's foreign financial institution customers. A bank's resources are most appropriately directed at those accounts that pose a more significant money laundering risk. The bank's due diligence program should provide for the risk assessment of foreign correspondent accounts considering all relevant factors, including, as appropriate:

- The nature of the foreign financial institution's business and the markets it serves.
- The type, purpose, and anticipated activity of the foreign correspondent account.
- The nature and duration of the bank's relationship with the foreign financial institution (and, if relevant, with any affiliate of the foreign financial institution).
- The AML and supervisory regime of the jurisdiction that issued the charter or license to the foreign financial institution and, to the extent that information regarding such jurisdiction is reasonably available, of the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered.
- Information known or reasonably available to the bank about the foreign financial institution's AML record, including public information in standard industry guides, periodicals, and major publications.

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

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

---

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

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

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

Enhanced Due Diligence

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

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

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

---

[113] The USA PATRIOT Act (31 USC 5318(i)(4)(A) and 31 CFR 103.175(k)) define an offshore banking license as a license to conduct banking activities that, as a condition of the license, prohibits the licensed entity from conducting banking activities with the citizens, or in the local currency of, the jurisdiction that issued the license.

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

- Determine, for any such foreign bank whose shares are not publicly traded, the identity of each of the owners of the foreign bank, and the nature and extent of the ownership interest of each such owner.[115]

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

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

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

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

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

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

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

[115] An "owner" is any person who directly or indirectly owns, controls, or has the power to vote 10 percent or more of any class of securities of a foreign bank (31 CFR 103.176(b)(3)). "Publicly traded" means shares that are traded on an exchange or an organized over-the-counter market that is regulated by a foreign securities authority, as defined in section 3(a)(50) of the Securities Exchange Act of 1934 (15 USC 78c(a)(50)) (31 CFR 103.176(b)(3)).

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

Special Procedures When Due Diligence Cannot Be Performed

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

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

Examination Procedures

Foreign Correspondent Account Recordkeeping and Due Diligence

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

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

Foreign Shell Bank Prohibition and Foreign Correspondent Account Recordkeeping

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

Special Due Diligence Program for Foreign Correspondent Accounts

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

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

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

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

7. Ensure the program is reasonably designed to:

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

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

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

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

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

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

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

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

Transaction Testing

Foreign Shell Bank Prohibition and Foreign Correspondent Account Recordkeeping

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

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

Special Due Diligence Program for Foreign Correspondent Accounts

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

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

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

14. From the original sample, determine whether the bank has implemented EDD procedures for foreign banks operating under:

    - An offshore banking license.
    - A banking license issued by a foreign country that has been designated as noncooperative with international AML principles or procedures.
    - A banking license issued by a foreign country that has been designated by the Secretary of the Treasury as warranting special measures due to AML concerns.

15. From a sample of accounts that are subject to EDD, verify that the bank has taken reasonable steps, in accordance with the bank's policies, procedures, and processes, to:

    - Determine, for any such foreign bank whose shares are not publicly traded, the identity of each of the owners of the foreign bank with the power to vote 10 percent or more of any class of securities of the bank, and the nature and extent of the ownership interest of each such owner.
    - Conduct enhanced scrutiny of any accounts held by such banks to guard against money laundering and report suspicious activity.
    - Determine whether such foreign bank provides correspondent accounts to other foreign banks and, if so, obtain information relevant to assess and mitigate money laundering risks associated with the foreign bank's correspondent accounts for other foreign banks, including, as appropriate, the identity of those foreign banks.

16. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes to meet regulatory requirements associated with foreign correspondent account recordkeeping and due diligence.

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

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

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

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

The overview and examination procedures set forth in this section are intended to evaluate the bank's due diligence program concerning private banking accounts offered to non-U.S. persons. Additional procedures for specific risk areas of private banking are included in the expanded examination procedures, "Private Banking," pages 284 to 285.

Private Banking Accounts

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

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

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

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

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

Due Diligence Program

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

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

---

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

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

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

Ascertaining Source of Funds and Monitoring Account Activity

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

Enhanced Scrutiny of Private Banking Accounts for Senior Foreign Political Figures

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

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

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

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

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

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

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

---

[119] Additional red flags regarding transactions that may be related to the proceeds of foreign corruption are listed in *Guidance on Enhanced Scrutiny for Transactions That May Involve the Proceeds of Foreign Official Corruption*, issued by the U.S. Treasury, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision, and the Department of State, January 2001.

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

Identifying Senior Foreign Political Figures

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

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

Special Procedures When Due Diligence Cannot Be Performed

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

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

Examination Procedures

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

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

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

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

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

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

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

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

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

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

Transaction Testing

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

---

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

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

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

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

Special Measures — Overview

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

Section 311 of the USA PATRIOT Act added 31 USC 5318A to the BSA, which authorizes the Secretary of the Treasury to require domestic financial institutions and domestic financial agencies to take certain special measures against foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts of primary money laundering concern. Section 311 provides the Secretary of the Treasury with a range of options that can be adapted to target specific money laundering and terrorist financing concerns. Section 311 is implemented through various orders and regulations that are incorporated into 31 CFR 103.[124] As set forth in section 311, certain special measures may be imposed by an order without prior public notice and comment, but such orders must be of limited duration and must be issued together with a Notice of Proposed Rulemaking.

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

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

Types of Special Measures

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

Recordkeeping and Reporting of Certain Financial Transactions

Under the first special measure, banks may be required to maintain records or to file reports, or both, concerning the aggregate amount of transactions or the specifics of each transaction with respect to a jurisdiction, financial institution, class of transactions, or type of account that is of primary money laundering concern. The statute contains

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

minimum information requirements for these records and reports and permits the Secretary of the Treasury to impose additional information requirements.

Information Relating to Beneficial Ownership

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

Information Relating to Certain Payable Through Accounts

Under the third special measure, banks that open or maintain a payable through account in the United States involving a jurisdiction, financial institution, class of transactions, or type of account that is of primary money laundering concern may be required (i) to identify each customer (and representative) who is permitted to use the account or whose transactions are routed through the account and (ii) to obtain information about each customer (and representative) that is substantially comparable to that which the bank obtains in the ordinary course of business with respect to its customers residing in the United States.[125]

Information Relating to Certain Correspondent Accounts

Under the fourth special measure, banks that open or maintain a correspondent account in the United States involving a jurisdiction, financial institution, class of transactions, or type of account that is of primary money laundering concern may be required to: (i) identify each customer (and representative) who is permitted to use the account or whose transactions are routed through the account; and (ii) obtain information about each such customer (and representative) that is substantially comparable to that which a United States depository institution obtains in the ordinary course of business with respect to its customers residing in the United States.[126]

---

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

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

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

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

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

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

Special Measures Guidance

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

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

Examination Procedures

Special Measures

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

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

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

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

Transaction Testing

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

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

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

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

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

Foreign Bank and Financial Accounts Reporting — Overview

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

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

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

A bank must file this form on its own accounts that meet this definition; additionally, the bank may be obligated to file these forms for customer accounts in which the bank has a financial interest or over which it has signature or other authority.

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

---

[127] As defined in 31 CFR 103.11(z), the term "person" means an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture or other unincorporated organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal personalities. The instructions to the FBAR further state that the term "United States person" means a citizen or resident of the United States or a person in and doing business in the United States. The IRS has indicated that generally a person is not considered to be "in and doing business in the United States" unless that person is conducting business within the United States on a regular and continuous basis. Refer to *FAQs Regarding Report of Foreign Bank and Financial Accounts (FBAR)*, February 12, 2009, www.irs.gov/businesses/small/article/0,,id=148845,00.html#UPS1. Furthermore, in Announcement 2009-51, 2009-25 I.R.B. 1105, issued June 5, 2009, the IRS indicated that it had suspended temporarily the FBAR filing requirement for persons who are not U.S. citizens, residents, or domestic entities.

[128] 31 CFR 103.24.

Examination Procedures

Foreign Bank and Financial Accounts Reporting

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

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

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

Transaction Testing

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

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

International Transportation of Currency or Monetary Instruments Reporting — Overview

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

Each person[129] (including a bank) who physically transports, mails, or ships currency or monetary instruments in excess of $10,000 at one time out of or into the United States (and each person who causes such transportation, mailing, or shipment) must file a Report of International Transportation of Currency or Monetary Instruments (CMIR) (FinCEN Form 105).[130] A CMIR must be filed with the appropriate Bureau of Customs and Border Protection officer or with the commissioner of Customs at the time of entry into or departure from the United States. When a person receives currency or monetary instruments in an amount exceeding $10,000 at one time that have been shipped from any place outside the United States, a CMIR must be filed with the appropriate Bureau of Customs and Border Protection officer or with the commissioner of Customs within 15 days of receipt of the instruments (unless a report has already been filed). The report is to be completed by or on behalf of the person requesting transfer of the currency or monetary instruments. However, banks are not required to report these items if they are mailed or shipped through the postal service or by common carrier.[131] In addition, a commercial bank or trust company organized under the laws of any state or of the United States is not required to report overland shipments of currency or monetary instruments if they are shipped to or received from an established customer maintaining a deposit relationship with the bank and if the bank reasonably concludes the amounts do not exceed what is commensurate with the customary conduct of the business, industry, or profession of the customer concerned.

Management should implement applicable policies, procedures, and processes for CMIR filing. Management should review the international transportation of currency and

---

[129] As defined in 31 CFR 103.11(z), the term "person" means an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture or other unincorporated organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal personalities.

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

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

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

Examination Procedures

International Transportation of Currency or Monetary Instruments Reporting

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

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

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

Transaction Testing

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

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

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

Office of Foreign Assets Control — Overview

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

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

OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and to freeze assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates; therefore, they are multilateral in scope, and involve close cooperation with allied governments. Other sanctions are specific to the interests of the United States. OFAC has been delegated responsibility by the Secretary of the Treasury for developing, promulgating, and administering U.S. sanctions programs.[132]

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

---

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

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

All U.S. persons,[134] including U.S. banks, bank holding companies, and nonbank subsidiaries, must comply with OFAC's regulations.[135] The federal banking agencies evaluate OFAC compliance systems to ensure that all banks subject to their supervision comply with the sanctions.[136] Unlike the BSA, the laws and OFAC-issued regulations apply not only to U.S. banks, their domestic branches, agencies, and international banking facilities, but also to their foreign branches, and often overseas offices and subsidiaries. In general, the regulations require the following:

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

Blocked Transactions

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

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

For example, if a U.S. bank receives instructions to make a funds transfer payment that falls into one of these categories, it must execute the payment order and place the funds

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

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

[136] 31 CFR chapter V.

into a blocked account.[137] A payment order cannot be canceled or amended after it is received by a U.S. bank in the absence of an authorization from OFAC.

Prohibited Transactions

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

It is important to note that the OFAC regime specifying prohibitions against certain countries, entities, and individuals is separate and distinct from the provision within the BSA's CIP regulation (31 CFR 103.121) that requires banks to compare new accounts against government lists of known or suspected terrorists or terrorist organizations within a reasonable period of time after the account is opened. OFAC lists have not been designated government lists for purposes of the CIP rule. Refer to the core overview section, "Customer Identification Program," pages 52 to 58, for further guidance. However, OFAC's requirements stem from other statutes not limited to terrorism, and OFAC sanctions apply to transactions, in addition to account relationships.

OFAC Licenses

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

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

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

Specific licenses are issued on a case-by-case basis.[139] A specific license is a written document issued by OFAC authorizing a particular transaction or set of transactions. To receive a specific license, the person or entity who would like to undertake the transaction must submit an application to OFAC. If the transaction conforms to U.S. foreign policy under a particular program, the license will be issued. If a bank's customer claims to have a specific license, the bank should verify that the transaction conforms to the terms of the license and obtain and retain a copy of the authorizing license.

OFAC Reporting

Banks must report all blockings to OFAC within 10 days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30).[140] Once assets or funds are blocked, they should be placed in a blocked account. Prohibited transactions that are rejected must also be reported to OFAC within 10 days of the occurrence.

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

Additional information concerning OFAC regulations, such as Sanctions Program and Country Summaries brochures; the SDN list, including both entities and individuals; recent OFAC actions; and "Frequently Asked Questions," can be found on OFAC's Web site.[141]

OFAC Compliance Program

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

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

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

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

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

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

OFAC Risk Assessment

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

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

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

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

- International funds transfers.
- Nonresident alien accounts.
- Foreign customer accounts.
- Cross-border automated clearing house (ACH) transactions.
- Commercial letters of credit and other trade finance products.
- Transactional electronic banking.

- Foreign correspondent bank accounts.
- Payable through accounts.
- International private banking.
- Overseas branches or subsidiaries.

Appendix M ("Quantity of Risk — OFAC Procedures") provides guidance to examiners on assessing OFAC risks facing a bank. The risk assessment can be used to assist the examiner in determining the scope of the OFAC examination. Additional information on compliance risk is posted by OFAC on its Web site under "Frequently Asked Questions."[142]

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

Internal Controls

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

Identifying and reviewing suspect transactions. The bank's policies, procedures, and processes should address how the bank will identify and review transactions and accounts for possible OFAC violations, whether conducted manually, through interdiction software, or a combination of both. For screening purposes, the bank should clearly define its criteria for comparing names provided on the OFAC list with the names in the bank's files or on transactions and for identifying transactions or accounts involving sanctioned countries. The bank's policies, procedures, and processes should also address how it will determine whether an initial OFAC hit is a valid match or a false hit.[143] A high volume of false hits may indicate a need to review the bank's interdiction program.

The screening criteria used by banks to identify name variations and misspellings should be based on the level of OFAC risk associated with the particular product or type of transaction. For example, in a higher-risk area with a high-volume of transactions, the bank's interdiction software should be able to identify close name derivations for review. The SDN list attempts to provide name derivations; however, the list may not include all derivations. More sophisticated interdiction software may be able to catch variations of an SDN's name not included on the SDN list. Lower-risk banks or areas and those with

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

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

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

New accounts should be compared with the OFAC lists prior to being opened or shortly thereafter (e.g., during nightly processing). Banks that perform OFAC checks after account opening should have procedures in place to prevent transactions, other than initial deposits, from occurring until the OFAC check is completed. Prohibited transactions conducted prior to completing an OFAC check may be subject to possible penalty action. In addition, banks should have policies, procedures, and processes in place to check existing customers when there are additions or changes to the OFAC list. The frequency of the review should be based on the bank's OFAC risk. For example, banks with a lower OFAC risk level may periodically (e.g., monthly or quarterly) compare the customer base against the OFAC list. Transactions such as funds transfers, letters of credit, and noncustomer transactions should be checked against OFAC lists prior to being executed. When developing OFAC policies, procedures, and processes, the bank should keep in mind that OFAC considers the continued operation of an account or the processing of transactions post-designation, along with the adequacy of their OFAC compliance program, to be a factor in determining penalty actions.[144] The bank should maintain documentation of its OFAC checks on new accounts, the existing customer base and specific transactions.

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

Updating OFAC lists. A bank's OFAC compliance program should include policies, procedures, and processes for timely updating of the lists of blocked countries, entities, and individuals and disseminating such information throughout the bank's domestic operations and its offshore offices, branches and, in the case of Cuba and North Korea, foreign subsidiaries. This would include ensuring that any manual updates of interdiction software are completed in a timely manner.

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

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

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

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

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

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

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

---

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

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

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

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

Banks no longer need to file SARs based solely on blocked narcotics- or terrorism-related transactions, as long as the bank files the required blocking report with OFAC. However, because blocking reports require only limited information, if the bank is in possession of additional information not included on the blocking report filed with OFAC, a separate SAR should be filed with FinCEN including that information. In addition, the bank should file a SAR if the transaction itself would be considered suspicious in the absence of a valid OFAC match.[148]

Maintaining license information. OFAC recommends that banks consider maintaining copies of customers' OFAC licenses on file. This will allow the bank to verify whether a customer is initiating a legal transaction. Banks should also be aware of the expiration date on the license. If it is unclear whether a particular transaction is authorized by a

---

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

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

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

license, the bank should confirm with OFAC. Maintaining copies of licenses will also be useful if another bank in the payment chain requests verification of a license's validity. Copies of licenses should be maintained for five years, following the most recent transaction conducted in accordance with the license.

Independent Testing

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

Responsible Individual

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

Training

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

Examination Procedures

Office of Foreign Assets Control

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

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

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

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

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

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

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

Transaction Testing

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

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

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

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

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

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

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

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

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

7. Identify any potential matches that were not reported to OFAC, discuss with bank management, advise bank management to immediately notify OFAC of unreported transactions, and immediately notify supervisory personnel at your regulatory agency.
8. Determine the origin of deficiencies (e.g., training, audit, risk assessment, internal controls, management oversight), and conclude on the adequacy of the bank's OFAC compliance program.
9. Discuss OFAC related examination findings with bank management.
10. Include OFAC conclusions within the report of examination, as appropriate.

EXPANDED EXAMINATION OVERVIEW AND PROCEDURES FOR CONSOLIDATED AND OTHER TYPES OF BSA/AML COMPLIANCE PROGRAM STRUCTURES

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.[149] 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.[150] 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.

---

[149] Neither FinCEN nor banking agency rules impose a specific BSA/AML compliance program obligation on Bank Holding Companies, Unitary Savings and Loan Holding Companies, and parents of Industrial Loan Companies. Nevertheless, these entities, as a result of their primary business function (e.g., insurance company or broker-dealer), may be subject to a BSA/AML compliance program obligation under Treasury rules or rules of other agencies.

[150] For further detail, refer to *Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles,* Federal Reserve Board SR Letter 08-8, October 16, 2008 (FRB Guidance). The FRB Guidance generally addresses overall compliance functions within large, complex firms, and endorses for all firms the principles set forth in the Basel Committee on Banking Supervision's guidance, *Compliance and the compliance function in banks* (April 2005) at www.bis.org/publ/bcbs113.htm.

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.[151] 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," page 28. 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.

---

[151] For additional guidance, refer to the expanded overview section, "Foreign Branches and Offices of U.S. Banks," pages 169 to 172, and the Basel Committee on Banking Supervision's guidance *Consolidated Know Your Customer (KYC) Risk Management* at www.bis.org/press/p041006.htm.

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.[152] 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

[152] Foreign banking organizations should ensure that, with respect to their U.S. operations, the responsibilities of the board described in this section are fulfilled in an appropriate manner through their oversight structure and BSA/AML risk management framework.

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 and implemented.

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," pages 169 to 172.

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.

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 (12 CFR 225.4(f)). 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 103.16) and broker/dealers (31 CFR 103.19)). 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," pages 67 to 80, 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.

   - 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.[153] For additional guidance, refer to the core overview and examination procedures, "Suspicious Activity Reporting," pages 67 to 80 and 81 to 85, respectively.
6. Once the examiner has completed the above procedures, the examiner should discuss their findings with the following parties, as appropriate:
   - Examiner in charge.

[153] 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 (12 CFR 225.4(f)). 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 103.16) and broker/dealers (31 CFR 103.19)). 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," pages 67 to 80, for additional information.

- 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.

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[154] 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.[155] 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.[156] 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.[157]

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

---

[154] Foreign offices include affiliates and subsidiaries.

[155] Edge and agreement corporations may be used to hold foreign investments (e.g., foreign portfolio investments, joint ventures, or subsidiaries).

[156] 71 Fed. Reg. 13935.

[157] For additional information, refer to *Consolidated Know Your Customer (KYC) Risk Management*, Basel Committee on Banking Supervision, 2004, at www.bis.org/forum/research.htm.

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[158] 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.

---

[158] Foreign offices include affiliates and subsidiaries.

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," pages 157 to 159, 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.

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.[159]

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.

---

[159] For additional risks associated with parallel banking, refer to the *Joint Agency Statement on Parallel-Owned Banking Organizations* issued by the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and Office of Thrift Supervision, April 23, 2002.

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 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," pages 157 to 159, 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.

EXPANDED EXAMINATION OVERVIEW AND PROCEDURES FOR PRODUCTS AND SERVICES

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 will sign a service agreement with the respondent bank[160] outlining each party's responsibilities. The service agreement may include the following:

- Products and services provided.
- Responsibility for recordkeeping (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 will be utilizing the account.

[160] A respondent bank is any bank for which another bank establishes, maintains, administers, or manages a correspondent account relationship.

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," pages 147 to 156 and 157 to 159, respectively.

Examination Procedures

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," pages 157 to 159, for guidance.

Transaction Testing

5. On the basis of the bank's review of respondent accounts[161] 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.

[161] A respondent bank is any bank for which another bank establishes, maintains, administers, or manages a correspondent account relationship.

- 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.

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 some customers to conduct transactions anonymously through the U.S. bank account (e.g., payable through accounts[162] and nested accounts).

Nested Accounts

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

Risk Mitigation

U.S. banks that offer foreign correspondent financial institution services should have policies, procedures, and processes to manage the BSA/AML risks inherent with these relationships and 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 products, services, customers, and geographic locations. The Clearing House Payments Co., LLC. and The Wolfsberg Group have published suggested industry standards and guidance for banks that provide foreign correspondent banking services.[163] Also, additional information relating to risk assessments and due diligence is contained in the core overview section, "Foreign Correspondent Account Recordkeeping

[162] Refer to the expanded overview section, "Payable Through Accounts," pages 198 to 200, for additional information.

[163] Refer to *Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking* (March 2002) at www.theclearinghouse.org/docs/000592.pdf and *Wolfsberg AML Principles for Correspondent Banking* (November 2002) at www.wolfsberg-principles.com/standards.html.

and Due Diligence," pages 117 to 124. The U.S. bank's policies, procedures, and processes should:

- Specify appropriate account-opening procedures, which may include minimum levels of documentation to be obtained from prospective customers; an account approval process independent of the correspondent account business line for potential higher-risk customers; and a description of circumstances when the bank will 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 of the accounts and expected account activity (e.g., determine whether the relationship will serve as a payable through account).
- Understand the foreign correspondent financial institution's other correspondent relationships (e.g., determine whether nested accounts will be utilized).
- Conduct adequate and ongoing due diligence on the foreign correspondent financial institution relationships, which may include periodic visits.
- Establish a formalized process for escalating suspicious information on potential and existing customers to an appropriate management level for review.
- Ensure that foreign correspondent financial institution relationships are appropriately included within the U.S. bank's suspicious activity monitoring and reporting systems.
- Ensure that appropriate due diligence standards are applied to those accounts determined to be higher risk.
- Establish criteria for closing the foreign correspondent financial institution account.

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

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," pages 157 to 159, 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 bulk shipments of currency and management's implementation of effective monitoring and reporting systems.*

Bulk shipments of currency entail the use of common, independent, or Postal Service air/land/sea carriers to transport large volumes of bank notes (U.S. or foreign) from sources either inside or outside the United States to a bank in the United States. Often, but not always, shipments take the form of containerized cargo.

Shippers may be "Currency Originators," 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 "Intermediaries" that ship currency gathered from their customers who are Currency Originators. Intermediaries may also ship currency gathered from other Intermediaries. 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. 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 it becomes recorded as held on the bank's behalf.

Banks are required to report shipments of currency in an aggregate amount exceeding $10,000 received from or shipped to locations outside the U.S. via FinCEN Form 105 (Report of International Transportation of Currency or Monetary Instruments). Banks are exempt from this reporting requirement when the currency is shipped overland via the Postal Service or common carrier (see 31 CFR 103.23). Banks are not exempt from this reporting requirement when the currency is shipped by other methods, including air courier or via the airlines. Regardless of whether an exemption from filing FinCEN Form 105 applies, banks must still monitor for, and report, suspicious activity. In addition, and regardless of reporting requirements on FinCEN Form 105, banks are required to report the receipt or disbursement of currency in excess of $10,000 via FinCEN Form 104 (Currency Transaction Report), subject to the exemptions at 31 CFR 103.122(d). This reporting requirement applies even if the international transactions are subject to the exemption from filing Form 105.

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.[164] 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 a U.S. bank. Often, this occurs through the use of a foreign financial institution 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.[165] Experience has shown a direct correlation between the smuggling of bulk currency, the heightened use of cash letter instruments or wire transfers from certain foreign financial institutions, and bulk shipments of currency into the United States from the same foreign financial institutions.[166]

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. 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 also should guard against introducing the monetary proceeds of criminal or terrorist activity into the financial system. To inform banks on the topic of bulk currency shipments, FinCEN issued an advisory in 2006 that sets forth certain activities that may be associated with currency smuggling.[167] 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 advisory deals specifically with the

---

[164] U.S. Money Laundering Threat Assessment (December 2005) on page 33. Congress criminalized the act of smuggling large amounts of cash as part of the USA PATRIOT Act. Specifically, Title 31 U.S.C. 5332-Bulk Cash Smuggling makes it a crime to smuggle or attempt to smuggle over $10,000 in currency or other monetary instruments into or out of the United States, with the specific intent to evade the U.S. currency-reporting requirements codified in 31 U.S.C. 5316.

[165] In certain cases, the foreign financial institution will ship the cash to its central bank or a money center bank in the foreign country in which the cash letter instrument originated. Sometimes numerous layered transactions are used to disguise the origins of the cash, after which the currency may be returned directly to the United States or further shipped to or through other jurisdictions. The cash will be repatriated back to the United States for the account of the U.S. bank in which the cash letter instrument was processed or funds transfer deposit was made.

[166] For an example of these types of transactions, refer to National Drug Intelligence Center's National Drug Threat Assessment 2008, Illicit Finance (December 2007).

[167] FinCEN Guidance to Financial Institutions on the Repatriation of Currency Smuggled into Mexico from the U.S., FIN-2006-A003 (April 28, 2006).

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.

Law enforcement has identified the following activities that, in various combinations, may be associated with currency smuggling:[168]

- 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.

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, and the nature, source, location, and control of

[168] *Id.*

bulk currency. For additional information relating to risk assessments and due diligence, refer to the core overview sections "BSA/AML Risk Assessment" on pages 22 to 30 and "Customer Due Diligence" on pages 63 to 65.

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 will 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, and any required BSA reporting obligations (CTRs, CMIRs, etc.).

- Identify the characteristics of acceptable and unacceptable transactions, including circumstances when the bank will or will 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.

- Once the relationship is established, require adequate and ongoing due diligence, which, as appropriate, may include periodic visits to the shipper and to shipping-preparation sites. As necessary, scrutinize for legitimacy the root source of cash shipments, 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.

As a sound practice, U.S. banks should inform Currency Originators 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 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 or Intermediaries. 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 Currency Originator or Intermediary, and the Currency Originator or Intermediary's customers. The agreement or contract should also address expectations about due diligence and permitted third-party usage of the shipper's services. 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 bulk shipments of currency, and management's ability to implement effective due diligence, monitoring, and reporting systems.*

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

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

3. Review the list of Currency Originators 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 and Intermediaries. Consider the source of the Currency Originator 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 or Intermediaries, review a sample agreement or contract to determine whether each party's responsibilities, products, and services provided, and allowable third-party usage of the relationship, 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'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.

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

Transaction Testing

9. Based on the bank's risk assessment of its relationships with Currency Originators and Intermediaries, as well as prior examination and audit reports, select a sample of Currency Originators or Intermediaries and recent bulk currency shipments. The sample should include relationships with Currency Originators 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.

10. 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 and Intermediaries.
    - Determine whether the nature, volume, and frequency of activity is consistent with the expectations associated with the Currency Originator and Intermediary. Discuss with bank management any inconsistencies identified. 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.

11. If the Currency Originator or Intermediary, or the referral agent who works for the Currency Originator or Intermediary has an account with the bank, review a sample of account activity.

12. 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 will be returned for processing at the U.S. correspondent bank.

Risk Mitigation

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

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

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 "subaccountholders," with checks that allow them to draw funds from the foreign financial institution's account at the U.S. bank.[169] The subaccountholders, 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 subaccountholders 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 subaccountholder checks and other transactions, including currency deposits, through the

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

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 subaccountholders 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 subaccountholders 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 subaccountholders (e.g., casas de cambio, finance companies, funds remitters, or other nonbank financial institutions).
- Prohibitions or restrictions on multi-tier subaccountholders.[170]
- Access to the foreign financial institution's internal documents and audits that pertain to its PTA activity.

[170] It is possible for a subaccount to be subdivided into further subaccounts for separate persons.

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," pages 157 to 159, 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,[171] to transport currency, monetary instruments, and other documents from outside the United States to a bank in the United States.[172] 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 on pages 208 to 211.

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.

---

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

[172] For additional guidance, refer to the core overview section, "International Transportation of Currency or Monetary Instruments Reporting," on pages 144 to 145.

- 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," pages 157 to 159, 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,[173] bearer securities, prepaid cards, gems, art, illegal substances or contraband, or other items that should not ordinarily appear in a bank's pouch.

[173] Refer to core examination procedures, "International Transportation of Currency or Monetary Instruments Reporting," on pages 144 to 145, for additional guidance.

