Bank Secrecy Act / Anti-Money Laundering Examination Manual

Expanded Examination Overview and Procedures

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

2007

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

EXPANDED EXAMINATION OVERVIEW AND PROCEDURES FOR AN ENTERPRISE-WIDE COMPLIANCE PROGRAM AND OTHER STRUCTURES

Enterprise-Wide BSA/AML Compliance Program — Overview

Objective. *Assess the organization's enterprise-wide program for BSA/AML compliance through the holding company or lead financial institution.*[138]

Similar to the approach to consolidated credit, market, and operational risk, effective control of BSA/AML risk may call for coordinated risk management. An enterprise-wide BSA/AML compliance program coordinates the specific regulatory requirements throughout an organization inside a larger risk management framework. Such frameworks seek a consolidated understanding of the organization's risk exposure to money laundering and terrorist financing across all activities, business lines, or legal entities. For example, the holding company or lead financial institution may have a centralized function to evaluate BSA/AML risk; this may include the ability to understand world-wide exposure to a given customer, particularly those considered high-risk or suspicious, consistent with applicable laws.[139]

Many organizations, typically those that are larger or more complex and that may include international operations, implement an enterprise-wide BSA/AML compliance program that manages risks in an integrated fashion across affiliates, business lines, and risk types (e.g., reputation, compliance, or transaction). Aggregating risks on an enterprise-wide basis for larger or more complex organizations may enable an organization to better identify risks and risk exposures within or 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. Such programs manage risk at both operational and strategic levels.

While there are currently no regulatory requirements for holding companies or lead financial institutions to adopt an enterprise-wide BSA/AML compliance program, many

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

[139] For additional guidance, refer to the expanded overview section, "Foreign Branches and Offices of U.S. Banks," page 156, and the Basel Committee on Bank Supervision's guidance *Consolidated Know Your Customer (KYC) Risk Management*, located at www.bis.org.

organizations view this as an effective tool in managing the BSA/AML risks associated with failure to comply with BSA laws and regulations, or the corresponding laws in foreign jurisdictions in which they operate. A sound practice for complex organizations is to establish corporate standards for BSA/AML compliance that reflect the expectations of the organization's board of directors. Senior management should ensure that these standards are implemented across the organization through effective programs tailored to the activities, business lines, or legal entities. This allows the holding company or lead financial institution to demonstrate to its board of directors that it has effective BSA/AML compliance programs in place across the consolidated organization. Each program should reflect the organization's business structure and be tailored to its size, complexity, and legal requirements that may vary due to the specific business line or host country jurisdiction.[140]

The enterprise-wide program should include a central point where BSA/AML risks throughout the organization are aggregated. Structurally, the point of consolidation could be established at either the level of the holding company or the lead financial institution. Therefore, organizations that implement an enterprise-wide program should assess risk both individually within business lines and on a consolidated basis across all activities and legal entities. Enterprise-wide systems that operate on a global basis need to consider the various jurisdictions in which they operate as well as the AML laws and requirements they are subject to, and then incorporate these into their overall compliance program. Internal audit should assess the level of compliance with the enterprise-wide 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 consolidate all its funds transfer functions in a national bank subsidiary, while centralizing its audit function at the holding company. This arrangement may present a challenge to the examiner reviewing a legal entity within the organization, as it may be difficult to evaluate that entity's BSA/AML compliance.

Subsidiaries, Affiliates, and Business Lines

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

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

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

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

Holding Company or Lead Financial Institution

Holding companies or lead financial institutions 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 holding company or lead financial institution enterprise-wide 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, organizations that centrally manage an enterprise-wide BSA/AML compliance program should among other things provide appropriate structure; advise the business lines, subsidiaries, and foreign branches on the development of appropriate guidelines; and set risk limits consistent with their domestic and international activities. For additional guidance, refer to the expanded overview section, "Foreign Branches and Offices of U.S. Banks," page 156.

Organizations that implement an enterprise-wide BSA/AML compliance program should assess risk on a consolidated basis across all activities, business lines, and legal entities. Once the organization appropriately assesses its risk on an enterprise-wide basis, this process should be ongoing. Business line subsidiaries and foreign branches should provide periodic updates to the risk assessment process to the central point within the holding company or lead financial institution. The risk assessment should serve as the basis for the development of risk-based policies, procedures, and processes within the activities, business lines, and legal entities. Subsidiary entities should advise the holding company or lead financial institution on the development of risk-based policies, procedures, and processes. After the policies, procedures, and processes are complete, they should be approved by the holding company or lead financial institution. Increasingly, organizations use software or programming solutions to assist in the

implementation of the BSA/AML compliance program; these solutions typically include, but are not limited to, monitoring, identifying, and reporting suspicious activity.

Suspicious Activity Reporting

A bank holding company (BHC) or any non-bank subsidiary thereof, or a foreign bank that is subject to the BHC Act or any non-bank subsidiary of such a foreign bank operating in the United States, is required to file a Suspicious Activity Report (SAR) (12 CFR 225.4(f)).[141] Certain savings and loan holding companies, and their non-depository 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.

Interagency guidance clarifies that banking organizations may share SARs with head offices and controlling companies, whether located in the United States or abroad.[142] The guidance does not address whether a banking organization may share a SAR with an affiliate other than a controlling company or head office. Therefore, banking organizations should not share SARs with such affiliates. However, in order to manage risks across the organization, banks may disclose to entities within their organization the underlying information supporting a SAR filing. Refer to the core overview section, "Suspicious Activity Reporting," page 60, for additional guidance.