8. If the courier, or the referral agent who works for the courier, has 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), pages 59 to 62, for further guidance. Additional information on e-banking is available in the FFIEC *Information Technology Examination Handbook*.[174]

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

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

reports, new account activity reports, change of Internet address reports, Internet Protocol (IP) address reports, and reports to identify related or linked accounts (e.g., common addresses, phone numbers, e-mail addresses, and tax identification numbers). In determining the level of monitoring required for an account, banks should include how the account was opened as a factor. Banks 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.[175] 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 www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf.

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

[175] For additional information, refer to *Authentication in an Internet Banking Environment* issued by the FFIEC, October 13, 2005.

items are not typically forwarded to banks, but instead the customer or the customer's service provider retains them. As a result, recordkeeping, 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).[176]

[176] Franking involves printing or stamping such phrases as "Processed" or "Electronically Processed" on the front of the original check. This process is used as an indicator that the paper check has already been electronically processed, and, therefore, should not be subsequently physically deposited.

Examination 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," pages 157 to 159, 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.*[177]

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®)[178] and the Clearing House Interbank Payments System (CHIPS).[179] 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

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

[178] Fedwire® is a registered service mark of the Federal Reserve Banks. Refer to www.frbservices.org/fedwire/index.html for further information.

[179] CHIPS is a private multilateral settlement system owned and operated by The Clearing House Payments Co., LLC.

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.[180] 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.

---

[180] 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.

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.

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.[181] 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.[182] 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.

---

[181] Additional information on the details of the MT 202 COV format can be found at SWIFT's Web site, www.swift.com/about_swift/press_room/swift_news_archive/home_page_stories_archive_2009/Newstandardsforcoverpayments.page.

[182] Sources of information on IVTS include:

- FinCEN Advisory 33, *Informal Value Transfer Systems*, March 2003.
- U.S. Treasury *Informal Value Transfer Systems Report to the Congress in Accordance with Section 359 of the Patriot Act*, November 2002.
- 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.

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.

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 will determine which type of funds transfer system the bank uses. The vast majority of funds transfer instructions are conducted electronically; however, examiners need to be mindful that physical instructions may be transmitted by other informal methods, as described earlier.

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. 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 mitigant of risk in providing funds transfer services. Because of the nature of funds transfers, adequate and effective CDD policies, procedures, and processes are critical in detecting unusual and suspicious activities. 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 103.176). 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).[183] 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:

---

[183] Basel Committee on Banking Supervision, *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers* available at www.bis.org/publ/bcbs154.htm. In addition, during August 2009, the committee, along with the Clearinghouse Payments Co. LLC, released Q&As in order to enhance understanding of the MT 202 COV.

- 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. From review of MIS and internal risk rating factors, 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," pages 157 to 159, 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[184] and one-time ACH debits, reflecting the lower cost of ACH processing relative to check processing.[185] 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[186] 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.[187]

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.

---

[184] In 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 check.

[185] Refer to www.nacha.org.

[186] The Federal Reserve Banks operate FedACH, a central clearing facility for transmitting and receiving ACH payments, and FedGlobal, which sends cross-border ACH credits payments to more than 35 countries around the world, plus debit payments to Canada only.

[187] Refer to OCC Bulletin 2006-39 (September 1, 2006) at www.occ.gov/ftp/bulletin/2006-39.pdf.

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 accountholder receiving funds (payee). Within the ACH system, these participants and users are 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 Operator (GO).** A financial institution, ACH Operator, or ODFI that acts as an entry or exit point to or from the United States. A formal declaration of status as a Gateway Operator is not required. ACH operators and ODFIs acting in the role of Gateway Operators have specific warranties and obligations related to certain international entries. A financial institution acting as a Gateway Operator generally may process inbound and outbound debit and credit transactions. ACH Operators acting as Gateway Operators may process outbound debit and credit entries, but can limit inbound entries to credit entries only and reversals.

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.[188] The IAT is a new Standard Entry Class code for ACH payments that enables financial institutions to identify and monitor international ACH payments, and perform screening as required by OFAC. The rules require Gateway Operators to classify payments that are transmitted to or received from a financial agency[189] outside the

[188] For additional information on the IAT, refer to www.nacha.org/c/IATIndustryInformation.cfm.

[189] "Financial agency" means an entity that is authorized by applicable law to accept deposits or is in the business of issuing money orders or transferring funds.

territorial jurisdiction of the United States as IATs. The classification will depend 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 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 new 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 Operator (FGO): A Gateway Operator that acts as an entry point to or exit point from a foreign country.

Additional Information

The new IAT format increases the amount of originator and beneficiary data that will be available to banks. This additional data may assist banks in their OFAC, anti-money laundering, and monitoring efforts.[190] Examples of information now available to banks under the new 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.

Refer to www.nacha.org for 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

[190] For convenience, this information is sometimes referred to as "Travel Rule" information, but as a technical matter the funds transfer recordkeeping and travel rules at 31 CFR 103.33(g) do not apply to ACH transactions and NACHA operating rules have not changed.

with respect to the processing of ACH entries.[191] NACHA operating rules define TPSPs and relevant subsets of TPSPs that include "Third-Party Senders" and "Sending Points."[192] 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.[193] 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

[191] Third-party service provider is a generic term for any business that provides services to a bank. A third-party payment processor is a specific type of service provider that processes payments such as checks, ACH files, or credit and debit card messages or files. Refer to expanded overview section, "Third-Party Payment Processors," pages 239 to 241, for additional guidance.

[192] When independent TPSPs contract with independent sales organizations or other third-party payment processors, there may be two or more layers between the ODFI and the Originator.

[193] A bank's underwriting policy should define what information each application should contain. The depth of the review of an originator's application should match the level of risk posed by the originator. The underwriting policy should require a background check of each originator to support the validity of the business.

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 GO.
- 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

All parties to an ACH transaction are subject to the requirements of OFAC. (Refer to core overview section, "Office of Foreign Assets Control," pages 147 to 156, for additional guidance.) OFAC has clarified the application of its rules for domestic and cross-border ACH transactions and provided more detailed guidance on cross-border ACH.[194]

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 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

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

policies might involve screening each unbatched ACH record. Similarly, banks that have relationships with third-party service providers 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 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 requirements. For outbound IATs,, 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 core overview section, "Office of Foreign Asset Control," pages 147 to 156, for additional guidance.

In guidance issued on March 10, 2009, OFAC authorized institutions in the United States when they are acting as an ODFI/GO for inbound IAT debits to reject transactions that appear to involve blockable property or property interests.[195] The guidance further stated 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 payments.

Additional information on the types of retail payment systems (ACH payment systems) is available in the FFIEC *Information Technology Examination Handbook*.[196]

---

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

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

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," pages 157 to 159, 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.

Electronic Cash — Overview

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

E-cash (e-money) is a digital representation of money. E-cash comes in several forms, including computer-based, mobile telephone-based, and prepaid cards. Computer e-cash is accessed through personal computer hard disks via a modem or stored in an online repository. Mobile telephone-based e-cash is accessed through an individual's mobile telephone. Prepaid cards, discussed in more detail below, are used to access funds generally held by issuing banks in pooled accounts.

In the case of computer e-cash, monetary value is electronically deducted from the bank account when a purchase is made or funds are transferred to another person. Additional information on types of e-cash products is available in the FFIEC *Information Technology Examination Handbook*.[197]

Risk Factors

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

- Funds may be transferred to or from an unknown third party.
- Customers may be able to avoid border restrictions as the transactions can become mobile and may not be subject to jurisdictional restrictions.
- Transactions may be instantaneous.
- Specific cardholder activity may be difficult to determine by reviewing activity through a pooled account.
- The customer may perceive the transactions as less transparent.

Risk Mitigation

Banks should establish BSA/AML monitoring, identification, and reporting for unusual and suspicious activities occurring through e-cash. Useful MIS for detecting unusual activity on higher-risk accounts include ATM activity reports (focusing on foreign transactions), funds transfer reports, new account activity reports, change of Internet address reports, Internet Protocol (IP) address reports, and reports to identify related or linked accounts (e.g., common addresses, phone numbers, e-mail addresses, and taxpayer identification numbers). The bank also may institute other controls, such as establishing

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

transaction and account dollar limits that require manual intervention to exceed the preset limit.

Prepaid Cards/Stored Value Cards

Consistent with industry practice, the term "prepaid card" is primarily used in this document. Although some sources use the term "stored value card" more broadly, it most commonly refers to cards where the monetary value is physically stored on the card. The term "prepaid card" generally refers to an access device linked to funds held in a pooled account, which is the type of product most frequently offered by U.S. banking organizations. Prepaid cards can cover a variety of products, functionalities, and technologies. Prepaid cards operate within either an "open" or "closed" system. Open-system prepaid cards can be used for purchases at any merchant or to access cash at any automated teller machine (ATM) that connects to the affiliated global payment network. Examples of open system cards are payroll cards and gift cards that can be used anywhere a credit card can be used. Some prepaid cards may be reloaded, allowing the cardholder to add value. Closed-system 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 system cards include merchant-specific retail gift cards, mall cards, and mass transit system cards.

Some prepaid card programs may combine multiple features, such as a flexible spending account card that can be used to purchase specific health services as well as products at a variety of merchants. These programs are often referred to as "hybrid" cards.

Prepaid cards provide a compact and transportable way to maintain and access funds. They also offer individuals without bank accounts an alternative to cash and money orders. As an alternate method of cross-border funds transmittal, 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.

Many banks that offer prepaid card programs do so as issuer or issuing bank. Most payment networks require that their branded prepaid cards be issued by a bank that is a member of that payment network. In addition to issuing prepaid cards, banks may participate in other aspects of a card program such as marketing and distributing cards issued by another financial institution. Banks often rely on multiple third parties to accomplish the design, implementation, and maintenance of their prepaid card programs. These third parties may include program managers, distributors, marketers, merchants, and processors. Under payment network requirements, the issuing bank may have due diligence and other responsibilities relative to these third parties.

Contractual Agreements

Each relationship that a U.S. bank has with another financial institution or third party as part of a prepaid card 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

Money laundering, terrorist financing, and other criminal activity may occur through prepaid card programs if effective controls are not in place. Law enforcement investigations have found that some prepaid cardholders used false identification and funded their initial deposits with stolen credit cards or purchased multiple cards under aliases. In the placement phase of money laundering, because many domestic and offshore banks offer cards with currency access through ATMs internationally, criminals may load cash from illicit sources onto prepaid cards through unregulated load points and send the cards to their accomplices inside or outside the country. Investigations have disclosed that both open and closed system prepaid cards have been used in conjunction with, or as a replacement to, bulk cash smuggling. Third parties involved in prepaid card programs may or may not be subject to regulatory requirements, oversight, and supervision. In addition, these requirements may vary by party.

Prepaid card 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 card program, banks should consider the program's specific features and functionalities. No single indicator is necessarily determinative of lower or higher BSA/AML risk. Higher potential money laundering risk associated with prepaid cards results from the anonymity of the cardholder, fictitious cardholder information, cash access of the card (especially internationally), and the volume of funds that can be transacted on the card. Other risk factors include type and frequency of card loads and transactions, geographic location of card activity, relationships with parties in the card program, card value limits, distribution channels, and the nature of funding sources.

Risk Mitigation

Banks that offer prepaid cards or otherwise participate in prepaid card programs should have policies, procedures, and processes sufficient to manage the related BSA/AML risks. Guidance provided by the Network Branded Prepaid Card Association is an additional resource for banks that provide prepaid card services.[198] Customer due diligence is an important mitigant of BSA/AML risk in prepaid card programs. A bank's CDD program should provide for a risk assessment of all third parties involved in the prepaid card program, considering all relevant factors, including, as appropriate:

---

[198] Refer to "Recommended Practices for Anti-Money Laundering Compliance for U.S.-Based Prepaid Card Programs," February 28, 2008, at www.nbpca.com/docs/NBPCA-AML-Recommended-Practices-080220.pdf

- The identity and location of all third parties involved in the prepaid card program, including any subagents.
- Corporate documentation, licenses, references (including independent reporting services), and, if appropriate, documentation on principal owners.
- The nature of the third-parties' businesses and the markets and customer bases served.
- The information collected to identify and verify cardholder identity.
- The type, purpose, and anticipated activity of the prepaid card program.
- The nature and duration of the bank's relationship with third parties in the card program.
- The BSA/AML and OFAC obligations of third parties.

As part of their system of internal controls, banks should establish a means for monitoring, identifying, and reporting suspicious activity related to prepaid card 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 card transaction information from processors or other third parties. Monitoring systems should have the ability to identify foreign card 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 card loads followed immediately by withdrawals of the full amount from another location.

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

- Limits or prohibitions on cash loads, access, or redemption.
- Limits or prohibitions on amounts of loads and number of loads/reloads within a specific time frame (velocity or speed of fund use).
- Controls on the number of cards purchased by one individual.
- Maximum dollar thresholds on ATM withdrawals and on the number of withdrawals within a specific time frame (velocity or speed of fund use).
- Limits or prohibitions on certain usage (e.g., merchant type) and on geographic usage, such as outside the United States.
- Limits on aggregate card values.

Examination Procedures

Electronic Cash

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

1. Review the policies, procedures, and processes related to e-cash, including prepaid cards. Evaluate the adequacy of the policies, procedures, and processes given the bank's e-cash activities, including prepaid cards, 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 higher-risk e-cash transactions, including prepaid card transactions.

3. Determine whether the bank's system for monitoring e-cash transactions, including prepaid card transactions, 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," pages 157 to 159, for guidance.

Transaction Testing

5. On the basis of the bank's risk assessment of its e-cash activities, including prepaid card activities, as well as prior examination and audit reports, select a sample of e-cash transactions. From the sample selected perform the following examination 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-cash 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),[199] 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 act as a third-party sender of ACH transactions. In either case, the bank does not have a direct relationship with the merchant. The increased use by processor customers, particularly telemarketers, of RCCs also raises the risk of fraudulent payments being processed through the processor's bank account. The Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency have issued guidance regarding the risks, including the BSA/AML risks, associated with banking third-party processors.[200]

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, and illicit transactions or transactions 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

[199] A remotely created check (sometimes called a "demand draft") is a check that is not created by the paying bank (often created by a payee or its service provider), drawn on a customer's bank account. The check often is authorized by the customer remotely, by telephone or online, and, therefore, does not bear the customer's handwritten signature.

[200] Guidance on Payment Processor Relationships, FDIC FIL-127-2008, November 7, 2008, and Risk Management Guidance: Payment Processors, OCC Bulletin 2008-12, April 24, 2008.

implemented an adequate processor-approval program that goes beyond credit risk management, it could be vulnerable to processing illicit or OFAC-sanctioned transactions.

Banks with third party payment processor customers should be aware of the heightened risk of unauthorized returns and use of services by higher-risk merchants. Some higher-risk merchants routinely use third parties to process their transactions because of the difficulty they have in establishing a direct bank relationship. These entities might include certain mail order and telephone order companies, telemarketing companies, illegal online gambling operations, online payday lenders, businesses that are located offshore, and adult entertainment businesses. 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, state incorporation departments, Internet searches, and other investigative processes) 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 will allow processing services. These entities may include higher risk entities such as offshore companies, online gambling-related operations, telemarketers, and online payday lenders. 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.[201]

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

- 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, and geographic location.
- 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.

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.

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

- Merchant base.
- Merchant activities.
- Average number of dollar volume and number of transactions.
- "Swiping" versus "keying" volume for credit card transactions.
- Charge-back history, including rates of return for ACH debit transactions and RCCs.
- Consumer complaints 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. A bank should implement appropriate policies, procedures, and processes that address compliance and fraud risks. High levels of RCCs or ACH debits returned for insufficient funds or as unauthorized can be an indication of fraud or suspicious activity.

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," pages 157 to 159, 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 unauthorized 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 that monetary instruments are sold, determine whether the bank appropriately manages the risk 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.[202]

4. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," pages 157 to 159, for guidance.

[202] Money launderers are known to identify the ownership or source of illegal funds through the use of unique and unusual stamps.

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," pages 147 to 156, or "Customer Identification Program" core examination procedures, pages 59 to 62.[203] 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

[203] For the purpose of the CIP rule, in the case of brokered deposits, the "customer" will be the broker that opens the account. A bank will not need to look through the deposit broker's account to determine the identity of each individual subaccountholder, it need only verify the identity of the named accountholder.

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 targeted customer markets (e.g., foreign or domestic customers) and methods for soliciting clients.
- Determine whether the deposit broker is subject to regulatory oversight.
- Evaluate whether the deposit broker's BSA/AML 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.

Examination Procedures

Brokered Deposits

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

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," pages 157 to 159, 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.[204]

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*.[205]

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.

---

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

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

Risk Factors

Most states do not currently register, limit ownership, monitor, or examine privately owned ATMs or their ISOs.[206] 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, third- and fourth-level 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:

---

[206] FinCEN has issued interpretive guidance, *Application of the Definition of Money Services Business to Certain Owner-Operators of Automated Teller Machines Offering Limited Services,* FIN-2007-G006, December 3, 2007, clarifying the circumstances under which a nonbank owner and operator of an ATM would be a money services business for the purposes of the Bank Secrecy Act and its implementing regulations.

- 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, ascertain the types of businesses in which the ATMs are located, and identify 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. Determine whether the bank obtains information from the ISO regarding due diligence on its sub-ISO arrangements.

Transaction Testing

5. 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.

6. 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.

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

Nondeposit 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 will observe functional supervision requirements of the Gramm–Leach–Bliley Act.[207] Federal banking agencies are responsible for supervising NDIP activity conducted directly by the bank. Different types of networking arrangements may include co-branded products, dual-employee arrangements, or third-party arrangements.

Co-Branded Products

Co-branded products are offered by another company or financial services corporation[208] 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.

---

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

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

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.[209]

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.[210] In addition, the bank may also offer its own

[209] If the bank uses the reliance provision under the CIP, responsibility for CIP shifts to the third-party provider. Refer to core overview section, "Customer Identification Program," pages 52 to 58, for additional information.

[210] In certain circumstances, a bank may not be considered a broker, and an employee need not register as a broker/dealer. Refer to 15 USC 78c(a)(4) for a complete list.

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),[211] 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.

---

[211] Refer to expanded overview section, "Business Entities (Domestic and Foreign)," pages 323 to 328, for additional guidance on PICs.

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. From a review of MIS reports (e.g., exception reports, funds transfer reports, and activity monitoring reports) and internal risk rating factors, determine 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," pages 157 to 159, 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 rules impose AML compliance program requirements and SAR obligations on insurance companies similar to those that apply to banks.[212] 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 of the 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.[213] 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.

---

[212] 31 CFR 103.137 and 31 CFR 103.16.

[213] 70 Fed. Reg. 66758 (November 3, 2005). Also refer to FFIEC Guidance FIN-2006-G015, *Frequently Asked Question, Customer Identification Programs and Banks Serving as Insurance Agents*, December 12, 2006, at www.fincen.gov/final_bank_insurance_agent_faq_12122006.pdf.

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.[214]

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* at www.fincen.gov.

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).[215]
- 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.

---

[214] FinCEN has issued a Frequently Asked Questions document, *Anti-Money Laundering Program and Suspicious Activity Reporting Requirements for Insurance Companies* at www.fincen.gov). Unless the SAR form accommodates multiple filers, only one institution is identified as the filer in the "Filer Identification" section of the SAR form. In these cases, the narrative must include the words "joint filing" and identify the other institutions on whose behalf the report is filed.

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

Risk Mitigation

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

- The identification of 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," pages 157 to 159, 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 recordkeeping for these accounts. Policies should establish guidelines to identify, measure, monitor, and control the risks.

Risk Mitigation

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

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

- Maintaining a comprehensive system that identifies, bank-wide, the general ledger accounts used as concentration accounts, as well as the departments and individuals authorized to use those accounts.
- Requiring dual signatures on general ledger tickets.
- Prohibiting direct customer access to concentration accounts.
- Capturing customer transactions in the customer's account statements.
- Prohibiting customer's knowledge of concentration accounts or their ability to direct employees to conduct transactions through the accounts.

- Retaining appropriate transaction and customer identifying information.
- Frequent reconciling of the accounts by an individual who is independent from the transactions.
- Establishing timely discrepancy resolution process.
- Identifying recurring customer names.

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," pages 157 to 159, 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,[216] trade finance,[217] 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 will vary according to the BSA/AML risks present, but could include performing reference checks, obtaining credit references, verifying the source of collateral, and obtaining tax or financial statements on the borrower and any or all of the various parties involved in the loan.

---

[216] FinCEN has published strategic analytical reports on trends and patterns relating to mortgage loan fraud as well as money laundering through commercial and residential real estate. Refer to www.fincen.gov/news_room/rp/strategic_analytical.html.

[217] Refer to the expanded overview section, "Trade Finance Activities," pages 273 to 277, for additional guidance.

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 higher-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," pages 157 to 159, 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.[218] 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 under-valued in an effort to evade AML 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

[218] Refer to the Financial Action Task Force's report on *Trade Based Money Laundering,* June 23, 2006, at www.fatf-gafi.org/dataoecd/60/25/37038272.pdf.

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," pages 63 to 65, 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.[219] The Wolfsberg Group also has published suggested industry standards and guidance for banks that provide trade finance services.[220]

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

[219] Refer to *Trade Based Money Laundering,* June 23, 2006, at www.fatf-gafi.org/dataoecd/60/25/37038272.pdf.

[220] Refer to *The Wolfsberg Trade Finance Principles*, January 2009, at www.wolfsberg-principles.com/pdf/WG_Trade_Finance_Principles_Final_(Jan_09).pdf.

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.[221] 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," pages 147 to 156, 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," pages 67 to 80, and expanded overview section, "Funds Transfers," pages 213 to 220, 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 noncooperative 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

[221] For instance, U.S. Customs and Border Protection Form 7501 (Entry Summary) (http://forms.cbp.gov/pdf/CBP_Form_7501.pdf) and U.S. Department of Commerce Form 7525-V (Shipper's Export Declaration) (www.census.gov/foreign-trade/regulations/forms/new-7525v.pdf) classify all U.S. imports and exports by 10-digit harmonized codes. (Refer to www.census.gov/foreign-trade/faq/sb/sb0008.html for additional guidance.)

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 structure appears 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. 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 trade-based money laundering (TBML) and black market peso exchange (BMPE) activities, FinCEN requested in the advisory that financial institutions check the appropriate box in the Suspicious Activity Information section of the SAR form and include the abbreviation TBML or BMPE in the narrative section of the SAR. The advisory can be found at www.fincen.gov.

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," pages 157 to 159, 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).[222]
- The facilitation of shell companies and offshore entities (e.g., Private Investment Companies (PIC), international business corporations (IBC), and trusts).[223]
- Lending services (e.g., mortgage loans, credit cards, personal loans, and letters of credit).

---

[222] For additional guidance, refer to the expanded overview and examination procedures, "Trust and Asset Management Services," pages 286 to 290 and 291 to 292, respectively.

[223] For additional guidance, refer to the expanded overview and examination procedures, "Business Entities (Domestic and Foreign)," pages 323 to 328 and 329 to 330, respectively.

- Financial planning services including tax and estate planning.
- Custody services.
- Other services as requested (e.g., mail services).

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

Risk Factors

Private banking services can be vulnerable to money laundering schemes, and past money laundering prosecutions have demonstrated that vulnerability. The 1999 Permanent Subcommittee on Investigations' "Private Banking and Money Laundering: A Case Study of Opportunities and Vulnerabilities"[224] outlined, in part, the following vulnerabilities to money laundering:

- Private bankers as client advocates.
- Powerful clients including politically exposed persons, industrialists, and entertainers.
- Culture of confidentiality and the use of secrecy jurisdictions or shell companies.[225]
- 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)," pages 130 to 134. 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.

---

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

[225] Refer to the expanded overview section, "Business Entities (Domestic and Foreign)," pages 323 to 328, for additional guidance.

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 politically exposed persons (PEP).[226]
- **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.[227] 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

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

[227] Due diligence policies, procedures, and processes are required for private banking accounts for non-U.S. persons by section 312 of the USA PATRIOT Act. Refer to the core overview section, "Private Banking Due Diligence Program (Non-U.S. Persons)," pages 130 to 134, for additional guidance.

(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[228] and to determine whether the account is maintained for non-U.S. persons.[229]

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, long-time customers, banks may find that periodically re-certifying beneficial ownership is effective. A strong CDD program is an effective underlying

[228] 31 CFR 103.121(b)(2)(ii)(C).

[229] Refer to the core examination procedures, "Private Banking Due Diligence Program (Non-U.S. Persons)," pages 135 to 137, for additional guidance.

control through which banks can determine the nature, purpose, and expected use of shell companies and apply appropriate monitoring and documentation standards.

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

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

Given the sensitive nature of private banking and the potential liability associated with it, banks should thoroughly investigate the background of newly hired private banking relationship managers. 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," pages 157 to 159, 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[230] services, and management's ability to implement effective due diligence, monitoring, and reporting systems.*

Trust[231] 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,[232] 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. However, the CIP rule excludes employee benefit accounts established pursuant to the Employee Retirement Income Security Act of 1974 (ERISA).

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"

---

[230] Asset management accounts can be trust or agency accounts and are managed by the bank.

[231] The Office of the Comptroller of the Currency and the Office of Thrift Supervision use the broader term "fiduciary capacity" instead of "trust." Fiduciary capacity includes a trustee, an executor, an administrator, a registrar of stocks and bonds, a transfer agent, a guardian, an assignee, a receiver, or a custodian under a uniform gifts to minors act; an investment adviser, if the bank receives a fee for its investment advice; and any capacity in which the bank possesses investment discretion on behalf of another (12 CFR 9.2(e) and 12 CFR 550.30).

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

individuals with authority or control over such an account, including signatories, in order to verify the customer's identity.[233] For example, in certain circumstances involving revocable trusts, the bank may need to gather information about the settlor, grantor, trustee, or other persons with the authority to direct the trustee, and who thus have authority or control over the account, in order to establish the true identity of the customer.

In the case of an escrow account, if a bank establishes an account in the name of a third party, such as a real estate agent, who is acting as escrow agent, then the bank's customer is the escrow agent. If the bank is the escrow agent, then the person who establishes the account is the bank's customer. For example, if the purchaser of real estate directly opens an escrow account and deposits funds to be paid to the seller upon satisfaction of specified conditions, the bank's customer will be the purchaser. Further, if a company in formation establishes an escrow account for investors to deposit their subscriptions pending receipt of a required minimum amount, the bank's customer will be the company in formation (or if not yet a legal entity, the person opening the account on its behalf). However, the CIP rule also provides that, based on the bank's risk assessment of a new account opened by a customer that is not an individual, the bank may need "to obtain information about" individuals with authority or control over such an account, including signatories, in order to verify the customer's identity.[234]

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.

---

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

[234] *Id.*

- 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),[235] 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),[236] agency accounts, and unidentified beneficiaries). While the majority of traditional trust and asset management accounts will 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.[237] 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," pages 97 to 102, and expanded overview section, "Politically Exposed Persons," pages 297 to 300, for additional guidance.

---

[235] For additional guidance on PICs, refer to the expanded overview section, "Business Entities (Domestic and Foreign)," pages 323 to 328.

[236] APTs are a special form of irrevocable trust, usually created (settled) offshore for the principal purposes of preserving and protecting part of one's wealth against creditors. Title to the asset is transferred to a person named as the trustee. APTs are generally tax neutral with the ultimate function of providing for the beneficiaries.

[237] Management and examiners should be aware that OFAC list-matching is not a BSA requirement. However, because trust systems are typically separate and distinct from bank systems, verification of these checks on the bank system is not sufficient to ensure that these checks are also completed in the trust and asset management department. Moreover, OFAC's position is that an account beneficiary has a future or contingent interest in funds in an account and, consistent with a bank's risk profile, beneficiaries should be screened to assure OFAC compliance. Refer to the core overview section, "Office of Foreign Assets Control," pages 147 to 156, for additional guidance.

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.[238]
- Interest on lawyers' trust accounts (IOLTA) holding and processing significant dollar amounts.

[238] For additional guidance, refer to the expanded overview section, "Nongovernmental Organizations and Charities," pages 320 to 321.

- 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[239] 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," pages 19 to 21, 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," pages 157 to 159, for guidance.

---

[239] Asset management accounts can be trust or agency accounts and are managed by the bank.

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.

EXPANDED EXAMINATION OVERVIEW AND PROCEDURES FOR PERSONS AND ENTITIES

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,[240] 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

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

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," pages 301 to 302, 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.[241]

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)," pages 130 to 137, and the expanded overview and examination procedures, "Politically Exposed Persons," pages 297 to 302.

---

[241] Additional information can be found at www.irs.gov/formspubs. Also refer to IRS Bulletin 515 *Withholding of Tax on Nonresident Aliens and Foreign Entities*.

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," pages 157 to 159, 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 [242] refer to core overview section, "Private Banking Due Diligence Program (Non-U.S. Persons)," pages 130 to 134, 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 will 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.[243] 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.[244] 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.

---

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

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

[243] *Guidance on Enhanced Scrutiny for Transactions that may Involve the Proceeds for Foreign Official Corruption* issued by the U.S. Treasury, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision, and the U.S. Department of State, January 2001.

[244] It is important to note that while government-owned corporations may present risks of their own, the government-owned corporations themselves are not within the definition of a "senior foreign political figure."

- 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.[245] 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.[246] 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 will vary 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

[245] 71 Fed. Reg. 495–515.

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

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 will vary 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 will vary depending upon 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)," pages 130 to 134, 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 [247] refer to core overview section, "Private Banking Due Diligence Program (Non-U.S. Persons," pages 130 to 134, 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," pages 157 to 159, 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:

---

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

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

- 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 and Foreign Consulate Accounts — Overview

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

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.[248]

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

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

Risk Factors

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

- Accounts are from countries that have been designated as higher risk.
- Substantial currency transactions take place in the accounts.

[248] For additional guidance, refer to the expanded overview section, "Politically Exposed Persons," pages 297 to 300.

- Account activity is not consistent with the purpose of the account (e.g., pouch activity or payable upon proper identification transactions).
- Accounts directly fund personal expenses of foreign nationals, including but not limited to expenses for college students.
- Official embassy business is conducted through personal accounts.

Risk Mitigation

Banks should obtain comprehensive due diligence information on embassy and foreign consulate account relationships. For private banking accounts for non-U.S. persons specifically, banks must obtain due diligence information as required by 31 CFR 103.178.[249] The bank's due diligence related to embassy and foreign consulate account relationships should be commensurate with the risk levels presented. In addition, banks are expected to establish policies, procedures, and processes that provide for greater scrutiny and monitoring of all embassy and foreign consulate account relationships. Management should fully understand the purpose of the account and the expected volume and nature of account activity. Ongoing monitoring of embassy and foreign consulate account relationships is critical to ensuring that the account relationships are being used as anticipated.

[249] For additional guidance, refer to the core section overview, "Private Banking Due Diligence Program (Non-U.S. Persons)," pages 130 to 134.

Examination Procedures

Embassy and Foreign Consulate Accounts

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

1. Review the policies, procedures, and processes related to embassy and foreign consulate accounts. Evaluate the adequacy of the policies, procedures, and processes given the bank's embassy and foreign consulate 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 and foreign consulate accounts. Determine whether the board is aware of embassy 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 and foreign consulate accounts, particularly those that pose a higher risk for money laundering.

4. Determine whether the bank's system for monitoring embassy and foreign consulate 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," pages 157 to 159, for guidance.

Transaction Testing

6. On the basis of the bank's risk assessment of its embassy and foreign consulate accounts, as well as prior examination and audit reports, select a sample of embassy and foreign consulate 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 and foreign consulate 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.[250] 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).[251]
- Insurance companies.
- Other financial institutions (e.g., dealers in precious metals, stones, or jewels; pawnbrokers; loan or finance companies).

Some NBFIs are currently required to develop an AML program, comply with the reporting and recordkeeping requirements of the BSA, and report suspicious activity, as are 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 will not be 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

[250] Refer to Appendix D ("Statutory Definition of Financial Institution") for guidance.

[251] MSBs include five distinct types of financial services providers and the U.S. Postal Service: (1) currency dealers or exchangers; (2) check cashers; (3) issuers of traveler's checks, money orders, or stored value; (4) sellers or redeemers of traveler's checks, money orders, or stored value; and (5) money transmitters. There is a threshold requirement for businesses in the first four categories: a business that engages in such transactions will 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 103.11(uu)). FinCEN routinely publishes administrative letter rulings that address inquiries regarding whether persons who engage in certain specific business activities are MSBs. Refer to www.fincen.gov/financial_institutions/rulings.html.

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 by customers.
- Maintain limited or inconsistent recordkeeping on customers and transactions.
- Engage in frequent currency transactions.
- Are subject to varying levels of regulatory requirements and oversight.
- Can quickly change their product mix or location and quickly enter or exit an operation.
- Sometimes operate without proper registration or licensing.

Risk Mitigation

Banks that maintain account relationships with NBFIs should develop policies, procedures, and processes to:

- Identify 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, it will be 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.[252] 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.[253] Existing FinCEN regulations require certain MSBs to register with FinCEN.[254] 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.

The following regulatory expectations apply to banks with MSB customers:

---

[252] Refer to Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States, April 26, 2005, available at www.fincen.gov.

[253] Refer to 31 CFR 103.125 (requirement for money services businesses (MSBs) to establish and maintain an anti-money laundering program); 31 CFR 103.22 (requirement for MSBs to file Currency Transaction Reports); 31 CFR 103.20 (requirement for MSBs to file Suspicious Activity Reports, other than for check cashing and stored value transactions); 31 CFR 103.29 (requirement for MSBs that sell money orders, traveler's checks, or other monetary instruments for currency to verify the identity of the customer and create and maintain a record of each currency purchase between $3,000 and $10,000, inclusive); 31 CFR 103.33(f) and (g) (rules applicable to certain transmittals of funds); and 31 CFR 103.37 (additional recordkeeping requirement for currency exchangers including the requirement to create and maintain a record of each exchange of currency in excess of $1,000).

[254] Refer to 31 CFR 103.41. All MSBs must register with FinCEN (whether or not licensed as an MSB by any state) except: a business that is an MSB solely because it serves as an agent of another MSB; a business that is an MSB solely as an issuer, seller, or redeemer of stored value; the U.S. Postal Service; and agencies of the United States, of any state, or of any political subdivision of any state. A business that acts as an agent for a principal or principals engaged in MSB activities, and that does not on its own behalf perform any other services of a nature or value that would cause it to qualify as an MSB, is not required to register with FinCEN. FinCEN has issued guidance on MSB registration and de-registration. Refer to FIN-2006-G006, *Registration and De-Registration of Money Services Businesses*, February 3, 2006, at www.fincen.gov.

- 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 will not be held responsible for the MSB's BSA/AML program.

- Not all MSBs pose the same level of risk, and not all MSBs will 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 will be 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.[255]
- 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).

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

[255] On December 9, 2008, FinCEN and the Internal Revenue Service released the *Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses* (MSB Exam Manual), which was developed in collaboration with the Conference of State Bank Supervisors, the Money Transmitter Regulators Association, and state agencies responsible for MSB regulation. Refer to the MSB Exam Manual, available at www.fincen.gov.

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 will be 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 will 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 will 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[256] are:

- Apply the bank's CIP.[257]
- 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 will be receiving services directly or indirectly through the MSB account.

---

[256] Refer to Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States, April 26, 2005, available at www.fincen.gov.

[257] Refer to 31 CFR 103.121 (FinCEN); 12 CFR 21.21 (Office of the Comptroller of the Currency); 12 CFR 208.63(b), 211.5(m), 211.24(j) (Board of Governors of the Federal Reserve System); 12 CFR 326.8(b)(2) (Federal Deposit Insurance Corporation); 12 CFR 563.177(b) (Office of Thrift Supervision); 12 CFR 748.2(b) (National Credit Union Administration).

- 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:

   - 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.

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.

   7. 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," pages 90 to 94,

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," pages 157 to 159, 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.[258]

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).

[258] *Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities*, September 2006, is available at www.treasury.gov/offices/enforcement/key-issues/protecting/index.shtml.

- 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

Nongovernmental 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," pages 157 to 159, 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[259] business entity that may pose heightened risks.[260] 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.[261]

---

[259] The term "domestic" refers to entities formed or organized in the United States. These entities may have no other connection to the United States, and ownership and management of the entities may reside abroad.

[260] The term "shell company" generally refers to an entity without a physical presence in any country. FinCEN has issued guidance alerting financial institutions to the potential risks associated with providing financial services to shell companies and reminding them of the importance of managing those risks. Refer to FIN-2006-G014, *Potential Money Laundering Risks Related to Shell Companies*, November 2006, at www.fincen.gov.

[261] Refer to GAO, *Company Formations — Minimal Ownership Information is Collected and Available*, GAO-06-376, April 2006, at www.gao.gov/new.items/d06376.pdf. For additional information, Refer to *Failure to Identify Company Owners Impedes Law Enforcement*, Senate Hearing 109-845, held on November 14, 2006, at hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=4478b046-2b7e-4dd0-b061-efabbdbbf844, and *Tax Haven Abuses: The Enablers, The Tools & Secrecy*, Senate Hearing 109-797, held on August 1, 2006, (particularly the Joint Report of the Majority and Minority Staffs of the Permanent Subcommittee on Investigations), at hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=79a104cf-75cb-44aa-ae20-32301fa3c349.

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 which 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 which include, but are not limited to, the following:

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

Through an IBC, an individual is able to conduct the following:

- Open and hold bank accounts.
- Hold and transfer funds.
- Engage in international business and other related transactions.
- Hold and manage offshore investments (e.g., stocks, bonds, mutual funds, and certificates of deposit), many of which may not be available to "individuals" depending on their location of residence.
- Hold corporate debit and credit cards, thereby allowing convenient access to funds.

Private Investment Companies

PICs are separate legal entities. 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 incorporated frequently 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.[262]

---

[262] Money Laundering Threat Assessment Working Group, *U.S. Money Laundering Threat Assessment*, December 2005.

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.[263] 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 will disclose true ownership. Overall, the lack of ownership transparency; minimal or no recordkeeping requirements, financial disclosures, and supervision; and the range of permissible activities all increase money laundering risk.

While 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.[264] 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.[265]

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).

---

[263] For a general discussion of the risk factors associated with the misuse of business entities, refer to the Financial Action Task Force's *The Misuse of Corporate Vehicles, Including Trust and Company Service Providers,* October 13, 2006, at www.fatf-gafi.org.

[264] Failure to Identify Company Owners Impedes Law Enforcement. Refer to Senate Hearing 109-845 held on November 14, 2006.

[265] The federal banking agencies notify banks and the public about entities engaged in unauthorized banking activities, both offshore and domestic. These notifications can be found on the federal banking agencies' Web sites.

- 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 103.121 to obtain information about the individuals who have authority and control over such accounts in order to verify the customer's identity (the customer being the 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 that will be 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," pages 157 to 159, 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 will most likely be higher in comparison with similar restaurants in the area. The nature of cash-intensive businesses and the difficulty in identifying unusual activity may cause these businesses to be considered 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,[266] 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.

[266] As discussed in the core overview section, "Currency Transaction Reporting Exemptions," pages 90 to 94, certain entities are ineligible for currency transaction reporting exemptions as a non-listed business.

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," pages 157 to 159, 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. 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.

Appendix A: BSA Laws and Regulations

Statutes

12 USC 1829b, 12 USC 1951–1959, and 31 USC 5311, *et seq.* — "The Bank Secrecy Act"

12 USC 1818(s) — "Compliance with Monetary Recordkeeping and Report Requirements"
Requires that the appropriate federal banking agencies shall prescribe regulations requiring insured depository institutions to establish and maintain procedures reasonably designed to assure and monitor the compliance of such depository institutions with the requirements of the BSA. In addition, this section requires that each examination of an insured depository institution by the appropriate federal banking agency shall include a review of the procedures, and that the report of examination shall describe any problem with the procedures maintained by the insured depository institution. Finally, if the appropriate federal banking agency determines that an insured depository institution has either 1) failed to establish and maintain procedures that are reasonably designed to assure and monitor the institution's compliance with the BSA; or 2) failed to correct any problem with the procedures that a report of examination or other written supervisory communication identifies as requiring communication to the institution's board of directors or senior management as a matter that must be corrected, the agency shall issue an order requiring such depository institution to cease and desist from the violation of the statute and the regulations prescribed thereunder. Sections 1818(b)(3) and (b)(4) of Title 12 of the USC extend section 1818(s) beyond insured depository institutions.

12 USC 1786(q) — "Compliance with Monetary Recordkeeping and Report Requirements"
Requires that the NCUA Board prescribe regulations requiring insured credit unions to establish and maintain procedures reasonably designed to assure and monitor the compliance of such credit unions with the requirements of the BSA. In addition, this section requires the NCUA Board to examine and enforce BSA requirements.

Regulations

U.S. Treasury/FinCEN

31 CFR 103 — "Financial Recordkeeping and Reporting of Currency and Foreign Transactions"
Sets forth FinCEN regulations that promulgate the BSA. Select provisions are described below.

31 CFR 103.11 — "Meaning of Terms"
Sets forth the definitions used throughout 31 CFR Part 103.

31 CFR 103.16 — "Reports by Insurance Companies of Suspicious Transactions"
Sets forth the requirements for insurance companies to report suspicious transactions of $5,000 or more.

31 CFR 103.18 — "Reports by Banks of Suspicious Transactions"
Sets forth the requirements for banks to report suspicious transactions involving or aggregating $5,000 or more.

31 CFR 103.22 — "Reports of Transactions in Currency"
Sets forth the requirements for financial institutions to report currency transactions in excess of $10,000. Includes 31 CFR 103.22(d) — "Transactions of Exempt Persons," which sets forth the requirements for financial institutions to exempt transactions of certain persons from currency transaction reporting requirements.

31 CFR 103.23 — "Reports of Transportation of Currency or Monetary Instruments"
Sets forth the requirements for filing a Report of International Transportation of Currency or Monetary Instruments (CMIR).

31 CFR 103.24 — "Reports of Foreign Financial Accounts"
Sets forth the requirement that each person having a financial interest in, or signature or other authority over, a financial account in a foreign country must file a report with the IRS annually.

31 CFR 103.27 — "Filing of Reports"
Sets forth the filing and recordkeeping requirements for CTRs, CMIRs, and Report of Foreign Bank and Financial Accounts (FBAR).

31 CFR 103.28 — "Identification Required"
Sets forth the requirement that financial institutions verify the identity of persons conducting currency transactions in excess of $10,000.

31 CFR 103.29 — "Purchases of Bank Checks and Drafts, Cashier's Checks, Money Orders and Traveler's Checks"
Sets forth the requirements that financial institutions maintain records relating to purchases of monetary instruments with currency in amounts between $3,000 and $10,000, inclusive.

31 CFR 103.32 — "Records to Be Made and Retained by Persons Having Financial Interests in Foreign Financial Accounts"
Sets forth the requirement that persons having a financial interest in, or signature or other authority over, financial account in a foreign country maintain records relating to foreign financial bank accounts reported on an FBAR.

31 CFR 103.33 — "Records to Be Made and Retained by Financial Institutions"
Sets forth recordkeeping and retrieval requirements for financial institutions, including funds transfer recordkeeping and transmittal requirements.

31 CFR 103.34 — "Additional Records to Be Made and Retained by Banks"
Sets forth additional recordkeeping requirements for banks.

31 CFR 103.38 — "Nature of Records and Retention Period"
Sets forth acceptable forms of records required to be kept and establishes a five-year record-retention requirement.

31 CFR 103.41 — "Registration of Money Services Businesses"
Sets forth the requirements for money services businesses to register with the U.S. Treasury/FinCEN.

31 CFR 103.57 — "Civil Penalty"
Sets forth potential civil penalties for willful or negligent violations of 31 CFR Part 103.

31 CFR 103.59 — "Criminal Penalty"
Sets forth potential criminal penalties for willful violations of 31 CFR Part 103.

31 CFR 103.63 — "Structured Transactions"
Prohibits the structuring of transactions to avoid currency transaction reporting requirement.

31 CFR 103.100 — "Information Sharing Between Federal Law Enforcement Agencies and Financial Institutions"
Establishes procedures for information sharing between federal law enforcement authorities and financial institutions to deter terrorist activity and money laundering.

31 CFR 103.110 — "Voluntary Information Sharing Among Financial Institutions"
Establishes procedures for voluntary information sharing among financial institutions to deter terrorist activity and money laundering.

31 CFR 103.120 — "Anti-Money Laundering Program Requirements for Financial Institutions Regulated by a Federal Functional Regulator or a Self-Regulatory Organization, and Casinos"
Establishes, in part, the standard that a financial institution regulated only by a federal functional regulator satisfies statutory requirements to establish an AML program if the financial institution complies with the regulations of its federal functional regulator governing such programs.

31 CFR 103.121 — "Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks"
Sets forth the requirement for banks, savings associations, credit unions, and certain non-federally regulated banks to implement a written Customer Identification Program.

31 CFR 103.137 — "Anti-Money Laundering Programs for Insurance Companies"
Sets forth the requirement for insurance companies that issue or underwrite "covered products" to develop and implement a written AML program that is reasonably designed to prevent the insurance company from being used to facilitate money laundering or financing of terrorist activity.

31 CFR 103.176 — "Due Diligence Programs for Correspondent Accounts for Foreign Financial Institutions"
Sets forth the requirement for certain financial institutions to establish and apply 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 financial institution to detect and report known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed by the financial institution in the United States for a foreign financial institution.

31 CFR 103.177 — "Prohibition on Correspondent Accounts for Foreign Shell Banks; Records Concerning Owners of Foreign Banks and Agents for Service of Legal Process"
Prohibits a covered financial institution from establishing, maintaining, administering, or managing a correspondent account in the United States for or on behalf of a foreign shell bank, and requires the financial institution to maintain records identifying the owners of foreign financial institutions and regarding a person resident in the United States who is authorized to and has agreed to be an agent to receive service of legal process.

31 CFR 103.178 — "Due Diligence Programs for Private Banking Accounts"
Sets forth the requirement for certain financial institutions to 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 that is established, maintained, administered, or managed in the United States for a non-U.S. person.

31 CFR 103.185 — "Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationship"
Requires a financial institution to provide foreign financial institution records upon the request of an appropriate law enforcement official and to terminate a correspondent relationship with a foreign financial institution upon receipt of written notice from the U.S. Secretary of the Treasury or the U.S. Attorney General.

31 CFR 103, Subpart I, Appendix A — "Certification Regarding Correspondent Accounts for Foreign Banks"
Voluntary certification form to be obtained by a bank that establishes, maintains, administers, or manages a correspondent account in the United States for or on behalf of a foreign bank.

31 CFR 103, Subpart I, Appendix B — "Recertification Regarding Correspondent Accounts for Foreign Banks"
Voluntary re-certification form to be obtained by a bank that establishes, maintains, administers, or manages a correspondent account in the United States for or on behalf of a foreign bank.

Board of Governors of the Federal Reserve System

Regulation H — 12 CFR 208.62 — "Suspicious Activity Reports"
Sets forth the requirements for state member banks for filing a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.

Regulation H — 12 CFR 208.63 — "Procedures for Monitoring Bank Secrecy Act Compliance"
Sets forth the requirements for state member banks to establish and maintain procedures to ensure and monitor their compliance with the BSA.

Regulation K — 12 CFR 211.5(k) — "Reports by Edge and Agreement Corporations of Crimes and Suspected Crimes"
Sets forth the requirements for an Edge and agreement corporation, or any branch or subsidiary thereof, to file a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.

Regulation K — 12 CFR 211.5(m) — "Procedures for Monitoring Bank Secrecy Act Compliance"
Sets forth the requirements for an Edge and agreement corporation to establish and maintain procedures reasonably designed to ensure and monitor compliance with the BSA and related regulations.

Regulation K — 12 CFR 211.24(f) — "Reports of Crimes and Suspected Crimes"
Sets forth the requirements for an uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States to file a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.

Regulation K — 12 CFR 211.24(j) — "Procedures for Monitoring Bank Secrecy Act Compliance"
Sets forth the requirements for an uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States to establish and maintain procedures reasonably designed to ensure and monitor compliance with the BSA and related regulations.

Regulation Y — 12 CFR 225.4(f) — "Suspicious Activity Report"
Sets forth the requirements for a bank holding company or any nonbank subsidiary thereof, or a foreign bank that is subject to the Bank Holding Company Act or any nonbank subsidiary of such a foreign bank operating in the United States, to file a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.

Federal Deposit Insurance Corporation

12 CFR 326 Subpart B — "Procedures for Monitoring Bank Secrecy Act Compliance"
Sets forth requirements for state nonmember banks to establish and maintain procedures to ensure and monitor their compliance with the BSA.

12 CFR 353 — "Suspicious Activity Reports"
Establishes requirements for state nonmember banks to file a SAR when they detect a known or suspected violation of federal law, a suspicious transaction relating to a money laundering activity, or a violation of the BSA.

National Credit Union Administration

12 CFR 748 — "Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance"
Requires federally insured credit unions to maintain security programs and comply with the BSA.

12 CFR 748.1 — "Filing of Reports"
Requires federally insured credit unions to file compliance and Suspicious Activity Reports.

12 CFR 748.2 — "Procedures for Monitoring Bank Secrecy Act (BSA) Compliance"
Ensures that all federally insured credit unions establish and maintain procedures reasonably designed to assure and monitor compliance with the recordkeeping and reporting requirements in the BSA.

Office of the Comptroller of the Currency

12 CFR 21.11 — "Suspicious Activity Report"
Ensures that national banks file a Suspicious Activity Report when they detect a known or suspected violation of federal law or a suspicious transaction related to a money laundering activity or a violation of the BSA. This section applies to all national banks as well as any federal branches and agencies of foreign financial banks licensed or chartered by the OCC.

12 CFR 21.21 — "Procedures for Monitoring Bank Secrecy Act (BSA) Compliance"
Requires all national banks to establish and maintain procedures reasonably designed to assure and monitor their compliance with the requirements of subchapter II of chapter 53 of title 31, United States Code, and the implementing regulations promulgated thereunder by the Department of the Treasury at 31 CFR part 103.

Office of Thrift Supervision

12 CFR 563.177 — "Procedures for Monitoring Bank Secrecy Act (BSA) Compliance"
Requires savings associations to implement a program to comply with the recordkeeping and reporting requirements in the BSA.

12 CFR 563.180 — "Suspicious Activity Reports and Other Reports and Statements"
Sets forth the rules for savings associations or service corporations for filing a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.

Appendix B: BSA/AML Directives

Board of Governors of the Federal Reserve System

Supervision and Regulation Letters, commonly known as SR Letters, address significant policy and procedural matters related to the Federal Reserve System's supervisory responsibilities. Issued by the Board of Governors' Division of Banking Supervision and Regulation, SR Letters are an important means of disseminating information to banking supervision staff at the Board of Governors and the Reserve Banks and, in some instances, to supervised banking organizations. The applicable BSA/AML SR Letters are available at the following Web site: www.federalreserve.gov/boarddocs/srletters.

Federal Deposit Insurance Corporation

Financial Institution Letters (FIL) are addressed to the chief executive officers of the financial institutions on the FILs distribution list — generally, FDIC-supervised banks. FILs may announce new regulations and policies, new FDIC publications, and a variety of other matters of principal interest to those responsible for operating a bank or savings association. The applicable FILs are available at the following Web site: www.fdic.gov/news/news/financial/index.html.

National Credit Union Administration

National Credit Union Administration (NCUA) publishes Letters to Credit Unions (LCU) and Regulatory Alerts (RA) addressed to credit union boards of directors. LCUs and RAs are used to share information, announce new policies, and provide guidance for credit unions and credit union examination staff. The NCUA's Examiner's Guide provides overall guidance for the risk-focused examination and supervision of federally insured credit unions. NCUA's risk-focused program evaluates the degree to which credit union management identifies, measures, monitors, and controls (i.e., manages) existing and potential risks in their operations, including risk associated with AML programs. Applicable sections of the Examiner's Guide are available on the following Web site: www.ncua.gov.

Office of the Comptroller of the Currency

OCC Alerts are issuances published with special urgency to notify bankers and examiners of matters of pressing concern, often suspicious or illegal banking practices. OCC Bulletins and Advisory Letters contain information of continuing importance to bankers and examiners. Bulletins and Advisory Letters remain in effect until revised or rescinded. Specific BSA/AML OCC Alerts, Bulletins, and Advisory Letters are available at the following Web site: www.occ.treas.gov.

Office of Thrift Supervision

The Office of Thrift Supervision issues Regulatory Bulletins and CEO Letters to clarify regulations and to specify guidelines and procedures. These directives are an important means to keep examiners as well as savings associations continuously updated on BSA/AML issues. Specific BSA/AML Regulatory Bulletins and CEO Letters are available at the following Web site: www.ots.treas.gov.

Appendix C: BSA/AML References

Web Sites

Board of Governors of the Federal Reserve System
www.federalreserve.gov

Federal Deposit Insurance Corporation
www.fdic.gov

National Credit Union Administration
www.ncua.gov

Office of the Comptroller of the Currency
www.occ.treas.gov

Office of Thrift Supervision
www.ots.treas.gov

Financial Crimes Enforcement Network
www.fincen.gov

Office of Foreign Assets Control
www.treasury.gov/offices/enforcement/ofac

Federal Financial Institutions Examination Council
www.ffiec.gov

Manuals or Handbooks

Federal Reserve Commercial Bank Examination Manual

Federal Reserve Bank Holding Company Supervision Manual

Federal Reserve Examination Manual for U.S. Branches and Agencies of Foreign Banking Organizations

Federal Reserve Guidelines and Instructions for Examinations of Edge Corporations

FDIC Manual of Examination Policies

NCUA Compliance Self-Assessment Manual

NCUA Examiner's Guide

OCC Comptroller's Handbook — Asset Management

OCC Comptroller's Handbook — Community Bank Supervision

OCC Comptroller's Handbook — Compliance

OCC Comptroller's Handbook — Large Bank Supervision

OCC Money Laundering: A Banker's Guide to Avoiding Problems

OTS Examination Handbook

Other Materials

Federal Financial Institutions Examination Council (FFIEC)

The FFIEC's Web site (www.ffiec.gov) includes the following information:

- *BSA/AML Examination Manual* InfoBase
- *Information Technology Handbook* InfoBase

U.S. Government

Interagency U.S. Money Laundering Threat Assessment (MLTA) (December 2005)

The MLTA is a government-wide analysis of money laundering in the United States. The MLTA offers a detailed analysis of money laundering methods, ranging from well-established techniques for integrating dirty money into the financial system to modern innovations that exploit global payment networks as well as the Internet. (www.treas.gov/press/releases/reports/js3077_01112005_MLTA.pdf)

Financial Crimes Enforcement Network (FinCEN)

FinCEN's Web site (www.fincen.gov) includes, among a range of other material and information, the following:

- BSA Statutory Material, BSA Regulations, and *Federal Register* Notices — Links to legislation and regulations, as well as to proposed regulations.
- BSA Forms — Links to BSA reporting forms and corresponding preparation and filing instructions.
- BSA Guidance — FinCEN issues interpretations of BSA regulations as well as guidance to financial institutions on complying with the same.
- Reports — FinCEN periodically initiates and develops reports and publications covering AML issues, including the SAR Activity Review.
- Advisories — FinCEN issues advisories to financial institutions concerning money laundering or terrorist financing threats and vulnerabilities, for the purpose of enabling financial institutions to guard against such threats.
- Enforcement actions — FinCEN issues releases involving the assessment of civil money penalties against financial institutions for systemic noncompliance with the BSA.

Basel Committee on Banking Supervision (BCBS)

The BCBS Web site (on the Bank for International Settlements' Web site, www.bis.org) includes the following publications:

- Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-Border Wire Transfers
- Consolidated Know Your Customer Risk Management
- Sharing of Financial Records Between Jurisdictions in Connection with the Fight Against Terrorist Financing
- General Guide to Account Opening and Customer Identification
- Customer Due Diligence for Banks
- Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering
- Banking Secrecy and International Cooperation in Banking Supervision

Financial Action Task Force on Money Laundering (FATF)

FATF's Web site (www.fatf-gafi.org) includes the following publications:

- Forty Recommendations to Combat Money Laundering and Terrorism
- Special Recommendations Against Terrorist Financing
- Interpretive Notes to FATF Recommendations
- Noncooperative Countries or Territories
- Typologies on Money Laundering Risk
- Trade Based Money Laundering
- New Payment Methods
- The Misuse of Corporate Vehicles, Including Trust and Company Service Providers
- Complex Money Laundering Techniques — Regional Perspectives Report

The Clearing House Payments Co., LLC

The Clearing House's Web site (www.theclearinghouse.org) includes this publication: Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking

NACHA — The Electronic Payments Association (NACHA)

NACHA's Web site (www.nacha.org) includes the following:

- "The Next Generation ACH Task Force: Future Vision of the ACH Network"
- NACHA Operating Rules

The Wolfsberg Group

The Wolfsberg Group's Web site (www.wolfsberg-principles.com) includes the following:

- Wolfsberg AML Principles on Private Banking
- Wolfsberg Statement on the Suppression of the Financing of Terrorism
- Wolfsberg Statement on Payment Message Standards
- Wolfsberg AML Principles for Correspondent Banking
- Wolfsberg Statement on Monitoring Screening and Searching
- Wolfsberg Guidance on Risk Based Approach for Managing Money Laundering Risks
- Wolfsberg FAQs on Correspondent Banking
- Wolfsberg Trade Finance Principles
- Wolfsberg Statement on AML Screening, Monitoring and Searching 2009

Appendix D: Statutory Definition of Financial Institution

As defined in the BSA 31 USC 5312(a)(2), the term "financial institution" includes the following:

- An insured bank (as defined in section 3(h) of the FDI Act (12 USC 1813(h))).
- A commercial bank or trust company.
- A private banker.
- An agency or branch of a foreign bank in the United States.
- Any credit union.
- A thrift institution.
- A broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934 (15 USC 78a *et seq.)*.
- A broker or dealer in securities or commodities.
- An investment banker or investment company.
- A currency exchange.
- An issuer, redeemer, or cashier of traveler's checks, checks, money orders, or similar instruments.
- An operator of a credit card system.
- An insurance company.
- A dealer in precious metals, stones, or jewels.
- A pawnbroker.
- A loan or finance company.
- A travel agency.
- A licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system.
- A telegraph company.

- A business engaged in vehicle sales, including automobile, airplane, and boat sales.
- Persons involved in real estate closings and settlements.
- The United States Postal Service.
- An agency of the United States government or of a state or local government carrying out a duty or power of a business described in this paragraph.
- A casino, gambling casino, or gaming establishment with an annual gaming revenue of more than $1,000,000 that —
    - Is licensed as a casino, gambling casino, or gaming establishment under the laws of any state or any political subdivision of any state; or
    - Is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation that is limited to class I gaming (as defined in section 4(6) of such act).
- Any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity that is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage.
- Any other business designated by the Secretary whose currency transactions have a high degree of usefulness in criminal, tax, or regulatory matters.
- Any futures commission merchant, commodity trading advisor, or commodity pool operator registered, or required to register, under the Commodity Exchange Act (7 USC 1, *et seq.*).

Appendix E: International Organizations

Money laundering and terrorist financing can have a widespread international impact. Money launderers have been found to transfer funds and maintain assets on a global level, which makes tracing funds through various countries a complex and challenging process. Most countries support the fight against money laundering and terrorist funding; however, because of the challenges in creating consistent laws or regulations between countries, international groups have developed model recommendations for governments and financial institutions. Two key international bodies in this area follow:

- **The Financial Action Task Force on Money Laundering (FATF)** is an intergovernmental body established for the development and promotion of policies to combat money laundering and terrorist financing. The FATF has developed recommendations on various money laundering and terrorist financing issues published in the "FATF Forty Recommendations" and the "Special Recommendations on Terrorist Financing."[267]

- **The Basel Committee on Banking Supervision** is a committee of central banks and bank supervisors and regulators from numerous jurisdictions that meets at the Bank for International Settlements (BIS) in Basel, Switzerland, to discuss issues related to prudential banking supervision. The Basel Committee formulates broad standards and guidelines and makes recommendations regarding sound practices, including those on customer due diligence.

In addition, other global organizations are becoming increasingly involved in combating money laundering. The International Monetary Fund (IMF) and the World Bank have integrated AML and counter-terrorist financing issues into their financial sector assessments, surveillance, and diagnostic activities. Furthermore, various FATF-style regional bodies exist. These groups participate as observers in FATF meetings; assess their members against the FATF standards; and, like FATF members, frequently provide input to the IMF and World Bank assessment program.

---

[267] Another well-known FATF initiative is its noncooperative countries and territories (NCCT) exercise, wherein jurisdictions have been identified as NCCT. Currently, there are no countries on the list. However, on February 18, 2010, FATF issued a list of jurisdictions that are subject to countermeasures, have AML deficiencies that have not been addressed, or have deficiencies that in the process of being addressed. That list can be found at FATF's Web site at www.fatf-gafi.org/dataoecd/34/29/44636171.pdf.

Appendix F: Money Laundering and Terrorist Financing "Red Flags"

The following are examples of potentially suspicious activities, or "red flags" for both money laundering and terrorist financing. Although these lists are not all-inclusive, they may help banks and examiners recognize possible money laundering and terrorist financing schemes. Management's primary focus should be on reporting suspicious activities, rather than on determining whether the transactions are in fact linked to money laundering, terrorist financing, or a particular crime.

The following examples are red flags that, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny should help to determine whether the activity is suspicious or one for which there does not appear to be a reasonable business or legal purpose.

Potentially Suspicious Activity That May Indicate Money Laundering

Customers Who Provide Insufficient or Suspicious Information

- A customer uses unusual or suspicious identification documents that cannot be readily verified.
- A customer provides an individual tax identification number after having previously used a Social Security number.
- A customer uses different tax identification numbers with variations of his or her name.
- A business is reluctant, when establishing a new account, to provide complete information about the nature and purpose of its business, anticipated account activity, prior banking relationships, the names of its officers and directors, or information on its business location.
- A customer's home or business telephone is disconnected.
- The customer's background differs from that which would be expected on the basis of his or her business activities.
- A customer makes frequent or large transactions and has no record of past or present employment experience.
- A customer is a trust, shell company, or Private Investment Company that is reluctant to provide information on controlling parties and underlying beneficiaries. Beneficial owners may hire nominee incorporation services to establish shell companies and open bank accounts for those shell companies while shielding the owner's identity.

Efforts to Avoid Reporting or Recordkeeping Requirement

- A customer or group tries to persuade a bank employee not to file required reports or maintain required records.
- A customer is reluctant to provide information needed to file a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed.
- A customer is reluctant to furnish identification when purchasing negotiable instruments in recordable amounts.
- A business or customer asks to be exempted from reporting or recordkeeping requirements.
- A person customarily uses the automated teller machine to make several bank deposits below a specified threshold.
- A customer deposits funds into several accounts, usually in amounts of less than $3,000, which are subsequently consolidated into a master account and transferred outside of the country, particularly to or through a location of specific concern (e.g., countries designated by national authorities and Financial Action Task Force on Money Laundering (FATF) as noncooperative countries and territories).
- A customer accesses a safe deposit box after completing a transaction involving a large withdrawal of currency, or accesses a safe deposit box before making currency deposits structured at or just under $10,000, to evade CTR filing requirements.

Funds Transfers

- Many funds transfers are sent in large, round dollar, hundred dollar, or thousand dollar amounts.
- Funds transfer activity occurs to or from a financial secrecy haven, or to or from a higher-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history.
- Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer's business or history.
- Large, incoming funds transfers are received on behalf of a foreign client, with little or no explicit reason.
- Funds transfer activity is unexplained, repetitive, or shows unusual patterns.
- Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.

- Funds transfers are sent or received from the same person to or from different accounts.
- Funds transfers contain limited content and lack related party information.

Automated Clearing House Transactions

- Large-value, automated clearing house (ACH) transactions are frequently initiated through third-party service providers (TPSP) by originators that are not bank customers and for which the bank has no or insufficient due diligence.
- TPSPs have a history of violating ACH network rules or generating illegal transactions, or processing manipulated or fraudulent transactions on behalf of their customers.
- Multiple layers of TPSPs that appear to be unnecessarily involved in transactions.
- Unusually high level of transactions initiated over the Internet or by telephone.
- NACHA — The Electronic Payments Association (NACHA) information requests indicate potential concerns with the bank's usage of the ACH system.

Activity Inconsistent with the Customer's Business

- The currency transaction patterns of a business show a sudden change inconsistent with normal activities.
- A large volume of cashier's checks, money orders, or funds transfers is deposited into, or purchased through, an account when the nature of the accountholder's business would not appear to justify such activity.
- A retail business has dramatically different patterns of currency deposits from similar businesses in the same general location.
- Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals.
- The owner of both a retail business and a check-cashing service does not ask for currency when depositing checks, possibly indicating the availability of another source of currency.
- Goods or services purchased by the business do not match the customer's stated line of business.
- Payments for goods or services are made by checks, money orders, or bank drafts not drawn from the account of the entity that made the purchase.

Lending Activity

- Loans secured by pledged assets held by third parties unrelated to the borrower.
- Loan secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.
- Borrower defaults on a cash-secured loan or any loan that is secured by assets which are readily convertible into currency.
- Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.
- To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via currency or multiple monetary instruments.
- Loans that lack a legitimate business purpose, provide the bank with significant fees for assuming little or no risk, or tend to obscure the movement of funds (e.g., loans made to a borrower and immediately sold to an entity related to the borrower).

Changes in Bank-to-Bank Transactions

- The size and frequency of currency deposits increases rapidly with no corresponding increase in noncurrency deposits.
- A bank is unable to track the true accountholder of correspondent or concentration account transactions.
- The turnover in large-denomination bills is significant and appears uncharacteristic, given the bank's location.
- Changes in currency-shipment patterns between correspondent banks are significant.

Cross-Border Financial Institution Transactions[268]

- U.S. bank increases sales or exchanges of large denomination U.S. bank notes to Mexican financial institution(s).
- Large volumes of small denomination U.S. banknotes being sent from Mexican casas de cambio to their U.S. accounts via armored transport or sold directly to U.S. banks. These sales or exchanges may involve jurisdictions outside of Mexico.
- Casas de cambio direct the remittance of funds via multiple funds transfers to jurisdictions outside of Mexico that bear no apparent business relationship with the

[268] FinCEN Advisory FIN-2006-A003, *Guidance to Financial Institutions on the Repatriation of Currency Smuggled into Mexico from the United States*, April 28, 2006.

casas de cambio. Funds transfer recipients may include individuals, businesses, and other entities in free trade zones.

- Casas de cambio deposit numerous third-party items, including sequentially numbered monetary instruments, to their accounts at U.S. banks.
- Casas de cambio direct the remittance of funds transfers from their accounts at Mexican financial institutions to accounts at U.S. banks. These funds transfers follow the deposit of currency and third-party items by the casas de cambio into their Mexican financial institution.

Bulk Currency Shipments

- An increase in the sale of large denomination U.S. bank notes to foreign financial institutions by U.S. banks.
- 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 may 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 to their accounts at foreign financial institutions and thereafter direct wire transfers to the foreign nonbank financial institution's accounts at U.S. banks.

Trade Finance

- 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 noncooperative 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 structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
- Customer requests 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 should prompt additional OFAC review.

Privately Owned Automated Teller Machines

- Automated teller machine (ATM) activity levels are high in comparison with other privately owned or bank-owned ATMs in comparable geographic and demographic locations.
- Sources of currency for the ATM cannot be identified or confirmed through withdrawals from account, armored car contracts, lending arrangements, or other appropriate documentation.

Insurance

- A customer purchases products with termination features without concern for the product's investment performance.
- A customer purchases insurance products using a single, large premium payment, particularly when payment is made through unusual methods such as currency or currency equivalents.
- A customer purchases a product that appears outside the customer's normal range of financial wealth or estate planning needs.
- A customer borrows against the cash surrender value of permanent life insurance policies, particularly when payments are made to apparently unrelated third parties.
- Policies are purchased that allow for the transfer of beneficial ownership interests without the knowledge and consent of the insurance issuer. This would include secondhand endowment and bearer insurance policies.
- A customer is known to purchase several insurance products and uses the proceeds from an early policy surrender to purchase other financial assets.

- A customer uses multiple currency equivalents (e.g., cashier's checks and money orders) from different banks and money services businesses to make insurance policy or annuity payments.

Shell Company Activity

- A bank is unable to obtain sufficient information or information is unavailable to positively identify originators or beneficiaries of accounts or other banking activity (using Internet, commercial database searches, or direct inquiries to a respondent bank).

- Payments to or from the company 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 have other address inconsistencies.

- Unusually large number and variety of beneficiaries are receiving funds transfers from one company.

- Frequent involvement of multiple jurisdictions or beneficiaries located in higher-risk offshore financial centers.

- 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.

Embassy and Foreign Consulate Accounts

- Official embassy business is conducted through personal accounts.

- Account activity is not consistent with the purpose of the account, such as pouch activity or payable upon proper identification transactions.

- Accounts are funded through substantial currency transactions.

- Accounts directly fund personal expenses of foreign nationals without appropriate controls, including, but not limited to, expenses for college students.

Employees

- Employee exhibits a lavish lifestyle that cannot be supported by his or her salary.
- Employee fails to conform to recognized policies, procedures, and processes, particularly in private banking.
- Employee is reluctant to take a vacation.

Other Unusual or Suspicious Customer Activity

- Customer frequently exchanges small-dollar denominations for large-dollar denominations.
- Customer frequently deposits currency wrapped in currency straps or currency wrapped in rubber bands that is disorganized and does not balance when counted.
- Customer purchases a number of cashier's checks, money orders, or traveler's checks for large amounts under a specified threshold.
- Customer purchases a number of open-end prepaid cards for large amounts. Purchases of prepaid cards are not commensurate with normal business activities.
- Customer receives large and frequent deposits from online payments systems yet has no apparent online or auction business.
- Monetary instruments deposited by mail are numbered sequentially or have unusual symbols or stamps on them.
- Suspicious movements of funds occur from one bank to another, and then funds are moved back to the first bank.
- Deposits are structured through multiple branches of the same bank or by groups of people who enter a single branch at the same time.
- Currency is deposited or withdrawn in amounts just below identification or reporting thresholds.
- Customer visits a safe deposit box or uses a safe custody account on an unusually frequent basis.
- Safe deposit boxes or safe custody accounts opened by individuals who do not reside or work in the institution's service area, despite the availability of such services at an institution closer to them.
- Customer repeatedly uses a bank or branch location that is geographically distant from the customer's home or office without sufficient business purpose.

- Customer exhibits unusual traffic patterns in the safe deposit box area or unusual use of safe custody accounts. For example, several individuals arrive together, enter frequently, or carry bags or other containers that could conceal large amounts of currency, monetary instruments, or small valuable items.

- Customer rents multiple safe deposit boxes to store large amounts of currency, monetary instruments, or high-value assets awaiting conversion to currency, for placement into the banking system. Similarly, a customer establishes multiple safe custody accounts to park large amounts of securities awaiting sale and conversion into currency, monetary instruments, outgoing funds transfers, or a combination thereof, for placement into the banking system.

- Unusual use of trust funds in business transactions or other financial activity.

- Customer uses a personal account for business purposes.

- Customer has established multiple accounts in various corporate or individual names that lack sufficient business purpose for the account complexities or appear to be an effort to hide the beneficial ownership from the bank.

- Customer makes multiple and frequent currency deposits to various accounts that are purportedly unrelated.

- Customer conducts large deposits and withdrawals during a short time period after opening and then subsequently closes the account or the account becomes dormant. Conversely, an account with little activity may suddenly experience large deposit and withdrawal activity.

- Customer makes high-value transactions not commensurate with the customer's known incomes.

Potentially Suspicious Activity That May Indicate Terrorist Financing

The following examples of potentially suspicious activity that may indicate terrorist financing are primarily based on guidance "Guidance for Financial Institutions in Detecting Terrorist Financing" provided by the FATF.[269] FATF is an intergovernmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing.

[269] *Guidance for Financial Institutions in Detecting Terrorist Financing*, April 24, 2002, is available at www.fatf-gafi.org/.

Activity Inconsistent With the Customer's Business

- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from higher-risk countries (e.g., countries designated by national authorities and FATF as noncooperative countries and territories).
- The stated occupation of the customer is not commensurate with the type or level of activity.
- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
- Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

Funds Transfers

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.
- Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.

Other Transactions That Appear Unusual or Suspicious

- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.

- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations.
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from higher-risk locations when there appear to be no logical business reasons for dealing with those locations.
- Banks from higher-risk locations open accounts.
- Funds are sent or received via international transfers from or to higher-risk locations.
- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

Appendix G: Structuring

Structuring transactions to evade BSA reporting and certain recordkeeping requirements can result in civil and criminal penalties under the BSA. Under the BSA (31 USC 5324), no person shall, for the purpose of evading the CTR or a geographic targeting order reporting requirement, or certain BSA recordkeeping requirements:

- Cause or attempt to cause a bank to fail to file a CTR or a report required under a geographic targeting order or to maintain a record required under BSA regulations.
- Cause or attempt to cause a bank to file a CTR or report required under a geographic targeting order, or to maintain a BSA record that contain a material omission or misstatement of fact.
- Structure, as defined above, or attempt to structure or assist in structuring, any transaction with one or more banks.

The definition of structuring, as set forth in 31 CFR 103.11(gg) (which was implemented before a USA PATRIOT Act provision extended the prohibition on structuring to geographic targeting orders and BSA recordkeeping requirements), states, "a person structures a transaction if that person, acting alone, or in conjunction with, or on behalf of, other persons, conducts or attempts to conduct one or more transactions in currency in any amount, at one or more financial institutions, on one or more days, in any manner, for the purpose of evading the [CTR filing requirements]." "In any manner" includes, but is not limited to, breaking down a single currency sum exceeding $10,000 into smaller amounts that may be conducted as a series of transactions at or less than $10,000. The transactions need not exceed the $10,000 CTR filing threshold at any one bank on any single day in order to constitute structuring.

Money launderers and criminals have developed many ways to structure large amounts of currency to evade the CTR filing requirements. Unless currency is smuggled out of the United States or commingled with the deposits of an otherwise legitimate business, any money laundering scheme that begins with a need to convert the currency proceeds of criminal activity into more legitimate-looking forms of financial instruments, accounts, or investments, will likely involve some form of structuring. Structuring remains one of the most commonly reported suspected crimes on SARs.

Bank employees should be aware of and alert to structuring schemes. For example, a customer may structure currency deposit or withdrawal transactions, so that each is less than the $10,000 CTR filing threshold; use currency to purchase official bank checks, money orders, or traveler's checks with currency in amounts less than $10,000 (and possibly in amounts less than the $3,000 recordkeeping threshold for the currency purchase of monetary instruments to avoid having to produce identification in the process); or exchange small bank notes for large ones in amounts less than $10,000.

However, two transactions slightly under the $10,000 threshold conducted days or weeks apart may not necessarily be structuring. For example, if a customer deposits $9,900 in

currency on Monday and deposits $9,900 in currency on Wednesday, it should not be assumed that structuring has occurred. Instead, further review and research may be necessary to determine the nature of the transactions, prior account history, and other relevant customer information to assess whether the activity is suspicious. Even if structuring has not occurred, the bank should review the transactions for suspicious activity.

In addition, structuring may occur before a customer brings the funds to a bank. In these instances, a bank may be able to identify the aftermath of structuring. Deposits of monetary instruments that may have been purchased elsewhere might be structured to evade the CTR filing requirements or the recordkeeping requirements for the currency purchase of monetary instruments. These instruments are often numbered sequentially in groups totaling less than $10,000 or $3,000; bear the same handwriting (for the most part) and often the same small mark, stamp, or initials; or appear to have been purchased at numerous places on the same or different days.

Appendix H: Request Letter Items (Core and Expanded)

Core Examination Procedures

As part of the examination planning process, the examiner should prepare a request letter. The list below includes materials that examiners *may* request or request access to for a bank BSA/AML examination. This list should be tailored for the specific bank's risk profile and the planned examination scope. Additional materials may be requested as needed.

BSA/AML Compliance Program

_ Name and title of the designated BSA compliance officer and, if different, the name and title of the person responsible for monitoring BSA/AML compliance.

- Organization charts showing direct and indirect reporting lines.
- Copies of résumés and qualifications of person(s) new to the bank serving in BSA/AML compliance program oversight capacities.

_ Make available copies of the most recent written BSA/AML compliance program approved by board of directors (or the statutory equivalent of such a program for foreign financial institutions operating in the United States), including CIP requirements, with date of approval noted in the minutes.

_ Make available copies of the policy and procedures relating to all reporting and recordkeeping requirements, including suspicious activity reporting.

_ Correspondence addressed between the bank, its personnel or agents, and its federal and state banking agencies, the U.S. Treasury (Office of the Secretary and Department of the Treasury, IRS, FinCEN, IRS Enterprise Computing Center – Detroit (formerly the Detroit Computing Center), and OFAC) or law enforcement authorities since the previous BSA/AML examination. For example, please make available IRS correspondence related to CTR errors or omissions.

Independent Testing

_ Make available copies of the results of any internally or externally sourced independent audits or tests performed since the previous examination for BSA/AML, including the scope or engagement letter, management's responses, and access to the workpapers.

_ Make available access to the auditor's risk assessment, audit plan (schedule), and program used for the audits or tests.

Training

_ Training documentation (e.g., materials used for training since the previous BSA/AML examination).

_ BSA/AML training schedule with dates, attendees, and topics. A list of persons in positions for which the bank typically requires BSA/AML training but who did not participate in the training.

Risk Assessment

_ Make available copies of management's BSA/AML risk assessment of products, services, customers, and geographic locations.

_ List of bank identified higher-risk accounts.

Customer Identification Program

_ List of accounts without taxpayer identification numbers (TIN).

_ File of correspondence requesting TINs for bank customers.

_ A copy of any account opening forms (e.g., for loans, deposits or other accounts) used to document CIP/Customer Due Diligence information.

_ Written description of the bank's rationale for CIP exemptions for existing customers who open new accounts.

_ List of new accounts covering all product lines (including accounts opened by third parties) and segregating existing customer accounts from new customers, for _____. *(Examiner to insert a period of time appropriate for the size and complexity of the bank.)*

_ List of any accounts opened for a customer that provides an application for a TIN.

_ List of any accounts opened in which verification has not been completed or any accounts opened with exceptions to the CIP.

_ List of customers or potential customers for whom the bank took adverse action,[270] on the basis of its CIP.

_ List of all documentary and nondocumentary methods the bank uses to verify a customer's identity.

_ Make available customer notices and a description of their timing and delivery, by product.

---

[270] As defined by 12 CFR 202.2(c).

_ List of the financial institutions on which the bank is relying, if the bank is using the "reliance provision." The list should note if the relied-upon financial institutions are subject to a rule implementing the BSA/AML compliance program requirements of 31 USC 5318(h) and are regulated by a federal functional regulator.

_ Provide the following:

- Copies of any contracts signed between the parties.
- Copies of the CIP or procedures used by the other party.
- Any certifications made by the other party.

_ Copies of contracts with financial institutions and with third parties that perform all or any part of the bank's CIP.

Suspicious Activity Reporting

_ Access to SARs filed with FinCEN during the review period and the supporting documentation. Include copies of any filed SARs that were related to section 314(a) requests for information or to section 314(b) information sharing requests.

_ Any analyses or documentation of any activity for which a SAR was considered but not filed, or for which the bank is actively considering filing a SAR.

_ Description of expanded monitoring procedures applied to higher-risk accounts.

_ Determination of whether the bank uses a manual or an automated account monitoring system, or a combination of the two. If an automated system is used, determine whether the system is proprietary or vendor supplied. If the system was provided by an outside vendor, request (i) a list that includes the vendor, (ii) application names, and (iii) installation dates of any automated account monitoring system provided by an outside vendor. Request a list of the algorithms or rules used by the systems and copies of the independent validation of the software against these rules.

_ Make available copies of reports used for identification of and monitoring for suspicious transactions. These reports include, but are not limited to, suspected kiting reports, currency activity reports, monetary instrument records, and funds transfer reports. These reports can be generated from specialized BSA/AML software, the bank's general data processing systems, or both.

_ If not already provided, copies of other reports that can pinpoint unusual transactions warranting further review. Examples include nonsufficient funds (NSF) reports, account analysis fee income reports, and large item reports.

_ Provide name, purpose, parameters, and frequency of each report.

_ Correspondence received from federal law enforcement authorities concerning the disposition of accounts reported for suspicious activity.

_ Make available copies (or a log) of criminal subpoenas received by the bank since the previous examination or inspection.

_ Make available copies of policies, procedures, and processes used to comply with all criminal subpoenas, including National Security Letters (NSL), related to BSA.

Currency Transaction Reporting

_ Access to filed Currency Transaction Reports (CTR) (FinCEN Form 104) for the review period.

_ Access to internal reports used to identify reportable currency transactions for the review period.

_ List of products or services that may involve currency transactions.

Currency Transaction Reporting Exemptions

_ Access to filed Designation of Exempt Person form(s) for current exemptions (FinCEN Form 110).

_ List of customers exempted from CTR filing and the documentation to support the exemption (e.g., currency transaction history or, as applicable, risk-based analysis).

_ Access to documentation of required annual reviews for CTR exemptions.

Information Sharing

_ Documentation of any positive match for a section 314(a) request.

_ Make available documentation demonstrating that required searches have been performed.

_ Make available any vendor-confidentiality agreements regarding section 314(a) services, if applicable.

_ Make available copies of policies, procedures, and processes for complying with 31 CFR 103.100 (Information Sharing Between Federal Law Enforcement Agencies and Financial Institutions).

_ If applicable, a copy of the bank's most recent notification form to voluntarily share information with other financial institutions under 31 CFR 103.110 (Voluntary Information Sharing Among Financial Institutions), or a copy of the most recent correspondence received from FinCEN that acknowledges FinCEN's receipt of the bank's notice to voluntarily share information with other financial institutions.

_ If applicable, make available copies of policies, procedures, and processes for complying with 31 CFR 103.110.

Purchase and Sale of Monetary Instruments

_ Access to records of sales of monetary instruments in amounts between $3,000 and $10,000 (if maintained with individual transactions, provide samples of the record made in connection with the sale of each type of monetary instrument).

Funds Transfers Recordkeeping

_ Access to records of funds transfers, including incoming, intermediary, and outgoing transfers of $3,000 or more.

Foreign Correspondent Account Recordkeeping and Due Diligence

_ List of all foreign correspondent bank accounts, including a list of foreign financial institutions, for which the bank provides or provided regular services, and the date on which the required information was received (either by completion of a certification or by other means).

_ If applicable, documentation to evidence compliance with 31 CFR 103.177 (Prohibition on Correspondent Accounts for Foreign Shell Banks; Records Concerning Owners of Foreign Banks and Agents for Service of Legal Process) and 31 CFR 103.185 (Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationship) (for foreign correspondent bank accounts and shell banks).

_ List of all payable through relationships with foreign financial institutions as defined in 31 CFR 103.175.

_ Access to contracts or agreements with foreign financial institutions that have payable through accounts.

_ List of the bank's foreign branches and the steps the bank has taken to determine whether the accounts with its branches are not used to indirectly provide services to foreign shell banks.

_ List of all foreign correspondent bank accounts and relationships with foreign financial institutions that have been closed or terminated in compliance with the conditions in 31 CFR 103.177 (i.e., service to foreign shell banks, records of owners and agents).

_ List of foreign correspondent bank accounts that have been the subject of a 31 CFR 103.100 (Information Sharing Between Federal Law Enforcement Agencies and Financial Institutions) or any other information request from a federal law enforcement officer for information regarding foreign correspondent bank accounts and evidence of compliance.

_ Any notice to close foreign correspondent bank accounts from the Secretary of the Treasury or the U.S. Attorney General and evidence of compliance.

_ Make available copies of policies, procedures, and processes for complying with 31 CFR 103.177.

_ List of all the bank's embassy or consulate accounts, or other accounts maintained by a foreign government, foreign embassy, or foreign political figure.

_ List of all accountholders and borrowers domiciled outside the United States, including those with U.S. power of attorney.

Currency-Shipment Activity

_ Make available records reflecting currency shipped to and received from the Federal Reserve Bank or correspondent banks, or reflecting currency shipped between branches and their banks' central currency vaults for the previous _____ months. (*Examiner to insert a period of time appropriate for the size and complexity of the bank.)*

Other BSA Reporting and Recordkeeping Requirements

_ Record retention schedule and procedural guidelines.

_ File of Reports of International Transportation of Currency or Monetary Instruments (CMIR) (FinCEN Form 105, formerly Customs Form 4790).

_ Records of Report of Foreign Bank and Financial Accounts (FBAR) (TD F 90-22.1).

OFAC

_ Name and title of the designated OFAC compliance officer and, if different, the name and title of the person responsible for monitoring OFAC compliance.

_ Organization charts showing direct and indirect reporting lines.

_ Copies of résumés and qualifications of person (or persons) new to the bank serving in OFAC compliance program oversight capacities.

_ OFAC training schedule with dates, attendees, and topics. A list of persons in positions for which the bank typically requires OFAC training but who did not participate in the training.

_ Make available copies of the results of any internally or externally sourced independent audits or tests performed since the previous examination for OFAC, including the scope or engagement letter, management's responses, and access to the workpapers.

_ Make available copies of management's OFAC risk assessment of products, services, customers, and geographic locations.

_ Make available copies of OFAC policies and procedures.

_ Make available a list of blocked or rejected transactions with individuals or entities on the OFAC list and reported to OFAC. *(Banks must report all blockings within ten days by filing a Report of Blocked Transactions.)*

_ If maintained, make available logs or other documentation related to reviewing potential OFAC matches, including the method for reviewing and clearing those determined not to be matches.

_ Provide a list of any OFAC licenses issued to the bank. *(OFAC has the authority, through a licensing process, to permit certain transactions that would otherwise be prohibited under its regulations. If a bank's customer claims to have a specific license, the bank should verify that the transaction conforms to the terms of the license and obtain a copy of the authorizing license.)*

_ If applicable, provide a copy of the records verifying that the most recent updates to OFAC software have been installed.

_ Provide a copy of the Annual Report of Blocked Property submitted to OFAC (TD F 90-22.50). *(Banks must report all blocked assets to OFAC annually by September 30.)*

Expanded Examination Procedures

As part of the examination planning process, the examiner should prepare a request letter. The listing below includes materials that *may* be requested for a bank BSA/AML examination. This list should be tailored for the specific institution profile and the planned examination scope. Additional materials may be requested as needed.

Correspondent Accounts (Domestic)

_ Make available copies of policies, procedures, and processes specifically for correspondent bank accounts, including procedures for monitoring for suspicious activity.

_ Make available a list of domestic correspondent bank accounts.

_ Provide a list of SARs filed relating to domestic correspondent bank accounts.

Correspondent Accounts (Foreign)

_ Make available copies of policies, procedures, and processes specifically for foreign correspondent financial institution accounts, including procedures for monitoring for suspicious activity.

_ Make available a list of foreign correspondent financial institution accounts.

_ Provide risk assessments covering foreign correspondent financial institution account relationships.

_ Provide a list of SARs filed relating to foreign correspondent financial institution accounts.

Bulk Shipments of Currency

_ Make available copies of policies, procedures, and processes related to receiving shipments of bulk currency. Describe expanded monitoring procedures applied to Currency Originators and Intermediaries.

_ Make available a list of Currency Originators, Intermediaries, including referral agents, and foreign and domestic customers that send bulk currency shipments to the bank.

_ Provide a list of all foreign and domestic correspondent bank accounts, including a list of foreign financial institutions, from which the bank receives or sends bulk currency shipments.

_ Provide a copy of management's risk assessment of relationships and transactions of Currency Originators and Intermediaries.

_ Make available copies of reports used for identification of and monitoring for suspicious transactions related to Currency Originators and Intermediaries

_ Make available agreements or contracts with Currency Originators or Intermediaries.

_ Provide a list of SARs filed related to shipping relationships and transactions.

U.S. Dollar Drafts

_ Make available copies of policies, procedures, and processes specifically for U.S. dollar drafts, including procedures for monitoring for suspicious activity.

_ Make available a list of foreign correspondent bank accounts that offer U.S. dollar drafts. If possible, include the volume, by number and dollar amount, of monthly transactions for each account.

_ Provide a list of SARs filed relating to U.S. dollar drafts.

Payable Through Accounts

_ Make available copies of policies, procedures, and processes specifically for payable through accounts (PTA), including procedures for monitoring for suspicious activity.

_ Make available a list of foreign correspondent bank accounts with PTAs. Include a detailed summary (number and monthly dollar volume) of sub-accountholders for each PTA.

_ Provide a list of SARs filed relating to PTAs.

Pouch Activities

_ Make available copies of pouch activity policies, procedures, and processes, including procedures for monitoring for suspicious activity.

_ Provide a list of customer accounts permitted to use pouch services.

_ Provide a list of CTRs, CMIRs, or SARs filed relating to pouch activity.

_ As needed, provide a copy of pouch logs.

Foreign Branches and Offices of U.S. Banks

_ Make available copies of policies, procedures, and processes specific to the foreign branch or office, if different from the parent's policies, procedures, and processes.

_ Provide most recent management reports received on foreign branches and offices.

_ Make available copies of the bank's tiering or organizational structure report.

_ Provide AML audit reports, compliance reports, and supporting documentation for the foreign branches and offices.

_ Provide a list of the types of products and services offered at the foreign branches and offices and information on new products or services offered by the foreign branch, including those that are not already offered by the parent bank.

_ Provide a description of the method for aggregating each customer relationship across business units and geographic locations throughout the organization.

_ Provide the code of ethics for foreign branches or offices, if it is different from the bank's standard policy.

_ When testing will be performed, provide a list of accounts originated or serviced in the foreign branch or office. Examiners should try to limit this request and focus on accounts for specific products or services, higher-risk accounts only, or accounts for which exceptions or audit concerns have been noted.

_ Provide a list of the locations of foreign branches and offices, including, if possible, the host country regulatory agency and contact information.

_ Provide the organizational structure of the foreign branches and offices, including reporting lines to the U.S. bank level.

Parallel Banking

_ Provide a list of any parallel banking relationships.

_ Make available copies of policies, procedures, and processes specifically for parallel banking relationships, including procedures relating to higher-risk money laundering activities. Such policies and procedures should include those that are specific to the relationship with the parallel entity.

_ Provide a list SARs filed relating to parallel banking relationships.

_ Make available documents that specify limits or procedures that should be followed when dealing with the parallel entity.

_ Provide a list of directors or officers of the bank who are also associated with the foreign parallel bank.

Electronic Banking

_ Make available copies of any policies and procedures related directly to electronic banking (e-banking) that are not already included in the BSA/AML policies.

_ Provide management reports that indicate the monthly volume of e-banking activity.

_ Provide a list of business customers regularly conducting e-banking transactions, including the number and dollar volume of transactions.

_ Make available a list of service providers related to Remote Deposit Capture (RDC) activities.

_ Make available copies of contracts related to RDC activities.

Funds Transfers

_ Provide funds transfer activity logs, including funds transfers that involve cover payments, including transfers into and out of the bank. Include the number and dollar volume of funds transfer activity for the month.

_ Provide a list of funds transfers purchased with currency over a specified time period.

_ Provide a list of noncustomer transactions over a specified time period.

_ If not already included in the BSA/AML policies, make available copies of any policies, procedures, and processes related to funds transfers, including transfers that involve cover payments, or payable upon proper identification (PUPID).

_ Provide a list of suspense accounts used for PUPID proceeds.

_ Provide a list of PUPID transactions completed by the bank, either as the beneficiary bank or as the originating bank.

Automated Clearing House Transactions

_ Make available copies of any policies and procedures related directly to automated clearing house (ACH) and international ACH transactions (IAT) that are not already included in the BSA/AML policies.

_ Make available copies of management reports that indicate the monthly volume of ACH activity, including IATs.

_ Make available a list of large or frequent ACH transactions or IATs.

_ Make available a list of IATs (both those originated from or received by the bank).

_ Make available a list of customer complaints regarding ACH transactions and IATs.

Electronic Cash

_ Make available copies of any policies and procedures related directly to electronic cash (e-cash), including prepaid cards, that are not already included in the BSA/AML policies.

_ Provide management reports that indicate the monthly volume of e-cash activity, including prepaid cards.

_ Provide a list of business customers regularly conducting e-cash transactions, including prepaid cards, including the number and dollar volume of transactions.

Third-Party Payment Processors

_ If not already included in the BSA/AML policies, make available copies of any policies, procedures, and processes related to third-party payment processors.

_ Provide a list of third-party payment processor relationships. Include the number and dollar volume of payments processed per relationship.

_ Provide a list of SARs filed on third-party payment processor relationships.

Purchase and Sale of Monetary Instruments

_ If not already included in the BSA/AML policies, make available copies of any policies, procedures, and processes related to the sale of monetary instruments for currency. In particular, include policies, procedures, and processes related to the monitoring sales of monetary instruments in order to detect unusual activities.

_ Provide monetary instrument logs or other MIS reports used for the monitoring and detection of unusual or suspicious activities relating to the sales of monetary instruments.

_ Provide a list of noncustomer transactions over a specified period of time.

_ Provide a list of monetary instruments purchased with currency over a specified time period.

_ Provide a list of SARs filed related to the purchase or sale of monetary instruments.

Brokered Deposits

_ Make available copies of specific policies and procedures specifically for brokered deposits, including procedures for monitoring for suspicious activity.

_ Provide risk assessment covering brokered deposits.

_ Provide internal audits covering brokered deposits.

_ Provide a list of approved deposit brokers.

_ Provide management reports covering nonrelationship funding programs (including reports on balances, concentrations, performance, or fees paid).

_ Provide SARs and subpoenas related to brokered deposit relationships.

_ Provide a copy of account documentation or agreements for deposit broker arrangements.

Privately Owned Automated Teller Machines

_ Provide a risk assessment covering privately owned automated teller machines (ATM) and Independent Sales Organizations (ISO), including a list of higher-risk privately owned ATM relationships.

_ Make available copies of policies, procedures, and processes for privately owned ATM and ISO account acceptance, due diligence, and ongoing monitoring.

_ Provide a list of ISO clients and balances.

_ Provide SARs and subpoenas related to privately owned ATMs and ISOs.

Nondeposit Investment Products

_ Make available copies of policies, procedures, and processes relating to nondeposit investment products (NDIP) and relationships with any independent NDIP providers.

_ Provide internal audits covering NDIP sales and provider relationships.

_ Provide a risk assessment covering NDIP customers and transactions.

_ If available, provide a list of NDIP clients and balances.

_ Provide a list of suspense, concentration, or omnibus accounts used for NDIP. Describe the purpose for and controls surrounding each account.

_ Provide management reports covering 25 to 50 of the largest, most active, and most profitable NDIP customers.

_ Provide SARs and subpoenas related to NDIP customers.

_ Make available a copy of account opening documentation or agreements for NDIP.

_ Make available a copy of contracts or agreements between the bank and third-party NDIP providers for the completion of CIP, due diligence, and ongoing monitoring of NDIP customers.

Insurance

_ Make available copies of BSA/AML policies and procedures related to the sale of insurance.

_ Provide risk assessment covering insurance products.

_ Make available MIS reports related to the sales of insurance products. Reports may include large transaction reports, single premium payments, early cancellation, premium overpayments, and assignments of claims.

_ Make available a copy of contracts or agreements between the bank and insurance providers for the completion of CIP, due diligence, and ongoing monitoring of insurance customers.

_ Provide a list of insurance products approved for sale at the bank.

_ Provide management reports covering insurance products (including large transactions, funds transfers, single premium payments, and early cancellations).

_ Provide SARs or subpoenas related to insurance clients.

_ Provide a copy of account documentation requirements and applications for insurance products.

Concentration Accounts

_ Make available copies of BSA/AML policies, procedures, and processes that are specific to concentration accounts (also known as special-use, omnibus, suspense, settlement, intraday, sweep, or collection accounts).

_ Provide a list of all concentration accounts and each account's most recent reconcilement.

_ Provide account activity reports for concentration accounts for _____. (*Examiner to insert a period of time appropriate for the size and complexity of the bank.)*

Lending Activities

_ Make available copies of BSA/AML policies and procedures specific to lending.

_ Provide a risk assessment relating to the lending function, including a list of any higher-risk lending relationships identified by the bank.

_ For loans secured by cash collateral, marketable securities, or cash surrender value of life insurance products:

- Provide a list of all loans that have defaulted since the previous BSA/AML examination, including those that were charged off.
- Provide a list of all loans that have been extended since the previous BSA/AML examination.

Trade Finance Activities

_ Make available copies of BSA/AML policies and procedures specific to trade finance activities.

_ Provide a risk assessment relating to trade finance activities, including a list of any higher-risk trade finance transactions, accounts, or relationships identified by the bank.

_ Provide a list of customers involved in transactions with higher-risk geographic locations or for whom the bank facilitates trade finance activities with higher-risk geographic locations.

Private Banking

_ Make available copies of policies, procedures, and controls used to manage BSA/AML risks in the private banking department.

_ Make available business or strategic plans for the private banking department.

_ Provide the most recent version of management reports on private banking activity, such as customer aggregation reports, policy exception reports, client concentrations, customer risk classification reports, and unusual account activity.

_ Provide recent private banking reports from compliance, internal audit, risk management, and external auditors or consultants that cover BSA/AML.

_ Provide a list of products and services offered to private banking clients. Information on new products and services offered to private banking clients and the bank's process for approving new activities.

_ Provide a description of the method for aggregating customer holdings and activities across business units throughout the organization.

_ Provide a description of account officer and manager positions, and the compensation, recruitment, and training program for these positions.

_ Make available the code of ethics policy for private banking officers.

_ Provide a risk assessment covering private banking customers and transactions.

_ Provide a list of suspense, concentration, or omnibus accounts used for private banking transactions. Describe the purpose for each account and the controls governing it.

_ Provide management reports covering 25 to 50 of the largest, most active, or most profitable private banking customers.

_ Provide a list of the bank's private banking accountholders who meet the following criteria:

- Politically exposed persons (PEP), export or import business owners, money transmitters, Private Investment Companies (PIC), financial advisers, offshore entities, or money managers (when an intermediary is acting on behalf of customers).
- Customers who were introduced to the bank by individuals previously employed by other financial institutions.
- Customers who were introduced to the bank by a third-party investment adviser.
- Customers who use nominee names.
- Customers who are from, or do business with, a higher-risk geographic location.
- Customers who are involved in cash-intensive businesses.
- Customers who were granted exceptions to policies, procedures, and controls.
- Customers who frequently appear on unusual activity monitoring reports.

_ Provide SARs and subpoenas related to private banking customers.

_ Make available a copy of account-opening documentation or agreements for private banking customers.

Trust and Asset Management Services

_ Make available copies of BSA/AML policies, procedures, and processes for trust and asset management services.

_ Make available trust and asset management procedures and guidelines used to determine when EDD is appropriate for higher-risk accounts and parties to the relationship. These should include methods for identifying account-interested parties (i.e., individual grantors, co-trustees, or outside investment managers).

_ Provide a list of the bank's trust and asset management accountholders who meet the following criteria:

_ Provide a list of politically exposed persons (PEP), export or import business owners, money transmitters, Private Investment Companies (PIC), financial advisers, offshore entities, or money managers (when an intermediary is acting on behalf of customers).

- Customers who were introduced to the bank by individuals previously employed by other financial institutions.
- Customers who were introduced to the bank by a third-party investment adviser.
- Customers who use nominee names.

- Customers who are from, or do business with, a higher-risk geographic location.
- Customers who are involved in cash-intensive businesses.
- Customers who were granted exceptions to policies, procedures, and controls.
- Customers who frequently appear on unusual activity monitoring reports.

_ Make available reports and minutes submitted to the board of directors or its designated committee relating to BSA/AML matters pertaining to trust and asset management business lines and activities.

_ Provide an organizational chart for the BSA/AML compliance function as it relates to the trust and asset management services.

_ Provide a risk assessment of trust and asset management services that identifies those customers, prospective customers, or products the bank has determined to be higher risk.

_ Provide management reports covering 25 to 50 of the largest, most active, or most profitable trust and asset management customers.

_ Provide a BSA/AML independent review or audit of trust and asset management services. Make workpapers available upon request.

_ Make available a copy of the BSA/AML training materials for management and employees involved in trust and asset management activities.

_ Identify the trust accounting systems used. Briefly explain how they accommodate and assist compliance with BSA/AML regulations and guidelines.

_ Provide a list of newly opened trust and asset management accounts since _____. *(Examiner to insert a period of time appropriate for the size and complexity of the bank.)*

_ Provide procedures for checking section 314(a) requests relating to trust and asset management services.

_ Provide a list of all trust and asset management accounts designated as higher risk, and a list of all accounts whose assets consist of PICs and asset protection trusts.

_ Provide copies of SARs associated with trust and asset management services.

_ Provide a list of subpoenas, particularly BSA/AML-related, relating to trust and asset management activities.

Nonresident Aliens and Foreign Individuals

_ Make available copies of policies, procedures, and processes specific to nonresident alien (NRA) accounts, including guidelines and systems for establishing and updating W-8 exempt status.

_ Provide a list of NRA and foreign individual accounts held by the bank, particularly those accounts the bank has designated as higher risk.

_ Provide a list of NRA and foreign individual accounts without a TIN, passport number, or other appropriate identification number.

_ Provide a list of SARs and subpoenas related to NRA and foreign individual accounts.

Politically Exposed Persons

_ Make available copies of policies, procedures, and processes specific to politically exposed persons (PEP). Policies should include the bank's definition of a PEP as well as procedures for opening PEP accounts and senior management's role in the approval process for opening PEP accounts.

_ Provide a list of accounts in the name of or for the benefit of a PEP. List should include the country of residence of the PEP, the account balances, and the average number and dollar volume of transactions per month.

_ Provide a list of the information systems or other methods used to identify PEP accounts.

_ Make available management reports used to monitor PEP accounts, including reports for identifying unusual and suspicious activity.

Embassy and Foreign Consulate Accounts

_ Make available copies of policies, procedures, and processes specific to embassy and foreign consulate account relationships.

_ Provide a list of embassy and foreign consulate accounts held by the bank, including the average account balances and the average number and dollar volume of transactions per month.

_ Provide a list of accounts that are in the name of individuals who work for the embassy or foreign consulate.

Nonbank Financial Institutions

_ Make available copies of policies, procedures, and processes related to nonbank financial institutions.

_ Provide a list of nonbank financial institution accounts, including all related accounts.

_ Provide a risk assessment of nonbank financial institution accounts, identifying those accounts the bank has designated as higher risk. This list should include products and services offered by the nonbank financial institution; the average account balance; and the average number, type, and dollar volume of transactions per month.

_ Provide a list of foreign nonbank financial institution accounts, including the products and services offered; the average account balance; and the average, number, type, and dollar volume of transactions per month.

_ Provide a sample of account opening documentation for higher-risk nonbank financial institutions.

_ Provide a list of SARs and subpoenas related to nonbank financial institutions.

Professional Service Providers

_ Make available copies of policies, procedures, and processes related to professional service provider accounts.

_ Provide a list of professional service provider accounts, including all related accounts (such as interest on lawyers' trust accounts (IOLTA) which should include the name of the attorney on each account).

_ Provide a list of any professional service provider accounts that the bank has designated as higher risk.

Nongovernmental Organizations and Charities

_ Make available copies of policies, procedures, and processes related to nongovernmental organizations and charities.

_ List of nongovernmental organizations and charities, particularly those that the bank the bank has designated as higher risk. This list should include average account balances and the average number and dollar volume of transactions.

_ List of nongovernmental organizations involved in higher-risk geographic locations.

Business Entities (Domestic and Foreign)

_ Make available copies of policies, procedures, and processes specifically related to domestic and international business entities.

_ Provide a list of accounts opened by business entities. If this list is unreasonably long, amend the request to look at those entities incorporated in higher-risk jurisdictions or those accounts the bank has designated as higher risk.

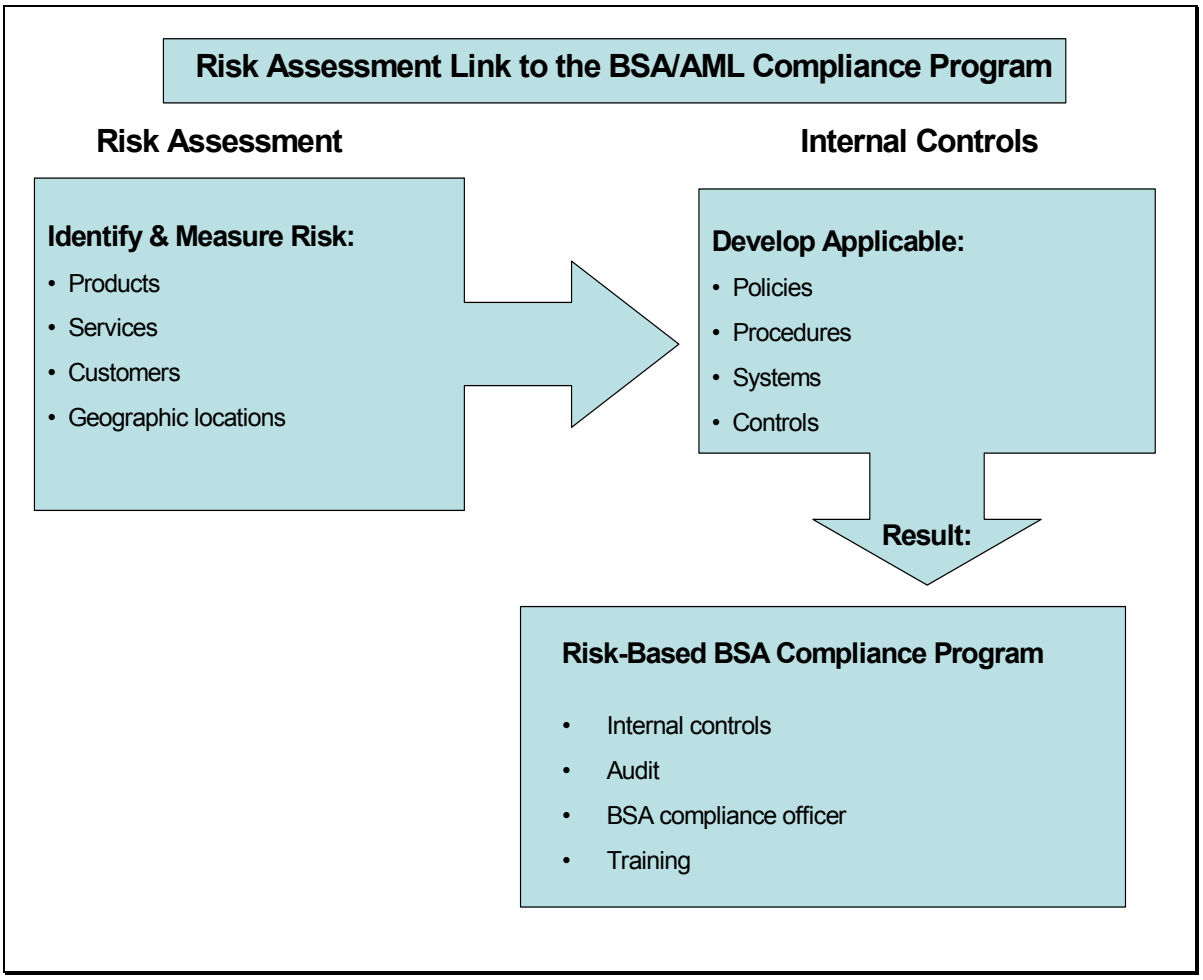
_ Provide a list of loans to business entities collateralized by bearer shares.

Cash-Intensive Businesses

_ Make available copies of policies, procedures, and processes related to other businesses and entities.

_ Provide risk assessment of other businesses and entities, list those other businesses and entities that the bank has designated as higher risk. The listing should include average account balances and the average number and dollar volume of transactions.

Appendix I: Risk Assessment Link to the BSA/AML Compliance Program



Appendix J: Quantity of Risk Matrix

Banks and examiners may use the following matrix to formulate summary conclusions. Prior to using this matrix, they should complete the identification and quantification steps detailed in the BSA/AML Risk Assessment Overview section at pages 22 to 30 of this manual.

Low	Moderate	High
Stable, known customer base.	Customer base increasing due to branching, merger, or acquisition.	A large and growing customer base in a wide and diverse geographic area.
No electronic banking (e-banking) or the Web site is informational or nontransactional.	The bank is beginning e-banking and offers limited products and services.	The bank offers a wide array of e-banking products and services (e.g., account transfers, e-bill payment, or accounts opened via the Internet).
On the basis of information received from the BSA-reporting database, there are few or no large currency or structured transactions.	On the basis of information received from the BSA-reporting database, there is a moderate volume of large currency or structured transactions.	On the basis of information received from the BSA-reporting database, there is a significant volume of large currency or structured transactions.
Identified a few higher-risk customers and businesses.	Identified a moderate number of higher-risk customers and businesses.	Identified a large number of higher-risk customers and businesses.
No foreign correspondent financial institution accounts. The bank does not engage in pouch activities, offer special-use accounts, or offer payable through accounts (PTA), or provide U.S. dollar draft services.	The bank has a few foreign correspondent financial institution accounts, but typically with financial institutions with adequate AML policies and procedures from lower-risk countries, and minimal pouch activities, special-use accounts, PTAs, or U.S. dollar draft services.	The bank maintains a large number of foreign correspondent financial institution accounts with financial institutions with inadequate AML policies and procedures, particularly those located in higher-risk jurisdictions, or offers substantial pouch activities, special-use accounts, PTAs, or U.S. dollar draft services.

Low	Moderate	High
The bank offers limited or no private banking services or trust and asset management products or services.	The bank offers limited domestic private banking services or trust and asset management products or services over which the bank has investment discretion. Strategic plan may be to increase trust business.	The bank offers significant domestic and international private banking or trust and asset management products or services. Private banking or trust and asset management services are growing. Products offered include investment management services, and trust accounts are predominantly nondiscretionary versus where the bank has full investment discretion.
Few international accounts or very low volume of currency activity in the accounts.	Moderate level of international accounts with unexplained currency activity.	Large number of international accounts with unexplained currency activity.
A limited number of funds transfers for customers, noncustomers, limited third-party transactions, and no foreign funds transfers.	A moderate number of funds transfers. A few international funds transfers from personal or business accounts with typically lower-risk countries.	A large number of noncustomer funds transfer transactions and payable upon proper identification (PUPID) transactions. Frequent funds from personal or business accounts to or from higher-risk jurisdictions, and financial secrecy havens or jurisdictions.
The bank is not located in a High Intensity Drug Trafficking Area (HIDTA)[271] or High Intensity Financial Crime Area (HIFCA). No fund transfers or account relationships involve HIDTAs or HIFCAs.	The bank is located in an HIDTA or an HIFCA. Bank has some fund transfers or account relationships that involve HIDTAs or HIFCAs.	Bank is located in an HIDTA and an HIFCA. A large number of fund transfers or account relationships involve HIDTAs or HIFCAs.
No transactions with higher-risk geographic locations.	Minimal transactions with higher-risk geographic locations.	Significant volume of transactions with higher-risk geographic locations.

[271] A list of HIDTAs is available at www.whitehousedrugpolicy.gov/index.html.

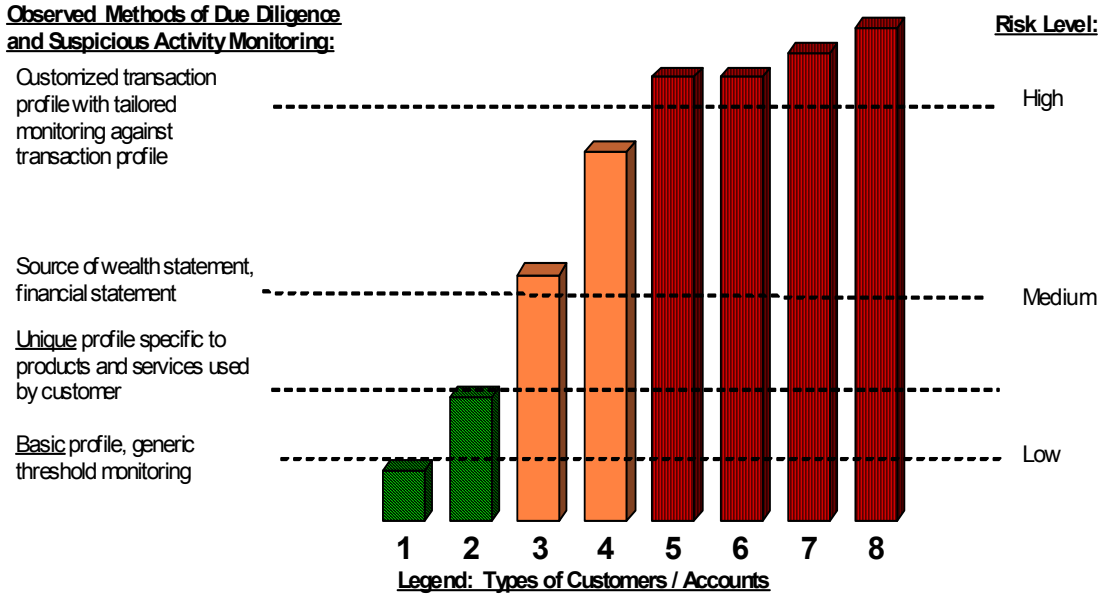
Low	Moderate	High
Low turnover of key personnel or frontline personnel (e.g., customer service representatives, tellers, or other branch personnel).	Low turnover of key personnel, but frontline personnel in branches may have changed.	High turnover, especially in key personnel positions.

Appendix K: Customer Risk Versus Due Diligence and Suspicious Activity Monitoring

FOR ILLUSTRATION ONLY

Customer Risk versus Due Diligence and Suspicious Activity Monitoring

Certain customer relationships may pose a higher risk than others. This chart provides an example of how a bank may stratify the risk profile of its customers (see legend and risk levels). Because the nature of the customer is only one variable in assessing risk, this simplified chart is for illustration purposes only. The chart also illustrates the progressive methods of due diligence and suspicious activity monitoring systems that banks may deploy as the risk level rises. (See Observed Methods, below.)



1 Resident Consumer Account (DDA, Savings, Time, CD)
2 Nonresident Alien Consumer Account (DDA, Savings, Time, CD)
3 Small Commercial and Franchise Businesses
4 Consumer Wealth Creation (at a threshold appropriate to the bank's risk appetite)
5 Nonresident Alien Offshore Investor
6 High Net Worth Individuals (Private Banking)
7 Multiple Tiered Accts (Money Managers, Financial Advisors, "Payable Through" Accounts)
8 Offshore and Shell Companies

Appendix L: SAR Quality Guidance

The following information is provided as guidance. Refer to FinCEN's *Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative* (November 2003) for original text, which can be found at www.fincen.gov. Banks also should consult *Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting* (October 10, 2007), available at www.fincen.gov.

Often SARs have been instrumental in enabling law enforcement to initiate or supplement major money laundering or terrorist financing investigations and other criminal cases. Information provided in SAR forms also allows FinCEN and the federal banking agencies to identify emerging trends and patterns associated with financial crimes. The information about those trends and patterns is vital to law enforcement agencies and provides valuable feedback to financial institutions.

Banks must file SAR forms that are complete, sufficient, and timely. Unfortunately, some banks file SAR forms that contain incomplete, incorrect, or disorganized narratives, making further analysis difficult, if not impossible. Some SAR forms are submitted with blank narratives. Because the SAR narrative serves as the only free text area for summarizing suspicious activity, the narrative section is "critical." The care with which the narrative is written may make the difference in whether or not the described conduct and its possible criminal nature are clearly understood by law enforcement, and thus a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.

The SAR form should include any information readily available to the filing bank obtained through the account opening process and due diligence efforts. In general, a SAR narrative should identify the five essential elements of information (who? what? when? where? and why?) for the suspicious activity being reported. The method of operation (or how?) is also important and should be included in the narrative.

Who is conducting the suspicious activity?

While one section of the SAR form calls for specific suspect information, the narrative should be used to further describe the suspect or suspects, including occupation, position or title within the business, the nature of the suspect's business (or businesses), and any other information and identification numbers associated with the suspects.

What instruments or mechanisms are being used to facilitate the suspect transactions?

A list of instruments or mechanisms that may be used in suspicious activity includes, but is not limited to, funds transfers, letters of credit and other trade instruments, correspondent accounts, casinos, structuring, shell companies, bonds or notes, stocks, mutual funds, insurance policies, traveler's checks, bank drafts, money orders, credit or debit cards, prepaid cards, and digital currency business services. The SAR narrative should list the instruments or mechanisms used in the reported suspicious activity. If a

SAR narrative summarizes the flow of funds, the narrative should always include the source of the funds (origination) and the use, destination, or beneficiary of the funds.

When did the suspicious activity take place?

If the activity takes place over a period of time, indicate the date when the suspicious activity was first noticed and describe the duration of the activity. When possible, in order to better track the flow of funds, individual dates and amounts of transactions should be included in the narrative rather than only the aggregated amount.

Where did the suspicious activity take place?

The narrative should indicate if multiple offices of a single bank were involved in the suspicious activity and provide the addresses of those locations. The narrative should also specify if the suspected activity or transactions involves a foreign jurisdiction.

Why does the filer think the activity is suspicious?

The SAR should describe, as fully as possible, why the activity or transaction is unusual for the customer, considering the types of products and services offered by the filing bank's industry, and drawing any applicable contrasts with the nature and normally expected activities of similar customers.

How did the suspicious activity occur?

The narrative should describe the "modus operandi" or the method of operation of the subject conducting the suspicious activity. In a concise, accurate, and logical manner, the narrative should describe how the suspect transaction or pattern of transactions was committed. For example, if what appears to be structuring of currency deposits is matched with outgoing funds transfers from the accounts, the SAR narrative should include information about both the structuring and outbound transfers (including dates, destinations, amounts, accounts, frequency, and beneficiaries of the funds transfers).

A bank should not include any supporting documentation with a filed SAR nor use the terms "see attached" in the SAR narrative.

When SAR forms are received at the IRS Enterprise Computing Center – Detroit (formerly the Detroit Computing Center), only information that is in an explicit, narrative format is keypunched; thus tables, spreadsheets, or other attachments are not entered into the BSA-reporting database. Banks should keep any supporting documentation in their records for five years so that this information is available to law enforcement upon request.

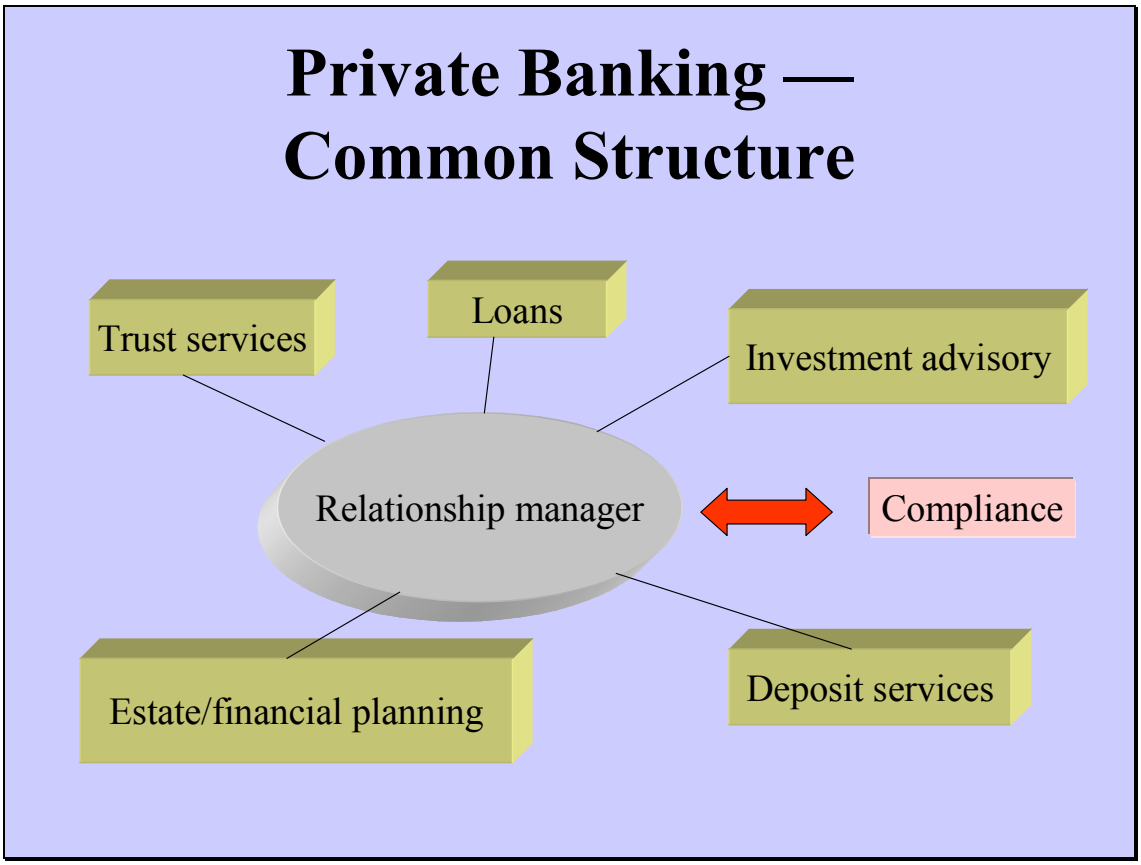
Appendix M: Quantity of Risk Matrix — OFAC Procedures

Examiners should use the following matrix, as appropriate, when assessing a bank's risk of encountering an OFAC issue.

Low	Moderate	High
Stable, well-known customer base in a localized environment.	Customer base changing due to branching, merger, or acquisition in the domestic market.	A large, fluctuating client base in an international environment.
Few higher-risk customers; these may include nonresident aliens, foreign individuals (including accounts with U.S. powers of attorney), and foreign commercial customers.	A moderate number of higher-risk customers.	A large number of higher-risk customers.
No overseas branches and no correspondent accounts with foreign banks.	Overseas branches or correspondent accounts with foreign banks.	Overseas branches or multiple correspondent accounts with foreign banks.
No electronic banking (e-banking) services offered, or products available are purely informational or nontransactional.	The bank offers limited e-banking products and services.	The bank offers a wide array of e-banking products and services (e.g., account transfers, e-bill payment, or accounts opened via the Internet).
Limited number of funds transfers for customers and noncustomers, limited third-party transactions, and no international funds transfers.	A moderate number of funds transfers, mostly for customers. Possibly, a few international funds transfers from personal or business accounts.	A high number of customer and noncustomer funds transfers, including international funds transfers.
No other types of international transactions, such as trade finance, cross-border ACH, and management of sovereign debt.	Limited other types of international transactions.	A high number of other types of international transactions.

Low	Moderate	High
No history of OFAC actions. No evidence of apparent violation or circumstances that might lead to a violation.	A small number of recent actions (e.g., actions within the last five years) by OFAC, including notice letters, or civil money penalties, with evidence that the bank addressed the issues and is not at risk of similar violations in the future.	Multiple recent actions by OFAC, where the bank has not addressed the issues, thus leading to an increased risk of the bank undertaking similar violations in the future.

Appendix N: Private Banking — Common Structure



Appendix O: Examiner Tools for Transaction Testing

Currency Transaction Reporting and Suspicious Activity Reporting

If the bank does not have preset filtering reports for currency transaction reporting and the identification of suspicious currency transactions, the examiner should consider requesting a custom report. For example, a report could be generated with the following criteria: currency transactions of $7,000 or higher (in and out) for the preceding period (*to be determined by the examiner*) before the date of examination. The time period covered and the transaction amounts may be adjusted as determined by the examiner. The report should also capture:

- The customer information file (CIF) number, if available, or Social Security number (SSN)/taxpayer identification number (TIN).
- The date, amount, and account number of each transaction.
- The teller and branch or other applicable identifying information.

This data should be prepared in an electronic spreadsheet or database format to facilitate the sorting of the data. The data can be sorted in a number of different criteria (e.g., by branch, by teller, by SSN/TIN, or CIF number, if available). Analysis of this information should enable the examiner to determine whether CTRs and SARs have been appropriately filed.

Funds Transfer Monitoring

If the bank does not have preset filtering reports for funds transfer recordkeeping and the identification of suspicious transactions, the examiner should consider requesting a custom report. The examiner may consider requesting that the bank provide a report from its funds transfer systems that identifies all funds transfers (in and out) for a time period determined by the examiner. The report should also capture:

- The customer's full name, country of residence, SSN/TIN, and BSA/AML risk rating, if applicable.
- The date, amount, transaction type, and account number of each transaction.
- The originator's name, country, financial institution, and account number.
- The beneficiary's name, country, financial institution, and account number.

The bank should provide a list of bank internal codes necessary to fully identify the account type, BSA/AML risk rating, country, transaction type, bank number, account

number, and any other codes on the electronic reports. The list should be sorted to identify those accounts that do not contain sufficient originator or beneficiary information. Missing information may indicate funds transfer monitoring deficiencies. A large number of transfers or those of high-dollar amounts to and from higher-risk jurisdictions or involving parties that do not appear likely to be involved in such transactions may indicate the need for additional scrutiny.

Adequacy of Deposit Account Information and Trust and Asset Management Account Information

This test is designed to ensure that the bank is in compliance with the CIP regulatory requirements and to test the adequacy of the bank's CDD policies, procedures, and processes.

The examiner should request an electronic list (spreadsheet or database) of all deposit accounts and trust/asset management accounts as of the date of examination. The balances should be reconciled to the general ledger. The report should also capture:

- The customer's full name, date of birth, address, country of residence, SSN/TIN, and BSA/AML risk rating, if applicable.
- The date the account was opened.
- The average daily balance (during the review period) and balance of the account as of the examination date.

The bank should provide a list of bank internal codes necessary to fully identify the account type, BSA/AML risk rating, country, transaction type, branch number, teller number, and any other codes found on the electronic reports. The list should be sorted to identify those accounts that do not contain sufficient information.

Testing of Currency-Shipment Logs for Unusual Activity

Review all, or a sample, of the bank's currency-shipment logs for significant aberrations or unusual patterns of currency-shipment activity. Examiners may also consider reviewing the FDIC Summary of Deposits (SOD) data for unusual trends in branch deposit growth.

Assess whether shipment levels and the frequency of shipments appear commensurate with the expected bank and branch activity levels. This assessment should include transactions to and from the central currency vault and the branches. Unusual activity warranting further research may include significant exchanges of small-denomination bills for large-denomination bills and significant requests for large bills.

Nonresident Aliens and Foreign Individuals

An effective method to identify and review the level of the bank's nonresident aliens (NRA), foreign individuals, and offshore corporations is by obtaining MIS reports that provide no TINs or accountholders with individual taxpayer identification numbers (ITIN). The report should capture:

- Customer's full name, date of birth, address, country of residence, and SSN/TIN.
- Date the account was opened.
- Average daily balance and balance of the account as of the examination date.

This data should be prepared in an electronic spreadsheet or database format to facilitate the sorting of the data. The bank should provide a list of bank internal codes necessary to fully identify the information on the spreadsheet. This information can be used to assess whether the amount of NRAs and foreign individuals provide heightened risk to the bank by determining the aggregate average daily balance, the account types, and countries in which the bank is exposed.

Funds Flow Reports

Examiners can review this information to identify customers with a high velocity of funds flow and those with unusual activity. A velocity of funds report reflects the total debits and credits flowing through a particular account over a specific period (e.g., 30 days). The electronic reports should capture:

- Name of customer.
- Account number.
- Date of transaction.
- Dollar amount of payments (debits).
- Dollar amount of receipts (credits).
- Average balance of the account.
- Type of account.

This data should be prepared in an electronic spreadsheet or database format to facilitate the sorting of the data. This report can be used to identify customer accounts with substantial funds flow relative to other accounts.

Appendix P: BSA Record Retention Requirements

This appendix is provided as a summary listing. For comprehensive and current BSA record retention requirements, refer to U.S. Treasury/FinCEN regulations found at 31 CFR 103. These BSA record retention requirements are independent of and in addition to record retention requirements under other laws.

Five-Year Retention for Records as Specified Below

The BSA establishes recordkeeping requirements related to various types of records including: customer accounts (e.g., loan, deposit, or trust), BSA filing requirements, and records that document a bank's compliance with the BSA. In general, the BSA requires that a bank maintain most records for at least five years. These records can be maintained in many forms including original, microfilm, electronic, copy, or a reproduction. A bank is not required to keep a separate system of records for each of the BSA requirements; however, a bank must maintain all records in a way that makes them accessible in a reasonable period of time.

The records related to the transactions discussed below must be retained by a bank for five years. However, as noted below, the records related to the identity of a bank customer must be maintained for five years after the account (e.g., loan, deposit, or trust) is closed. Additionally, on a case-by-case basis (e.g., U.S. Treasury Department Order, or law enforcement investigation), a bank may be ordered or requested to maintain some of these records for longer periods.

Extension of Credit in Excess of $10,000 (Not Secured by Real Property)

This record shall contain:

- Name of borrower.
- Address of borrower.
- Amount of credit extended.
- Nature or purpose of loan.
- Date of loan.

International Transactions in Excess of $10,000

A record of any request made or instructions received or given regarding a transfer of currency or other monetary instruments, checks, funds, investment securities, or credit greater than $10,000 to or from any person, account, or place outside the United States.

Signature Cards

A record of each grant of signature authority over each deposit account.

Account Statements

A statement, ledger card, or other record on each deposit account showing each transaction in, or with respect to, that account.

Checks in Excess of $100

Each check, draft, or money order drawn on the bank or issued and payable by it that is in excess of $100.

Deposits in Excess of $100

Each deposit slip or credit ticket reflecting a transaction in excess of $100 or the equivalent record for direct deposit or other funds transfer deposit transactions. The slip or ticket must record the amount of any currency involved.

Records to Reconstruct Demand Deposit Accounts

Records prepared or received by the bank in the ordinary course of business, which would be needed to reconstruct a transaction account and to trace a check in excess of $100 deposited in a demand deposit account through its domestic processing system or to supply a description of a deposited check in excess of $100.

Certificates of Deposit Purchased or Presented

This record shall contain:

- Name of customer (purchaser or presenter).
- Address of customer.
- Taxpayer identification number (TIN) of customer.
- Description of the certificate of deposit.
- Notation of the method of payment if purchased.
- Date of transaction.

Purchase of Monetary Instruments of $3,000 or More

A bank must maintain a record of each bank check or draft, cashier's check, money order, or traveler's check for $3,000 or more in currency.

If the purchaser has a deposit account with the bank, this record shall contain:

- Name of purchaser.
- Date of purchase
- Type(s) of instrument purchased.
- Amount in dollars of each of the instrument(s) purchased.
- Serial number(s) of the instrument(s) purchased.

If the purchaser does not have a deposit account with the bank, this record shall contain:

- Name of purchaser.
- Address of purchasers.
- Social security number of purchaser or alien identification number.
- Date of birth of purchaser.
- Date of purchase
- Type(s) of instrument purchased.
- Amount in dollars of each of the instrument(s) purchased.
- Serial number(s) of the instrument(s) purchased.
- Description of document or method used to verify the name and address of the purchaser (e.g., state of issuance and number driver's license).

Funds Transfers of $3,000 or More

A bank's BSA recordkeeping requirements with respect to funds transfer vary based upon the role of a bank with respect to the funds transfer.

Bank acting as an originator's bank. For each payment order that a bank accepts as the originator's bank, the bank must obtain and retain a record of the following information:

- Name and address of originator.
- Amount of the payment order.
- Execution date of the payment order.
- Any payment instruction received from the originator with the payment order.
- Identity of the beneficiary's bank.
- 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.

- For each payment order that a bank accepts for an originator that is not an established customer of the bank, in addition to the information listed above, a bank must obtain additional information as required under 31 CFR 103.33(e)(2).

Bank acting as an intermediary bank or a beneficiary's bank. For each payment order that a bank accepts as an intermediary bank, or a beneficiary's bank, the bank must retain a record of the payment order.

- For each payment order that a bank accepts for a beneficiary that is not an established customer of the bank, the bank must also obtain additional information as required under 31 CFR 103.33(e)(3).

Exceptions. The BSA does not require a bank to maintain records for the following types of funds transfers: (1) funds transfers where both the originator and beneficiary are the same person and that originator's bank and the beneficiary's bank are the same bank; and (2) transfers where the originator and beneficiary are any of the following:

- A bank.
- A wholly owned domestic subsidiary of a bank chartered in the United States.
- A broker or dealer in securities.
- A wholly owned domestic subsidiary of a broker or dealer in securities.
- The United States.
- A state or local government.
- A federal, state, or local government agency or instrumentality.

Taxpayer Identification Number

A record of the TIN of *any* customer opening an account. In cases of joint accounts, information on a person with a financial interest must be maintained. (If the person is a nonresident alien (NRA), record the passport number or a description of some other government document used to verify identity.) This information must be recorded within 30 days of the date the transaction occurs. In the event a bank is unable to secure the information, it must maintain a list containing the names, addresses, and account numbers of those members for whom it has been unable to secure the information.

Exceptions. A bank does not need to maintain TIN for accounts or transactions with the following:

- Agencies and instrumentalities of federal, state, local, or foreign governments.
- Judges, public officials, or clerks of courts of record as custodians of funds in controversy or under the control of the court.
- Certain aliens as specified in 31 CFR 103.34(a)(3)(iii-vi).
- Certain tax exempt organizations and units of tax-exempt organizations (31 CFR 103.34(a)(3)(vii)).
- A person under 18 years of age with respect to an account opened as a part of a school thrift savings program, provided the annual dividend is less than $10.
- A person opening a Christmas club, vacation club, and similar installment savings programs, provided the annual dividend is less than $10.
- NRAs who are not engaged in a trade or business in the United States.

Suspicious Activity Report and Supporting Documentation

A bank must maintain a record of any SAR filed and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing.

Currency Transaction Report

A bank must maintain a record of all Currency Transaction Reports (CTR) for a period of five years from the date of filing.

Designation of Exempt Person

A bank must maintain a record of all designation of persons exempt from CTR reporting as filed with the Treasury (i.e., FinCEN Form 110) for a period of five years from the designation date.

Customer Identification Program

A bank must maintain a record of all information it obtains under its procedures for implementing its CIP. At a minimum, these records must include the following:

- All identifying information about a customer (e.g., name, date of birth, address, and TIN).
- A description of the document that the bank relied upon to identity of the customer.
- A description of the nondocumentary methods and results of any measures the bank took to verify the identity of the customer.

- A description of the bank's resolution of any substantive discrepancy discovered when verifying the identifying information obtained.

A bank must retain the identifying information about a customer for a period of five years after the date the account is closed, or in the case of credit card accounts, five years after the account becomes closed or dormant.

A bank must retain the information relied on, methods used to verify identity, and resolution of discrepancies for a period of five years after the record is made.

As noted, these BSA recordkeeping requirements are independent of and in addition to requirements to file and retain reports imposed by other laws. For the meaning of the BSA terms, refer to 31 CFR 103.11.

Appendix Q: Acronyms

Acronym or abbreviation	Full name
ACH	Automated Clearing House
AML	Anti-money Laundering
APO	Army Post Office
ATM	Automated Teller Machine
APT	Asset Protection Trust
BCBS	Basel Committee on Banking Supervision
BHC	Bank Holding Company
BIS	Bank for International Settlements
BSA	Bank Secrecy Act
CDD	Customer Due Diligence
CFR	Code of Federal Regulations
CHIPS	Clearing House Interbank Payments System
CIF	Customer Information File
CIP	Customer Identification Program
CMIR	Report of International Transportation of Currency or Monetary Instruments
CTR	Currency Transaction Report
DCN	Document Control Number
E-banking	Electronic Banking
E-cash	Electronic Cash
EDD	Enhanced Due Diligence

EFT	Electronic Funds Transfer
EIC	Examiner in Charge
EIN	Employer Identification Number
EPN	Electronic Payments Network
ERISA	Employee Retirement Income Security Act of 1974
FAQ	Frequently Asked Question
FATF	Financial Action Task Force on Money Laundering
FBAR	Report of Foreign Bank and Financial Accounts
FBI	Federal Bureau of Investigation
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
Fedwire	Fedwire Funds Service
FFIEC	Federal Financial Institutions Examination Council
FGO	Foreign Gateway Operator
FIL	Financial Institution Letter
FinCEN	Financial Crimes Enforcement Network
FPO	Fleet Post Office
GAO	U.S. Government Accountability Office
GO	Gateway Operator
HIDTA	High Intensity Drug Trafficking area
HIFCA	High Intensity Financial Crime Area
IAIS	International Association of Insurance Supervisors
IAT	International Automated Clearing House Transaction

IBC	International Business Corporation
IMF	International Monetary Fund
INCSR	International Narcotics Control Strategy Report
IOLTA	Interest on Lawyers' Trust Account
IP	Internet protocol
IRA	Individual Retirement Account
IRS	Internal Revenue Service
ISO	Independent Sales Organization
ITIN	Individual Taxpayer Identification Number
IVTS	Informal Value Transfer System
KYC	Know Your Customer
LCU	Letters to Credit Unions
MIS	Management Information Systems
MLSA	Money Laundering Suppression Act of 1994
MLTA	U.S. Money Laundering Threat Assessment
MSB	Money Services Business
NACHA	NACHA — The Electronic Payments Association
NAICS	North American Industry Classification System
NASD	National Association of Securities Dealers
NASDAQ	National Association of Securities Dealers Automated Quotation Systems
NBFI	Nonbank Financial Institutions
NCCT	Noncooperative Countries and Territories
NCUA	National Credit Union Administration

NDIP	Nondeposit Investment Products
NGO	Nongovernmental Organization
NIS	Nominee Incorporation Services
NRA	Nonresident Alien
NSF	Nonsufficient Funds
NSL	National Security Letter
NYCH	New York Clearing House Association, L.L.C.
OCC	Office of the Comptroller of the Currency
ONDCP	Office of National Drug Control Policy
ODFI	Originating Depository Financial Institution
OFAC	Office of Foreign Assets Control
OFC	Offshore Financial Center
OTS	Office of Thrift Supervision
PEP	Politically Exposed Person
PIC	Private Investment Company
POS	Point-of-Sale
PTA	Payable Through Account
PUPID	Payable Upon Proper Identification
RA	Regulatory Alerts
RCC	Remotely Created Check
RDC	Remote Deposit Capture
RDFI	Receiving Depository Financial Institution
ROE	Report of Examination

SAR	Suspicious Activity Report
SDN	Specially Designated Nationals or Blocked Persons
SEC	U.S. Securities and Exchange Commission
SOD	Summary of Deposits
SSN	Social Security Number
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TD F	Treasury Department Form
TIN	Taxpayer Identification Number
TPSP	Third-Party Service Provider
UBPR	Uniform Bank Performance Report
U.S. Treasury	U.S. Department of the Treasury
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
USC	United States Code
Web CBRS	Web Currency and Banking Retrieval System

Appendix R: Enforcement Guidance

Interagency Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements[272]

This interagency statement, jointly issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration[273] sets forth the Agencies' policy on the circumstances in which an Agency will issue a cease and desist order to address noncompliance with certain Bank Secrecy Act/Anti-Money Laundering ("BSA/AML") requirements,[274] particularly in light of the specific BSA/AML compliance provisions in section 8(s) of the Federal Deposit Insurance Act ("FDIA") and section 206(q) of the Federal Credit Union Act ("FCUA").[275]

BSA/AML Compliance Program Requirement.

Under section 8(s) of the FDIA and section 206(q) of the FCUA, each of the Agencies is directed to prescribe regulations requiring each insured depository institution to establish and maintain procedures reasonably designed to assure and monitor the institution's compliance with the requirements of the Bank Secrecy Act ("BSA Compliance Program"). Sections 8(s) and 206(q) also require that each Agency's examinations of an insured depository institution review the BSA Compliance Program and that its reports of examination describe any problem with the BSA Compliance Program. Finally, sections 8(s) and 206(q) state that if an insured depository institution has failed to establish and maintain a BSA Compliance Program or has failed to correct any problem with the BSA Compliance Program previously reported to the institution by the appropriate Agency, the appropriate Agency shall issue a cease and desist order against the institution. As required by sections 8(s) and 206(q), each of the Agencies has issued regulations that require any institution it supervises or insures to establish and maintain a BSA Compliance Program. Each of these regulations imposes substantially the same

---

[272] This statement is intended to set forth general policy guidance. It is not intended to compel or preclude an enforcement or other supervisory action as necessary in a specific factual situation.

[273] Collectively the "Agencies" or individually the "Agency."

[274] This statement does not address the assessment of civil money penalties for violations of the BSA or its implementing regulations. FinCEN has authority to assess such penalties under the BSA. Likewise, the Agencies also have such authority under their general enforcement statutes. 12 USC 1818(i)(2), 1786(k)(2).

[275] 12 USC 1818(s); 12 USC 1786(q).

requirements.[276] Specifically, under each Agency's regulations, a BSA Compliance Program must have, at a minimum, the following elements:

- A system of internal controls to assure ongoing compliance with the BSA;
- Independent testing for BSA/AML compliance;
- A designated individual or individuals responsible for coordinating and monitoring BSA/AML compliance; and
- Training for appropriate personnel.

In addition, a BSA Compliance Program must include a CIP with risk-based procedures that enable the institution to form a reasonable belief that it knows the true identity of its customers.[277]

Communication of Supervisory Concerns about BSA Compliance Programs.

When an Agency identifies supervisory concerns relating to a banking organization's or credit union's BSA Compliance Program in the course of an examination or otherwise, the Agency may communicate those concerns by various means. The particular method of communication used typically depends on the seriousness of the concerns. These methods include:

- Informal discussions by examiners with an institution's management during the examination process;
- Formal discussions by examiners with the board of directors as part of or following the examination process;
- Supervisory letters and other written communications from examiners or the agency to an institution's management;

---

[276] 12 CFR 21.21 (OCC); 208.63 (Board of Governors); 326.8(c) (FDIC); 563.177 (OTS); 748.2 (NCUA). The provisions of section 8(s) are also made applicable to certain banking organizations other than insured depository institutions. 12 USC 1818(b)(3), (b)(4). The OCC's regulations also apply to federal branches and agencies of foreign banks. 12 USC 3102(b); 12 CFR 28.13. The Federal Reserve's regulations also apply to Edge and agreement corporations, and branches, agencies, and other offices of foreign banking organizations. 12 CFR 211.5, 211.24. BSA Compliance Programs that comply with these Agency regulations are also deemed to comply with Treasury regulations issued pursuant to the BSA, which separately requires that financial institutions establish AML programs. Refer to 31 CFR 103.120(b); 31 USC 5318(h).

[277] 12 CFR 21.21(b)(2) (OCC); 208.63(b)(2), 211.5(m)(2), 211.24(j)(2), (Board of Governors); 326.8(b)(2) (FDIC); 563.177(b)(2) (OTS); 748.2(b)(2) (NCUA); 31 CFR 103.121.

- A finding contained in the report of examination or in other formal communications from an Agency to an institution's board of directors indicating deficiencies or weaknesses in the BSA Compliance Program; or

- A finding contained in the report of examination or in other formal communications from the Agency to an institution's board of directors of a violation of the regulatory requirement to implement and maintain a reasonably designed BSA Compliance Program.

As explained below, in order to be a "problem" with the BSA Compliance Program that will result in a cease and desist order under sections 8(s) or 206(q) if not corrected by the institution, deficiencies in the BSA Compliance Program must be identified in a report of examination or other written document as requiring communication to an institution's board of directors or senior management as matters that must be corrected. However, other issues or suggestions for improvement may be communicated through other means.

Enforcement Actions for BSA Compliance Program Failures.

In accordance with sections 8(s)(3) and 206(q)(3), the appropriate Agency will issue a cease and desist order against a banking organization or a credit union for noncompliance with BSA Compliance Program requirements in the following circumstances, based on a careful review of all the relevant facts and circumstances.

Failure to establish and maintain a reasonably designed BSA Compliance Program. The appropriate Agency will issue a cease and desist order based on a violation of the requirement in sections 8(s) and 206(q) to establish and maintain a reasonably designed BSA Program where the institution:

- Fails to have a written BSA Compliance Program, including a CIP that adequately covers the required program elements (i.e., internal controls, independent testing, designated compliance personnel, and training); or

- Fails to implement a BSA Compliance Program that adequately covers the required Program elements (institution-issued policy statements alone are not sufficient; the program as implemented must be consistent with the banking organization's written policies, procedures, and processes); or

- Has defects in its BSA Compliance Program in one or more program elements that indicate that either the written Compliance Program or its implementation is not effective, for example, where the deficiencies are coupled with other aggravating factors, such as (i) highly suspicious activity creating a significant potential for unreported money laundering or terrorist financing, (ii) patterns of structuring to evade reporting requirements, (iii) significant insider complicity, or (iv) systemic failures to file CTRs, SARs, or other required BSA reports.[278]

[278] These examples do not in any way limit the ability of an Agency to bring an enforcement action where the failure to have or to implement a BSA Compliance Program is demonstrated by other deficiencies.

For example, an institution that has procedures to provide BSA/AML training to appropriate personnel, independent testing, and a designated BSA/AML compliance officer, would nonetheless be subject to a cease and desist order if its system of internal controls (such as customer due diligence, procedures for monitoring suspicious activity, or an appropriate risk assessment) fails with respect to a higher risk area or to multiple lines of business that significantly impact the institution's overall BSA compliance. Similarly, a cease and desist order would be warranted if, for example, an institution has deficiencies in the required independent testing element of the Program and those deficiencies are coupled with evidence of highly suspicious activity creating a significant potential for unreported money laundering or terrorist financing in the institution. However, other types of deficiencies in an institution's BSA Compliance Program or in implementation of one or more of the required Program elements will not necessarily result in the issuance of a cease and desist order, unless the deficiencies are so severe as to render the Program ineffective when viewed as a whole. For example, an institution that has deficiencies in its procedures for providing BSA/AML training to appropriate personnel, but has effective controls, independent testing, and a designated BSA/AML compliance officer, may ordinarily be subject to examiner criticism and/or supervisory action other than the issuance of a cease and desist order, unless the training program deficiencies, viewed in light of all relevant circumstances, are so severe as to result in a finding that the organization's Program, taken as a whole, is not effective.

In determining whether an organization has failed to implement a BSA Compliance Program, an Agency will also consider the application of the organization's Program across its business lines and activities. In the case of institutions with multiple lines of business, deficiencies affecting only some lines of business or activities would need to be evaluated to determine if the deficiencies are so severe or significant in scope as to result in a conclusion that the institution has not implemented an effective overall program.

Failure to correct a previously reported problem with the BSA Compliance Program. A history of deficiencies in an institution's BSA Compliance Program in a variety of different areas, or in the same general areas, may result in a cease and desist order on that basis. An Agency will, in accordance with sections 8(s) and 206(q), and based on a careful review of the relevant facts and circumstances, issue a cease and desist order whenever an institution fails to correct a problem with BSA/AML compliance identified during the supervisory process. In order to be considered a "problem" within the meaning of sections 8(s)(3)(B) and 206(q)(3)(B), however, a deficiency reported to the institution ordinarily would involve a serious defect in one or more of the required components of the institution's BSA Compliance Program or implementation thereof that a report of examination or other written supervisory communication identifies as requiring communication to the institution's board of directors or senior management as a matter that must be corrected. For example, failure to take any action in response to an express criticism in an examination report regarding a failure to appoint a qualified compliance officer could be viewed as an uncorrected problem that would result in a cease and desist order.

An Agency will ordinarily not issue a cease and desist order under sections 8(s) or 206(q) for failure to correct a BSA Compliance Program problem unless the deficiencies

subsequently found by the Agency are substantially the same as those previously reported to the institution. For example, if an Agency notes in one examination report that an institution's training program was inadequate because it was out of date (for instance if it did not reflect changes in the law), and at the next examination the training program is adequately updated, but flaws are discovered in the internal controls for the BSA/AML Program, the Agency may determine not to issue a cease and desist order under sections 8(s) or 206(q) for failure to correct previously reported problems and will consider the full range of potential supervisory responses. Similarly, if an institution is cited in an examination report described above for failure to designate a qualified BSA compliance officer, and the institution by the next examination has appointed an otherwise qualified person to assume that responsibility, but the examiners recommend additional training for the person, an Agency may determine not to issue a cease and desist order under sections 8(s) or 206(q) based solely on that deficiency. Statements in a written examination report or other supervisory communication identifying less serious issues or suggesting areas for improvement that the examination report does not identify as requiring communication to the board of directors or senior management as matters that must be corrected would not be considered "problems" for purposes of sections 8(s) and 206(q).

The Agencies recognize that certain types of problems with an institution's BSA Compliance Program may not be fully correctable before the next examination, for example, remedial action involving adoption or conversion of computer systems. In these types of situations, a cease and desist order is not required provided the Agency determines that the institution has made acceptable substantial progress toward correcting the problem at the time of the examination immediately following the examination where the problem was first identified and reported to the institution.

Other enforcement actions for BSA Compliance Program deficiencies. As noted above, in addition to the situations described in this Statement where an Agency will issue a cease and desist order for a violation of the BSA Compliance Program regulation or for failure to correct a previously reported Program "problem," an Agency may also issue a cease and desist order or enter into a formal written agreement, or take informal enforcement action against an institution for other types of BSA/AML Program concerns. In these situations, depending upon the particular facts involved, an Agency may pursue enforcement actions based on unsafe and unsound practices or violations of law, including the BSA. The form of the enforcement action in a particular case will depend on the severity of the noncompliance, weaknesses, or deficiencies, the capability and cooperation of the institution's management, and the Agency's confidence that the institution will take appropriate and timely corrective action.

BSA Reporting and Recordkeeping Requirements.

Suspicious activity reporting requirements. Under regulations of the Agencies and the Treasury Department, organizations subject to the Agencies' supervision are required to file a SAR when they detect certain known or suspected criminal violations or suspicious

transactions.[279] Suspicious activity reporting forms the cornerstone of the BSA reporting system, and is critical to the United States' ability to utilize financial information to combat money laundering, terrorist financing, and other financial crimes. The regulations require banking organizations and credit unions to file SARs with respect to the following general types of activity:

- Known or suspected criminal violations involving insider activity in any amount;
- Known or suspected criminal violations aggregating $5,000 or more when a suspect can be identified;
- Known or suspected criminal violations aggregating $25,000 or more regardless of potential suspects; or
- Suspicious transactions of $5,000 or more that involve potential money laundering or BSA violations.

The SAR must be filed within 30 days of detecting facts that may constitute a basis for filing a SAR (or within 60 days if there is no subject).

The Agencies will cite a violation of the SAR regulations, and will take appropriate supervisory action, if the organization's failure to file a SAR (or SARs) evidences a systemic breakdown in its policies, procedures, or processes to identify and research suspicious activity, involves a pattern or practice of noncompliance with the filing requirement, or represents a significant or egregious situation.

Other BSA reporting and recordkeeping requirements. Banking organizations and credit unions also are subject to other BSA reporting and recordkeeping requirements set forth in regulations issued by the Treasury Department.[280] These requirements are reviewed in detail in the *FFIEC BSA/AML Examination Manual*; they include, inter alia, requirements applicable to cash and monetary instrument transactions and funds transfers, Currency Transaction Report ("CTR") filing and exemption rules, and due diligence, certification, and other requirements for foreign correspondent and private banking accounts.

Enforcement actions for nonprogram BSA/AML requirements. In appropriate circumstances, an Agency may take formal or informal enforcement actions to address violations of BSA/AML requirements other than the BSA Compliance Program requirements. These other requirements include, for example, the SAR and CTR regulatory obligations described above.

---

[279] 12 CFR 21.11 (OCC); 208.62, 211.5(k), 211.24(f), 225.4(f) (Board of Governors); Part 353 (FDIC); 563.180(d) (OTS); 748.1(c) (NCUA); 31 CFR 103.18 (Treasury).
[280] 31 CFR Part 103.

Appendix S: Key Suspicious Activity Monitoring Components

Index

A

Account Closure,
foreign correspondent accounts, 20, 119, 128
Affiliate,
BSA/AML Compliance Program Structures, 160, 162, 164, 165
concentration accounts, 267
Customer Identification Program (CIP) reliance, 57
foreign branches, 169, 173
foreign correspondent accounts, 118, 121, 126
insurance (sales of), 262, 265
nondeposit investment products (NDIP), 57, 255, 257
private banking, 281
Section 314(a) information requests, 99, 100, 103, 104
Suspicious Activity Reports (SAR), 67, 74, 80
Aggregate Risk Profile. *See* Risk Assessment.
Aggregation. *See* Currency Transaction Reports (CTR).
Annuity Contract. *See* Insurance.
Annunzio–Wylie Anti-Money Laundering Act, 7, 110
Applications,
Automated Clearing House (ACH) transactions, 228
insurance, H-14
mergers, acquisitions, and other business combinations (consideration of a bank's AML record in), 8, 10
Office of Foreign Assets Control (OFAC) licenses, 150, 154
pouch activities, 204
taxpayer identification number, 54, 60, H-2
Army Post Office (APO),
customer address, 54, 115
Asset Protection Trust (APT), 292, H-17
Asset Seizure, 19, 280
Attorney General. *See* U.S. Attorney General.
Audit. *See* Independent Testing.
Automated Clearing House (ACH) Transactions. *See also* Electronic Funds Transfers (EFT); Funds Transfers; Funds Transfers Recordkeeping; Remote Deposit Capture (RDC).
24, 72, 213, 25-251, C-4, Q-1
cross-border, 151, 224, 230, M-1
examination procedures, 232-233
international ACH transactions (IAT), 154, 224, 225, 232, H-11
Office of Foreign Assets Control (OFAC) screening, 153-154, 231
Originating Depository Financial Institution (ODFI), 155, 225, 226, 227-231
overview, 224-231

Receiving Depository Financial Institution (RDFI), 154, 225-231
red flags, F-3
request letter items, H-11
third-party service provider (TPSP), 239, 241
Automated Teller Machine (ATM) Transactions, 24, 72, 86, 208, 209, 213, 234-237, 250-254, F-331
foreign, 294
privately owned, 25, 250-252, F-6, H-13

B

Backfiling. *See* Currency Transaction Reports (CTR).
Bank for International Settlements (BIS), 160, 161, 169, 218, C-3, E-1
Bank Holding Company (BHC), 67, 80, A-5, C-1
filing Suspicious Activity Reports (SAR), 165, 167, A-5
Office of Foreign Assets Control (OFAC) application to, 148
Section 314(a) information sharing, 100
sharing SARs, 80
Bank Secrecy Act (BSA) Officer, 35, 36, 40, 311, H-1
designation of, 33
periodic training for, 37
Basel Committee on Banking Supervision (BCBS), 160, 161, 169, 218, C-3, E-1
Bearer Shares, 224-226, 228, 229, 282, H-19
request letter items, H-19
Beneficial Owners. *See* Nominal and Beneficial Owners.
Blocked Transactions. *See* Office of Foreign Assets Control (OFAC).
Brokered Deposits. *See also* Contractual Agreements, Contracts.
definition of customer for Customer Identification Program (CIP), 246
examination procedures, 248-249
overview, 246-247
request letter items, H-12
Brokers/Dealers. *See* Nonbank Financial Institutions.
BSA Compliance Program Structures,
consolidated programs, 164-165
examination procedures, 166-168
overview, 160-165
risk assessment, 28
suspicious activity reporting, 165
Bulk Currency Shipments, 188-194
contracts, 192
examination procedures, 193-194
overview, 188-192
red flags, F-5
request letter items, H-6
Bureau of Customs and Border Protection. *See* U.S. Bureau of Customs and Border Protection.
Business Entities. *See also* Foreign Business Entities.

25, 239
beneficial owners, 324, 325, 326, 327, 328, F-1
domestic, 323-324
examination procedures, 329-330
Nominee Incorporation Services (NIS), 325
overview, 323-328
red flags, F-7
request letter items, H-19

C

Casas de Cambio, 25, 199, 202
cross border financial institution transaction red flags, F-4, F-5
Cash-Intensive Businesses, 25, 285
examination procedures, 333
overview, 331-332
request letter items, H-16, H-17, H-20
Cash Management, 53, 183, 210, 255, 279, 286
Casinos. *See* Nonbank Financial Institutions.
Certificate of Deposit, 68, P-2
collateral to secure a loan, 270, F-4
Certifications,
bearer shares, 282
CIP reliance, 61, H-3
foreign correspondent accounts, 118, 119, 125, 128, A-4, H-5, R-6
Section 314(a) record searches, 97
Charities. *See* Nongovernmental Organizations.
Civil Liability, 14
SAR safe harbor, 68, 101
Civil Money Penalty(ies). *See also* Criminal Penalty(ies).
10, 14, 19, 120, C-2, M-2, R-1
Clearing House Interbank Payments System (CHIPS), 213-215, Q-1
described, 215
Collection Accounts. *See* Concentration Accounts.
Common Carrier. *See* International Transportation of Currency or Monetary Instruments.
Concentration Accounts, 24, 267-269, F-4, H-13, H-14
collection accounts, 267, H-14
examination procedures, 269
intraday accounts, 267, H-14
omnibus accounts, 267, H-13, H-14
overview, 267-268
request letter items, H-14
special use accounts, 24, H-14
suspense accounts, 267, H-11, H-13, H-14
sweep accounts, 183, 255, 267, 279, H-14
Confidentiality,
business entities, 326

grand jury proceedings, 70
international business corporations (IBC), 324
National Security Letters (NSL), 70-71, 81
private banking, 280
Private Investment Companies (PIC), 325
Section 314(a) record searches, 98, 99, 100, 103, H-4
Section 314(b) information sharing, 101, 102, 104, 105
Suspicious Activity Reports (SAR), 79-80
Continuous Linked Settlement (CLS) Bank, 215
Contractual Agreements, Contracts,
brokered deposits, 246
bulk currency shipments, 192-193, 194, H-9
business entities, 327
Customer Identification Program (CIP) reliance, 58, 61, H-3
funds transfers, F-2
insurance, 262, 265, H-14
foreign correspondent accounts, 183, 186, H-5
nondeposit investment products (NDIP), 256, 257, 260, H-13
payable through accounts (PTA), 199, 202, H-9
pouch activities, 205, 206
prepaid cards, 235-236
private banking, 280
privately owned automated teller machines (ATM), 251-252, 253, F-6, H-13
Remote Deposit Capture (RDC), 190, 209, 210-211, 212, H-11
SAR safe harbor, 68
shell companies, F-7
third-party payment processors, 239
trust and asset management services, 286
U.S. dollar drafts, 24, 117, 197
Correspondent Accounts (Domestic), L-1
examination procedures, 181-182
overview, 178-180
request letter items, H-8
Correspondent Accounts (Foreign). *See also* Foreign Correspondent Account Recordkeeping and Due Diligence.
6, 8, 17, 24, 27, 29, 41, 51, 141, 152, 175, 176, 204, 209, 218, 227, 303, 327, F-7, J-1, R-6
bulk currency shipments, 192
examination procedures, 186-187
laws and regulations, A-3, A-4
mandatory account closures, 20, 119, 120
nested accounts, 184
overview, 183-185
payable through accounts (PTA), 198-200, 202
recordkeeping and due diligence examination procedures, 125-129
recordkeeping and due diligence overview, 45, 117-124

request letter items, H-5, H-6, H-8, H-9
sound practices, 185
special measures, 139-140
U.S. dollar drafts, 195, 196
Correspondent Bank. *See also* Respondent Bank.
domestic, 178, 182, 195, 214-216, 219, 222, F-4, H-8
foreign, 6, 17, 41, 117, 120, 125, 127, 128, 141, 152, 175, 176, 183-187, 192, 196, 198, 202, 204, 218, 219, 222, 227, 327, C-3, C-4, F-7, H-5, H-6, H-8, H-9
Cover Payments. *See* Funds Transfers.
Credit Cards, 60, 112, 158, 208, 235, 236, 239, 241, 270, 279, 324
recordkeeping requirements, 56, P-6
system operators, 9, D-1
Criminal Activity, 13, 14, 76, 236, 326, F-1, G-1
Criminal Investigation Division. *See* Internal Revenue Service (IRS).
Criminal Penalty(ies). *See also* Civil Money Penalties.
8, 13-14, A-3, G-1
Currency Activity Reports, 71-72, 82, H-3
Currency Exchanges(ers), 25, 129, 132, 309, D-1, F-10
Currency Transaction Report Exemptions. *See also* Currency Transaction Reports (CTR).
17-18, 20, 34, 35, 39, 51, 86, 88, 166, 188, 316-317, 332, F-2, P-5, R-6
annual review — Phase I customer, 91
annual review — Phase II customer, 93
effect on other legal and regulatory requirements, 94
examination procedures, 95-96
filing time frames, 91, 93
ineligible businesses, 92
laws and regulations, A-2
nonlisted business, 91, 95
overview, 90-94
payroll customers, 93
Phase I exemptions, 90-91, 95
Phase II exemptions, 91-93, 95-96
request letter items, H-4
safe harbor, 93-94
supporting documentation, 95, 96
Currency Transaction Reports (CTR). *See also* Currency Transaction Report Exemptions.
17-18, 19, 20, 34, 35, 39, 46, 51, 71, 73, 84, 116, 179, 182, 191, 202, 205, 243, 332, F-2, G-1, G-2, Q-1, R-3, R-6
aggregation, 86, 88
backfiling, 86-87
examination procedures, 88-89
filing time frames, 86
laws and regulations, A-2
overview, 86-87

record retention, 86, P-5
request letter items, H-1, H-4, H-9
safe harbor, 93-94
tools for transaction testing, 96, O-1
Customer. *See* Customer Identification Program (CIP).
Customer Due Diligence (CDD). *See also* Enhanced Due Diligence (EDD); Know Your Customer (KYC).
34, 39, 40, 210, 212, 236, 238, 256, Q-1
adequacy of information, O-2
automated clearing house (ACH) transactions, 229-230
beneficial owners, 65
deposit brokers, 246-247
examination procedures, 66
for suspicious activity reporting, 71, 74, 82, 84
foreign correspondent accounts, 120-124, 126-129
funds transfers, 218
money services business, 311-313
OFAC risk assessment, 151
overview, 63-65
payable through accounts, 199
private banking, 130-137, 281-282
privately owned ATMs, 253-254
risk assessment, 27-28
trade finance, 275, 277
Customer Identification Program (CIP), 33, 35, 38, 40, 42, 50, 84, 151, 230, 233, 238, 247, 252, P-5, Q-1, R-2, R-3
"account" defined, 53
adequacy of information, O-2
brokered deposits — customer defined, 246
business entities (domestic and foreign), 327-328
cash intensive businesses, 333
comparison with government lists, 57
"customer" defined, 53
customer information required, 54
customer notice, 57
customer verification, 54-56
electronic banking, 208, 212
examination procedures, 59-62
laws and regulations, A-3
lending activities, 270, 272
money services businesses, 312
nondeposit investment products, 256, 260
nongovernmental organizations (NGO) and charities, 320
nonresident aliens (NRA) and foreign individuals, 294, 295
overview, 52-58
private banking, 282

recordkeeping requirements, 56-57, P-5-P-6
reliance on another financial institution, 57-58
request letter items, H-1, H-2, H-3, H-13, H-14
risk assessment, 27-28
separate from OFAC, 149
separate from other legal requirements, 58
trust and asset management services, 286-287, 288, 292
U.S. dollar drafts, 197
use of third parties, 58
Customer Notice. *See* Customer Identification Program (CIP).
Customer Verification. *See* Customer Identification Program (CIP).
Customers and Entities. *See* Risk Assessment.

D

Debit Cards, 142, 208, 213, 228, L-1
Developing Conclusions, 6, 16, 30, 43
appropriate supervisory response, 44, 48
overview, 44-47
examination procedures, 48-51
Document Control Number (DCN). *See* Internal Revenue Service (IRS).
Dollar Drafts. *See* U.S. Dollar Drafts.
Dual-Employee Arrangements. *See* Nondeposit Investment Products.

E

E-Cash. *See* Electronic Cash.
Electronic Banking (e-banking). *See also* Internet Banking.
23, 24, 151, 204, 208, 212, H-10, H-11, J-1, M-1
examination procedures, 212
overview, 208-211
request letter items, H-10
Electronic Cash (e-cash), 20
examination procedures, 238
overview, 234-237
prepaid/stored value cards, 12, 206, 234-238, 239, F-8, L-1
request letter items, H-11, H-12
stored value cards, 235
Electronic Funds Transfers (EFT). *See also* Automated Clearing House (ACH) Transactions; Clearing House Interbank Payment System (CHIPS); Funds Transfers; Funds Transfers Recordkeeping.
224, 225, 250, Q-2
Electronic Payments Network (EPN), 225
Embassy and Foreign Consulate Accounts, 303, A-3
examination procedures, 305, 306
overview, 303, 304
red flags, F-7

request letter items, H-6, H-18
Employer Identification Number (EIN), 88, 112
for Customer Identification Program (CIP), 54
Enforcement Guidance, R-1
interagency statement on, 11, R-1
Enhanced Due Diligence (EDD). *See also* Customer Due Diligence. 8, 64, 66, 289
for Automated Clearing House (ACH) transactions, 229
for bulk shipments of currency, 191, 194
for certain foreign banks, 120, 124, 126-129, A-4
for electronic banking, 209,
for higher-risk customers, 57-58
insurance, 264
money services business (MSB), 307, 310, 312-314
nondeposit investment products (NDIP), 256-258, 260
nongovernmental organizations and charities, 321
parallel banking, 176
payable through accounts (PTA), 201
private banking, 132
request letter items, H-16
trust and asset management services, 289
Enhanced Scrutiny,
funds transfers, 196
foreign correspondent accounts, 123, 127, 129, 132
private banking accounts, 130, 132-134, 136
Enterprise Computing Center – Detroit. *See* Internal Revenue Service.
Examination Scope, 5, 15, 16, 19
examination procedures, 19-21
request letter items, H-1, H-8
Examiner in Charge (EIC), 19, 49, 167
Export Administration Act of 1979, 26
Exporter,
trade finance, 273

F

Federal Banking Agencies, 7-11, 14
BSA responsibilities, 9-11
Currency Transaction Report (CTR) reviews, 91
Customer Identification Program (CIP) verification expectations, 56, 58
defined, 9
laws and regulations, A-1
nondeposit investment product (NDIP) activity — supervision of, 255
money services businesses (MSB) guidance, 309, 310, 313
OFAC compliance — evaluation of, 16
politically exposed persons (PEP) — verification of, 299
Suspicious Activity Reporting, 67, 76, 79, 80

Suspicious Activity Report (SAR) quality guidance, 388, L-1, L-2
Federal Bureau of Investigation (FBI), 70-71, 79
National Security Letters, 70-71
notifying law enforcement of suspicious activity, 67
Federal Credit Union Act (FCUA), 7, R-1
authority granted, 9
Federal Deposit Insurance Act (FDI Act), 7, R-1
authority granted, 9
definition of insured bank, D-1
Federal Financial Institutions Examination Council (FFIEC) *Information Technology Examination Handbook*, 15
information on electronic banking, 208
types of electronic cash products, 234
types of retail payment systems, 155, 231, 250
types of wholesale payment systems, 213
Federal Functional Regulator, 10, 57
defined, 10
laws and regulations, A-3
request letter items — Customer Identification Program (CIP) reliance provision, H-3
Fedwire Funds Service (Fedwire®). *See* Funds Transfers.
Financial Action Task Force on Money Laundering (FATF), 26, 122, 216, 275, C-3, E-1, F-2, F-9, F-10
business entities, 326
defined, E-1
Noncooperative Countries and Territories (NCCT), 276, C-3, E-1, F-2, F-5, F-10
trade finance activities standards, 274, 275
Financial Institution,
statutory definition of, D-1, D-2
Financial Institution Letters (FIL),
defined, B-1
Fleet Post Office (FPO), 54, 115
customer address, 54
Foreign Bank and Financial Accounts Reporting,
examination procedures, 143
form, 142, 143
laws and regulations, A-2
overview, 142
report of foreign bank and financial accounts (FBAR), 143
request letter items, H-6
Foreign Branches and Offices, 125, 148, 164, 166
examination procedures, 173-174
host jurisdiction-based examinations, 172
overview, 169-172
request letter items, H-5, H-9
scoping examinations, 171

U.S.-based examinations, 171
Foreign Business Entities. *See also* Offshore Entities.
323-330
examination procedures, 329-330
International Business Corporations (IBC), 25, 279, 281, 284, 324, 325, 328
Offshore Financial Centers (OFC), 26, 324, 326, 327, F-7
Private Investment Companies (PIC), 25, 257, 279, 284, 288, 292, 299, 324, 325, F-1, H-16
Foreign Consulate Accounts. *See* Embassy and Foreign Consulate Accounts.
Foreign Correspondent Account Recordkeeping and Due Diligence. *See also* Correspondent Accounts (Foreign).
24, 27, 29, 45, 117-129, 139-140, 183-187, 195-196, 198, A-3, A-4, H-5, H-8, M-1
account closure, 119
bulk currency shipments, 188-192
certifications, 118-119, 125, 128, A-4
enhanced due diligence, 121-122
examination procedures, 124-129
foreign shell bank prohibition, 117-118, 125, 128, A-4, H-5
general due diligence, 120-122
monitoring of, 121-122
overview, 117-124
recordkeeping, 117, 119
red flags, F-7
request letter items, H-5, H-8, H-9
risk assessment of foreign financial institutions, 121
special due diligence program for foreign correspondent accounts, 121, 126
special procedures when due diligence cannot be performed, 124
verification, 119
Foreign Financial Institutions. *See* Casas de Cambio; Money Transmitters; Currency Exchanges(ers).
Foreign Individuals. *See* Nonresident Aliens (NRA) and Foreign Individuals.
Foreign Shell Bank. *See* Correspondent Accounts (Foreign).
Formulating Conclusions. *See* Developing Conclusions.
Frequently Asked Questions (FAQ), 58, 98, 150-152, C-4
314(a) record searches, 98
Customer Identification Procedures (CIP), 58
correspondent banking, C-4
OFAC, 150-152
Funds Transfers. *See also* Automated Clearing House (ACH) Transactions; Clearing House Interbank Payment System (CHIPS); Electronic Funds Transfers (EFT); Funds Transfers Recordkeeping.
6, 13, 23, 24, 27, 29, 35, 36, 40, 41, 53, 71, 84, 86, 98, 148, 149, 151, 153, 158, 176, 178, 183, 189, 192, 199, 205, 208, 234, 249, 253, 258, 260, 261, 267, 269, 276, 279, 285, 289, 294, 312, 325,

326, 327, 328, 329, 330, F-2, H-3, H-11, H-14, J-2, L-1, L-2, M-1, O-1, O-2, R-6
cover payments, 215-219, 222, H-11
examination procedures, 221-223
Fedwire Funds Service (Fedwire®), 213-215
overview, 213-220
payable upon proper identification (PUPID), 24, 72, 217, 222, 304, F-7, H-11, J-2
red flags, F-2, F-3, F-4, F-5, F-7, F-9, F-10
request letter items, 213, 225, 250, H-11
Society for Worldwide Interbank Financial Telecommunication (SWIFT), 214-219, 221
Funds Transfers Recordkeeping. *See also* Automated Clearing House (ACH) Transactions; Electronic Funds Transfers (EFT); Funds Transfers.
24, 72, 110-116, 151, 153-154, 157, 192, 213, 224-225, 232, 239, 250, F-2, F-3, H-5, H-11
examination procedures, 116
laws and regulations, A-2
overview, 110-115
record retention requirements, P-1, P-3 to P-4
red flags, F-2, F-4, F-5, F-7, F-8, F-9, F-10
request letter items, H-5, H-10, H-11, H-13
responsibilities of beneficiary's banks, 110-111, 114
responsibilities of intermediary institutions, 110, 113, 116
responsibilities of originator's banks, 110-112, 116
Suspicious Activity Report (SAR) quality guidance, L-1, L-2
tools for transaction testing, O-1
travel rule, 110, 112-116
travel rule abbreviations and addresses, 114
Futures Commission Merchants, 9, D-2

G

Gateway Arrangements. *See* Independent Sales Organization (ISO).
Geographic Locations. *See* Risk Assessment.
Government Lists, 57, 59, 149
no designated list for customer identification purposes, 57
Grand Jury. *See* Confidentiality.

H

Hawala. *See* Informal Value Transfer Systems (IVTS).
Head Office,
foreign branches, 125, 169, 148, 164, 166, 169-174, H-5, H-9, H-10
sharing Suspicious Activity Reports (SAR) with, 80, 83, 165, 173, 176, 178-179, 181, 184-188, 190-191, 193-198, 200
High Intensity Drug Trafficking Area (HIDTA), J-2
defined, 26

High Intensity Financial Crimes Area (HIFCA), J-2
defined, 27
Home Banking Systems, 213
Host Jurisdiction-Based Examinations. *See* Foreign Branches and Offices.

I

Importer, 273-274, F-5, H-16
Independent Sales Organization (ISO), 240, 250, 253, H-13
defined, 240
gateway arrangements, 240
request letter items, H-13
Independent Testing, 6-7, 16-17, 20, 28, 33-36, 38, 41-44, 48-50, 88, 150, 156, 158, 161, 165-166, 172, 312, H-1, R-2, R-4
examination procedures, 6, 16-17, 34-35
frequency of, 34
minimum requirements, 35
money services business (MSB) requirements, 307, 314-315
OFAC, 16, 150, 156
request letter items, H-1
transaction testing, 16-18, 35-36, 40-43, O-1
Individual Retirement Account (IRA), 86
Individual Taxpayer Identification Number (ITIN). *See also* Taxpayer Identification Number (TIN). 88, O-3
for customer identification, 54
Informal Value Transfer Systems (IVTS), 9, 195-196, 216
hawala, 13, 216
Information Sharing, 8, 35, 97-105
documentation of searches performed, 100
examination procedures — 314(a), 103-104
examination procedures — 314(b), 104-105
laws and regulations, A-3
overview, 97-101
request letter items, H-3, H-4, H-5
restrictions and confidentiality, 99-100
safe harbor — 314(b), 101
search requirements, 97-99
voluntary information sharing — 314(b), 100-101
Insurance. *See also* Nonbank Financial Institutions (NBFI). 9, 25, 190, 199, 202, 214, 262-264, 307, F-6, H-18, H-19, L-1
AML compliance program requirements, 262-263
annuity contract, 262
examination procedures, 265-266
laws and regulations, A-2, A-3
life insurance, 262-263, F-6, H-13, H-14
networking arrangements, 262, 265

overview, 262-264
red flags, F-6, F-7, F-11
request letter items, H-13, H-14
suspicious activity reporting requirements for insurance companies, 262
Integration. *See* Money Laundering.
Interest on Lawyers' Trust Accounts (IOLTA), 289, 316, 318, H-19
request letter items, H-19
Internal Controls, 32-34, 39-40, 43, 45, 48-51, 61, 68, 80, 103-104, 125, 135, 150, 152, 159, 161-163, 170-171, 211, 217, 229, 237, 267, 280, 321, R-2, R-3, R-4
examination procedures, 30-32, 39
for a BSA/AML compliance program, 33-34
for an OFAC compliance program, 6, 20-21, 150-152, 158
for concentration accounts, 24, 267-269
Internal Revenue Service (IRS), 18, 19, 53, 78-79, 85, 88, 91, 93-95, 142-143, 293-294, 311, H-1, L-2
Criminal Investigation Division, 78
Document Control Number (DCN), 18
Enterprise Computing Center — Detroit, 19, 85-86, 88, 94, H-1, L-2
International Association of Insurance Supervisors (IAIS), ?
Report of Foreign Bank and Financial Accounts, 142-143
International Automated Clearing House Transactions (IAT). *See* Automated Clearing House Transactions; Office of Foreign Assets Control.
International Business Corporations (IBC). *See* Foreign Business Entities; Confidentiality.
International Monetary Fund (IMF), E-1
International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, 8
International Narcotics Control Strategy Report (INCSR), 26,
International Narcotics Traffickers, 11, 147
International Organization of Securities Commissions (IOSCO), 162
International Transportation of Currency or Monetary Instruments, 144-146, 188-194, 205, H-6, H-9
bulk currency shipments, 189-194
common carrier, 146
examination procedures, 146
laws and regulations, A-2
overview, 144-145
Report of International Transportation of Currency or Monetary Instruments (CMIR), 143, 146 188, 205, A-2
Internet, 59, 64, 70, 74, 98, 207, 208-209, 214, 228, 233-234, 239-240, 246, 248-249, 300, 325-326, C-2, F-3, F-6, J-1, M-1
Internet Banking. *See also* Electronic Banking.
208, 209, 325
Internet Broker, 248
Internet Protocol (IP), 208, 234,Q-3
Internet Service Providers, 70
Intraday Accounts. See Concentration Accounts.

K

Know Your Customer (KYC). *See also* Customer Due Diligence (CDD).
161, 169, C-3, Q-3

L

Layering. *See* Money Laundering.
Lending Activities, 24, 270-272, H-14
examination procedures, 272
lending agreement with an Independent Sales Organization (ISO), 240
lending arrangement, 37, 252, F-6
overview, 270, 271
red flags, 272
request letter items, H-14
Letter of Credit, 151, 153, 183, 273-277, 279, F-6, L-1
red flags, 275, F-6
Letters to Credit Unions (LCU), B-1, Q-3
Licenses. *See* Office of Foreign Assets Control (OFAC).
Life Insurance. *See* Insurance.

M

Management Information Systems (MIS), 34, Q-3
examples of reports, 36, 40, 43
insurance product sales reports, 265, H-14
nonresident aliens (NRA) and foreign individuals reports, 295, O-3
private banking reports, 283, 284, H-15
professional service providers reports, 316-318, H-19
systems for detecting unusual activity in higher-risk accounts, 71, 88, 141, 166, 170, 173, 176, 179, 181, 186, 193, 196, 201, 202, 206, 208, 212, 221, 230, 232, 234, 238, 243, 248, 253, 254, 260, 269, 272, 276, 278, 291, 301, 305, 314, 322, 329, 333
Monetary Instruments Recordkeeping, 106-109
acceptable identification, 106
contemporaneous purchases, 107
examination procedures, 109
indirect currency purchases, 107
overview, 106-108
purchase and sale of, 12, 13, 24, 41, 72, 243-245, A-2, F-4, F-5, F-8, F-9, G-1, G-2, H-5, H-12, P-2
purchaser verification, 106
recordkeeping and retention requirements, 94, 106-108, 144-146, 188, P-2, P-3
red flags, F-1, F-2
request letter items, H-5, H-6, H-12
transportation of, 7, 12, 204-207, H-6
Money Laundering. *See also* Structuring.

criminal penalties for, 8, 13-14, A-3, G-1
defined, 12
integration, 12, 218, 229, 251
international organizations, E-1
laws and regulations, 20, 48, 99, 101, 102, 123, 127, 157, 256, 307, A-1–A-6
layering, 12, 184, 188, 218, 229, 243, 251
placement, 12, 218, 236, 243, 251, F-9
red flags, F-1–F-11
Money Laundering Control Act of 1986, 7
Money Laundering Suppression Act of 1994 (MLSA), 7, 90, Q-3
Money Laundering Threat Assessment (MLTA), 189, 325, C-2, Q-3
Money Services Businesses (MSB). *See also* Nonbank Financial Institutions (NBFI).
25, F-7
defined, 307
examination procedures, 314
FinCEN registration, A-3
foreign money service providers, 169, 209
guidance on providing banking services to, 309-313
laws and regulations, 9
minimum due diligence requirements for, 310, 312
state licensing, 311, 314
Money Transmitters, 25, 121, 129, 307, 311, 312
request letter items, H-16
Mutual Funds, 9, 120, 121, 142, 255, 307, 324, L-1

N

National Association of Securities Dealers (NASD), 257, Q-3
NACHA — The Electronic Payments Association (NACHA). *See also* Automated Clearing House (ACH) Transactions; Electronic Funds Transfers; Funds Transfers; Funds Transfers Recordkeeping.
154, 224-230, C-4, F-3, Q-3
National Security Letters (NSL). *See* Federal Bureau of Investigation (FBI); Confidentiality.
Nested Accounts. *See* Correspondent Accounts (Foreign).
Networking Arrangements. *See* Insurance; Nondeposit Investment Products (NDIP).
Nominal and Beneficial Owners,
brokered deposits, 246
business entities (domestic and foreign), 325
enhanced due diligence (EDD), 65
OFAC, 151, 157
payable through accounts (PTA), 201
politically exposed persons (PEP), 299, 300
private banking, 130, 131, 133, 135-137, 281, 282
professional service providers, 316
red flags, F-1, F-6, F-9
special measures, 139

trust and asset management services, 288
Nominee Incorporation Services (NIS). *See* Business Entities.
Nominee Shareholders, 151, 157, 326
Nonbank Financial Institutions (NBFI). *See also* Insurance; Money Services Businesses (MSB).
brokers/dealers, 9, 25
casinos, 9, 25, 132
examination procedures, 314, 315
overview, 307-313
request letter items, H-18
Noncooperative Countries and Territories (NCCT). *See* Financial Action Task Force on Money Laundering (FATF).
Nongovernmental Organizations (NGO),
charities, 25
enhanced due diligence, 321
examination procedures, 322
overview, 320-321
request letter items, H-19
Nondeposit Investment Products (NDIP). *See also* Affiliate; Contractual Agreements, Contracts; Customer Identification Program (CIP); Enhanced Due Diligence (EDD); Federal Banking Agencies.
co-branded products, 255
dual-employee arrangements, 256
examination procedures, 260, 261
in-house sales and proprietary products, 256-257
networking arrangements, 255-256
overview, 255-259
request letter items, H-13
third-party arrangements, 256
Nonresident Aliens (NRA) and Foreign Individuals, 82, M-1
examination procedures, 295-296
overview, 293-294
request letter items, H-18
tools for transaction testing, O-3
Nonsufficient Funds (NSF), 35, 71, 82, H-3

O

Office of Foreign Assets Control (OFAC), 5, 6, 43, C-1
Automated Clearing House (ACH) transactions, 151, 153, 154, 157
beneficial owners, 151, 157
blocked transactions, 149, 153, 153-158
designation of responsible individual, 150, 153, 156
examination procedures, 157-159
identifying and reviewing suspect transactions, 152
independent testing, 156, 158
internal controls, 152-156

international Automated Clearing House transactions (IAT), 154, 155
licenses, 149
OFAC compliance program, 147, 150-153
OFAC risk assessment, 6, 16, 20, 151-152
OFAC reporting, 150
overview, 147-156
prohibited transactions, 149, 153
request letter items, H-6 to H-7
sanctions, 6, 26, 147
scoping and planning, 6
screening automated clearing house (ACH) transactions, 151, 153-155, 157, 213, 224-233
separate and distinct from the Bank Secrecy Act, 11
Specially Designated Nationals or Blocked Persons (SDN), 149
training, 150, 156
updating OFAC lists, 153
Offshore Bank,
offshore banking license, 122, 127, 129
Offshore Entities. *See also* Foreign Business Entities.
279, 285, H-16
Offshore Financial Center (OFC). *See* Foreign Business Entities.
26, 324, F-7
Omnibus Accounts. *See* Concentration Accounts.
Originating Depository Financial Institution (ODFI). *See* Automated Clearing House (ACH) Transactions.
154, 225

P

Parallel Banking,
examination procedures, 176-177
overview, 175
request letter items, H-10
Payable Through Accounts (PTA), 24, 117, 139, 141, 152, 176, 183, 198, 201, H-5, H-9, J-1
beneficial owners, 123, 127, 201
examination procedures, 201-203
foreign correspondent accounts, 199, 202
OFAC risks, 151
overview, 198-200
parallel banking, 176
request letter items, H-5, H-9
special measures — information relating to certain PTAs, 139
special measures — prohibitions or conditions on PTAs, 139-141
subaccountholder, 198, 199, 202, 203, H-9
Payable Upon Proper Identification (PUPID). *See* Funds Transfers.
24, 72, 217, 219, 222, H-11, J-2

Payroll Customer,
Currency Transaction Report (CTR) exemptions, 93-96
defined, 93
Placement. *See* Money Laundering.
Point-of-Sale (POS),
networks, 250
systems, 110, 213
Politically Exposed Person (PEP),
beneficial owners, 299-300
brokered deposits, 246-247
defined, 297-299
defined — senior foreign political figure, 297-298
embassy and foreign consulate accounts, 303
examination procedures, 301-302
nondeposit investment products (NDIP), 259
nonresident aliens (NRA) and foreign individuals, 294
overview, 297-300
payable through accounts (PTA), 201
private banking, 133
proceeds of foreign corruption, 298-299
request letter items, H-16, H-18
trust and asset management services, H-16
Pouch Activities, 172, 183, 204-207, H-9, J-1
examination procedures, 206-207
overview, 204-205
red flags, F-7
request letter items, H-9
Preliminary Evaluation of the Bank's BSA/AML Compliance Program, 43
Prepaid Cards. *See* Electronic Cash.
Private Banking. *See also* Private Banking Due Diligence Program (Non-U.S. Persons); Confidentiality.
8, 17, 24, 25, 27, 29, 37, 41, 46, 51, 60, 130, 131-137, 152, 267, 279-285, 287, 294, 297, 300-301, 304, J-2, N-1, R-6
bearer shares, 282, 324-329, H-19
beneficial owners, 130, 131, 133, 135-137, 281-282
board of directors and senior management oversight, 283
common structure, N-1
customer risk assessment, 281
due diligence, 130-137, 280
examination procedures, 284-285
laws and regulations, A-4
overview, 279-283
private banker deemed a "financial institution," D-1
red flags, F-7, F-8
request letter items, H-15, H-16
risk of shell companies, 279-284

typical products and services offered, 279-280
vulnerabilities to money laundering, 280
Wolfsberg principles, C-4
Private Banking Due Diligence Program (Non-U.S. Persons). *See also* Private Banking.
ascertaining source of funds, 132
defined — private banking account, 130-131
defined — senior foreign political figure, 132, 136
due diligence program, 131
enhanced scrutiny for senior foreign political figures, 132-134
examination procedures, 135-137
identifying senior foreign political figures, 134
monitoring account activity, 132
overview, 130-134
proceeds of foreign corruption, 133, 136
risk assessment of accounts for non-U.S. persons, 132, 137
special procedures when due diligence cannot be performed, 134
Private Investment Companies (PIC). *See* Foreign Business Entities; Confidentiality.
Privately Owned ATMs. *See* Automated Teller Machines (ATM).
Products and Services. *See* Risk Assessment.
Professional Service Providers, 25
beneficial owners, 316
examination procedures, 318-319
overview, 316-317
request letter items, H-19
Prohibited Transactions. *See* Office of Foreign Assets Control (OFAC).
Purchase and Sale of Monetary Instruments. *See* Monetary Instruments Recordkeeping.

R

Receiving Depository Financial Institution (RDFI). *See* Automated Clearing House (ACH) Transactions.
Record Retention Requirements, P-1 to P-6
Currency Transaction Reports (CTR), 86, P-5
Customer Identification Program (CIP), 56-57, P-5, P-6
Office of Foreign Assets Control (OFAC), 157
request letter items, H-6
Suspicious Activity Reports (SAR), 79, P-5
Recordkeeping. *See* Correspondent Accounts (Foreign), Credit Cards, Customer Identification Program (CIP), Foreign Correspondent Account Recordkeeping and Due Diligence; Funds Transfers Recordkeeping, Monetary Instruments Recordkeeping; Record Retention Requirements.
Red Flags, F-1–F-11
potentially suspicious activity that may indicate money laundering:
activity inconsistent with the customer's business, F-3
automated clearing house (ACH) transactions, F-3
changes in bank-to-bank transactions, F-4
cross-border financial institution transactions, F-4, F-5

customers who provide insufficient or suspicious information, F-1
efforts to avoid reporting or recordkeeping requirements, F-2
electronic banking, 208
embassy and foreign consulate accounts, F-7
employees, F-8
funds transfers, F-2, F-3
insurance, F-6, F-7
lending activity, F-4
other suspicious customer activity, F-8, F-9
politically exposed persons (PEP), 298
privately owned automated teller machines (ATM), F-6
shell company activity, F-7
trade finance, F-5
potentially suspicious activity that may indicate terrorist financing:
activity inconsistent with the customer's business, F-10
funds transfers, F-10
other transactions that appear unusual or suspicious, F-10
Regulatory Alerts (RA), B-1
Reliance. *See* Customer Identification Program (CIP).
Remotely Created Checks (RCC). *See* Third-Party Payment Processors.
Remote Deposit Capture (RDC), 192, 204, 208, 209, 212, H-11. *See also* Contractual Agreements, Contracts.
Report of Examination (ROE), 32, 44, 45, 50, 211, A-1, Q-4, R-2, R-3, R-4
include OFAC findings, 159
preparing comments for, 50-51
Report of Foreign Bank and Financial Accounts (FBAR). *See* Foreign Bank and Financial Accounts Reporting.
Report of International Transportation of Currency or Monetary Instruments (CMIR). *See* International Transportation of Currency or Monetary Instruments.
Request Letter Items, 15, 17, 29, H-1 to H-20
automated clearing house (ACH) transactions, H-11
bearer shares, H-19
brokered deposits, H-12
BSA/AML compliance program, H-1
bulk currency shipments, H-8
business entities (domestic and foreign), H-19
cash-intensive businesses, H-20
concentration accounts, H-14
correspondent accounts (domestic), H-8
correspondent accounts (foreign), H-8
currency-shipment activity, H-6
currency transaction reporting, H-4
currency transaction reporting exemptions, H-4
Customer Identification Program (CIP), H-2
electronic banking, H-10
electronic cash, H-11

embassy and foreign consulate accounts, H-18
foreign branches and offices of U.S. banks, H-9
foreign correspondent account recordkeeping and due diligence, H-5, H-6
funds transfers, H-11
funds transfer recordkeeping, H-5
independent testing, H-1
information sharing, H-4, H-5
insurance, H-13
lending activities, H-14
nonbank financial institutions (NBFI), H-18
nondeposit investment products (NDIP), H-13
nonresident aliens (NRA) and foreign individuals, H-18
Office of Foreign Assets Control (OFAC), H-6, H-7
other BSA reporting and recordkeeping requirements, H-6
parallel banking, H-10
payable through accounts (PTA), H-9
politically exposed persons (PEP), H-18
pouch activities, H-9
private banking, H-15
privately owned automated teller machines (ATM), H-13
professional service providers, H-19
purchase and sale of monetary instruments, H-5, H-12
training, H-2
risk assessment, 29, H-2
suspicious activity reporting, H-3, H-4
third-party payment processors, H-12
trade finance activities, H-15
trust and asset management services, H-16
U.S. dollar drafts, H-9
Respondent Bank. *See also* Correspondent Bank.
179, 180, 181, 326, 327, F-7
defined, 179, 181
Risk Assessment, 22
aggregate risk profile, 30
consolidated BSA/AML risk assessment, 28
customers and entities, 24, 25
developing a BSA/AML compliance program based upon, 28, 39, 32, 33, 39, I-1
evaluating the bank's BSA/AML risk assessment, 23-28
examination procedures, 31
examiner development of, 29-30
foreign financial institutions, 121
geographic locations, 25-27
money services business (MSB), 310, 314
nonbank financial institution (NBFI) risk assessment factors, 308-309
OFAC risk assessment, 151-152
overview, 22-30

private banking accounts, 117
products and services, 24
request letter items, H-1, H-2, H-7, H-8, H-12, H-13, H-14, H-15, H-17, H-19, H-20
review of, 15, 17
risk categories — analysis of, 27
risk categories — identification of, 23-27
updating the risk assessment, 28-29
Risk Categories. *See* Risk Assessment.

S

Safe Harbor. *See* Currency Transaction Report (CTR) Exemptions; Information Sharing; Suspicious Activity Reporting.
Sanctions, 6
Office of Foreign Assets Control (OFAC), 6,7,11,16, 26, 43, 147, 148, 149, 150, 151, 154, 155, 156, 157, 158, 159, 216, 230, 231, 246, 276
Scoping and Planning. *See* Examination Scope.
Screening Automated Clearing House (ACH) Transactions. *See* Office of Foreign Assets Control (OFAC).
Secretary of the Treasury, 9, 20, 26, 119, 120, 122, 127, 129, 138, 139, 140, 147, A-4, D-2, H-6
Section 311 of the USA PATRIOT Act. *See* Special Measures.
Section 314(a) of the USA PATRIOT Act. *See* Information Sharing; Confidentiality.
Section 314(b) of the USA PATRIOT Act. *See* Information Sharing; Confidentiality.
Seizure. *See* Asset Seizure.
Senior Foreign Political Figures. *See* Private Banking Due Diligence Program (Non-U.S. Persons); Politically Exposed Person (PEP).
Service Providers. *See* Automated Clearing House (ACH) Transactions; Management Information Systems (MIS); Money Services Businesses (MSB); Nominal and Beneficial Owners; Professional Service Providers; Third-Party Service Provider (TPSP).
Shell Bank. *See* Foreign Correspondent Account Recordkeeping and Due Diligence.
Shell Company, 184, 247, 275, 279, 280, 281, 282, 283, 284, 323, 324, 325, 326, 327, L-1
defined, 323
red flags, F-1, F-7
Social Security Number (SSN). *See also* Taxpayer Identfication Number. 47, 100-101, F-1, O-1, O-2, O-3, P-3
Society for Worldwide Interbank Financial Telecommunication (SWIFT). *See* Funds Transfers.
Special Due Diligence Program. *See* Foreign Correspondent Account Recordkeeping and Due Diligence.
Special Measures, 8, 10, 14, 22, 26, 122, 127, 129
examination procedures, 141
foreign correspondent account due diligence, 122-124
guidance, 140

overview, 138-140
types of, 138-140
Special Use Accounts. *See* Concentration Accounts.
Specially Designated Nationals or Blocked Persons (SDN). *See* Office of Foreign Assets Control (OFAC).
Stored Value/Prepaid Cards, 206, 213, 234, 235, 236, 238, 239, 243, 307, 309
red flags, F-8
Structuring. *See also* Money Laundering.
12, 14, 72, 73, 195, 196, 316, A-3, G-1, G-2, L-1, L-2
defined, G-1
laws and regulations, A-3
Subaccountholder. *See* Payable Through Accounts (PTA).
Subpoena, 19, 70, 79, 81, 82, 84, 119-120, 128, 248
laws and regulations, A-4, A-5
request letter items, H-4, H-5, H-12 to H-19
Subsidiary, 90, 91, 95, 110, 164, 165, 167, 168, 257, 260, 262, 263, 265, A-5, P-4
Supervisory Response. *See* Developing Conclusions.
Suspense Accounts. *See* Concentration Accounts.
Suspicious Activity Reporting. *See also* Confidentiality.
7, 8, 10, 17, 18, 19, 20, 28, 33, 34, 35, 36, 37, 39, 45, 46, 59, 61, 63, 94, 99, 102, 103, 104, 105, 124, 125, 131, 134, 145, 155, 166, 167, 205, 229, 248, 276, 277, 282, 295, 298, 311, 312, 330, 332, A-4, A-5, A-6, C-2, G-1, K-1, L-2, R-3, R-5, R-6
account monitoring — surveillance (automated), 72-73, 77, H-3
account monitoring — transaction (manual), 71-72, H-3
avoid comparing numbers of Suspicious Activity Reports (SAR) filed, 30
BSA/AML compliance program structure and management, 161, 164, 165
continuing activity — SAR filing on, 76
examination procedures, 81-85
identifying underlying crime, 75
insurance companies, 262-264, A-2
law enforcement inquiries and requests, 69-70
laws and regulations, A-4, A-5, A-6
managing alerts, 74-75
notifying board of directors of SAR filings, 79
overview, 67-80
proceeds of foreign corruption, 130, 133
prohibition of SAR disclosure, 79-80
record retention, 79, P-5
red flags, F-1 to F-11
request letter items, H-1, H-3, H-4
safe harbor, 68
SAR completion and filing, 77-80
SAR decision-making process, 75, 76
SAR monitoring components, S-1
SAR quality, 78, L-1

sharing SARs, 80
systems to identify, research and report suspicious activity, 68-69
timing of a SAR filing, 77-78
tools for transaction testing, O-1, O-2, O-3
Sweep Accounts. *See* Concentration Accounts.

T

Tax Withholding. *See also* W-8 Status.
294
Taxpayer Identification Number (TIN), 54, 59, 60, 88, 112, 114, 234, H-2, H-18, O-1, O-2, O-3, P-2, P-4, P-5
Terrorist Financing, 5, 9, 10, 11, 12, 13, 14, 24, 26, 32, 36, 38, 42, 63, 64, 66, 67, 74, 82, 138, 169, 170, 171, 173, 176, 181, 186, 189, 190, 193, 194, 196, 199, 201, 206, 208, 212, 221, 232, 236, 238, 242, 244, 246, 248, 253, 258, 260, 265, 269, 270, 272, 274, 275, 278, 280, 281, 284, 291, 295, 301, 305, 309, 310, 312, 314, 318, 320, 322, 323, 326, 329, 331, 332, 333, C-2, C-3, E-1, F-1, F-9, L-1, R-3, R-4, R-5
Third Party(ies), 98, 153, 178, 195, 202, 208, 234, 235-237, 256, 264, 270, 277, 282, 287, 316, 328, F-4, F-6, F-10, H-2, H-3
bearer shares, 282
correspondent accounts, 184, 186
Customer Identification Program (CIP), 58-61
information sharing, 98
lending, 270
nondeposit investment products (NDIP), 256
OFAC screening, 153
red flags, F-4, F-6, F-10
request letter items, H-2, H-3
Third-Party Payment Processors, 24
examination procedures, 242
overview, 239-241
remotely created checks (RCC), 239
request letter items, H-12
verification, 240
Third-Party Service Provider (TPSP). *See also* Automated Clearing House (ACH) Transactions.
227, 230
examination procedures, 232-233
screening ACH transactions (OFAC), 154, 230-231, 246
Section 314(a) information requests, 98
red flags, F-3
use of, 58
Trade Finance, 24, 151, 270, H-15
accepting bank, 274
advising bank, 274
applicant, 273

beneficiary, 273
confirming bank, 273
discounting bank, 274
documentary requirements, 275-277
examination procedures, 278
issuing bank, 151, 273, 274, 275, 277
lending, 270-271
negotiation, 274
nominated bank, 274
overview, 273-277
red flags, F-5, F-6
reimbursing bank, 274
request letter items, H-15
Society for Worldwide Interbank Financial Telecommunication (SWIFT), 276
Treasury Department. *See* U.S. Department of the Treasury.
Training, 28, 33, 35, 37, 45
documentation, 37
examination procedures, 42
OFAC, 150
request letter items, H-2, H-6, H-15, H-17, R-2–R-5
Travel Rule. *See* Funds Transfers Recordkeeping.
Trust and Asset Management, 24, 286-290, J-2
agency accounts, 286, 288, 291
beneficial owners, 299
business entities, 323-325, 329
court-supervised accounts, 286, 287, 289
corporate trusts, 286
examination procedures, 291-292
international business corporations (IBC), 25, 279, 281, 284, 324
nominee incorporation services (NIS), 325, F-1
overview, 286-290
personal trusts, 286
private banking, 287
professional service providers, 316, H-19
Private Investment Companies (PIC), 25, 257, 258, 279, 281, 282, 284, 288, 292, 299, 324, 325, H-16
red flags, 299, F-1
request list items, H-16–H-17
transaction testing, O-2

U

United Nations, 11, 147
Updating OFAC Lists. *See* Office of Foreign Assets Control (OFAC).
U.S. Attorney General, 20, 119, 120, A-4, H-6
correspondence from, 20, H-6
subpoenas, 19, 119

U.S.-Based Examinations. *See* Foreign Branches and Offices.
U.S. Bureau of Customs and Border Protection, 144
U.S. Department of the Treasury. *See also* Secretary of the Treasury.
5, 7-9, 57-58, 90, 106, 110, 119, 147, 165, 320, 340, A-1–A-6, P-1, P-5, R-5, R-6
request letter items, H-1
U.S. Dollar Drafts, 24, 117, J-1
overview, 195
examination procedures, 196-197
request letter items, H-9

V

Verification. *See also* Customer Identification Program (CIP).
54-56, 59-61, 294, 321, 328
additional, 55-58
certifications, 119. *See also* Foreign Correspondent Account Recordkeeping and Due Diligence.
documentary, 54, 55, 294, H-2
examination procedures, 59-62
lack of, 56
nondeposit investment products (NDIP), 258
nondocumentary, 54, 55, 60, 294, H-2, P-5
OFAC license, validity of, 149-150
purchaser, 106. *See also* Monetary Instruments Recordkeeping.
privately owned automated teller machine (ATM), 252
request letter items, H-2
source of funds, 132
third-party payment processors, 239-242
Violations, 7, 13-14, 20, 35, 36, 44, 49, 50, 61, 67, 75, 76, 147, 199, 231, R-5, R-6
isolated or technical, 46-47
OFAC violations, 146-156
systemic or recurring, 44-46

W

W-8 Status. *See also* Tax Withholding.
25, 294, 296
request letter items, H-18
Web Currency and Banking Retrieval System (Web CBRS), 15, 17, 29