[141] A BHC's non-bank subsidiaries operating only outside the United States are not required to file SARs.

[142] *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

Enterprise-Wide BSA/AML Compliance Program

Objective. *Assess the organization's enterprise-wide program for BSA/AML compliance through the holding company or lead financial institution.*[143]

1. Confirm the existence and review the scope of any enterprise-wide 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 holding company or lead financial institution. Determine the extent to which the enterprise-wide BSA/AML compliance program affects the organization being examined, considering the following:

   - The existence of enterprise-wide 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, and recordkeeping activities.

   - The centralization 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 holding company or lead financial institution (or other corporate-level unit, such as audit or compliance) performs regular independent testing of BSA/AML activities.

   - Whether a corporate-level unit sponsors BSA/AML training.

2. Review audits for BSA/AML compliance throughout the organization and identify program deficiencies.

3. Review board minutes to determine the adequacy of management information systems (MIS) and of reports provided to the board of directors. Ensure that the board of directors of the holding company has received appropriate notification of Suspicious Activity Reports (SARs) filed by the holding company.

4. Review policies, procedures, processes, and risk assessments formulated and implemented by the holding company's or lead financial institution's board of

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

directors, a board committee thereof, or senior management. As part of this review, assess effectiveness of the holding company's or lead financial institution's ability to perform the following responsibilities:

- Manage the enterprise-wide BSA/AML compliance program and provide adequate oversight and structure.
- Promptly identify and effectively measure, monitor, and control key risks throughout the consolidated organization.
- Develop an adequate enterprise-wide 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 enterprise-wide BSA/AML compliance program, as established by the holding company or lead financial institution.
- Identify enterprise-wide program weaknesses and implement necessary and timely corrective action, at both the holding company and subsidiary levels.

5. To ensure compliance with regulatory requirements,[144] review the holding company's or the lead financial institution's procedures for monitoring and filing SARs. For additional guidance, refer to the core overview and examination procedures, "Suspicious Activity Reporting," pages 60 and 72, 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.
   - Person (or persons) responsible for ongoing supervision of the organization and subsidiary banks, as appropriate.

[144] Bank holding companies (BHCs) or any non-bank subsidiary thereof, or a foreign bank that is subject to the BHC Act or any non-bank subsidiary of such a foreign bank operating in the United States, are required to file SARs (12 CFR 225.4(f)). A BHC's non-bank subsidiaries operating only outside the United States are not required to file SARs. Certain savings and loan holding companies, and their non-depository 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," page 60, for additional information.

- Corporate management.

7. On the basis of examination procedures completed, form a conclusion about the adequacy of policies, procedures, and processes associated with an enterprise-wide BSA/AML compliance program.

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[145] 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.[146] 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.[147] 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.[148]

Risk Factors

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

The examiner should understand the foreign jurisdiction's various AML requirements. Secrecy laws or their equivalent may affect the ability of the foreign branch or office to share information with the U.S. parent bank, or the ability of the examiner to examine on-site. While banking organizations with overseas branches or subsidiaries may find it necessary to tailor monitoring approaches as a result of local privacy laws, the

[145] Foreign offices include affiliates and subsidiaries.

[146] Edge and agreement corporations may be used to hold foreign investments (e.g., foreign portfolio investments, joint ventures, or subsidiaries).

[147] 71 *Federal Register* 13935.

[148] 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.

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

- The U.S. bank's head office and management at the foreign operation should understand the effectiveness and quality of bank supervision in the host country and understand the legal and regulatory requirements of the host country. The U.S. bank's head office should be aware of and understand any concerns that the host country supervisors may have with respect to the foreign branch or office.

- The U.S. bank's head office should understand the foreign branches' or offices' risk profile (e.g., products, services, customers, and geographic locations).

- The U.S. bank's head office and management should have access to sufficient information in order to periodically monitor the activity of their foreign branches and offices, including the offices' and branches' level of compliance with head office policies, procedures, and processes. Some of this may be achieved through management information systems reports.

- The U.S. bank's head office should develop a system for testing and verifying the integrity and effectiveness of internal controls at the foreign branches or offices by conducting in-country audits. Senior management at the head office should obtain and review copies, written in English, of audit reports and any other reports related to AML and internal control evaluations.

- The U.S. bank's head office should establish robust information-sharing practices between branches and offices, particularly regarding high-risk account relationships.

- The U.S. bank's head office should be able to provide examiners with any information deemed necessary to assess compliance with U.S. banking laws.

Foreign branch and office compliance and audit structures can vary substantially based on the scope of operations (e.g., geographic locations) and the type of products, services, and customers. Foreign branches and offices with multiple locations within a geographic region (e.g., Europe, Asia, and South America) are frequently overseen by regional

compliance and audit staff. Regardless of the size or scope of operations, the compliance and audit staff and audit programs should be sufficient to oversee the AML risks.

Scoping AML Examinations

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

- The risk profile of the foreign branch or office and whether the profile is stable or changing as a result of a reorganization, the introduction of new products or services, or other factors, including the risk profile of the jurisdiction itself.
- The effectiveness and quality of bank supervision in the host country.
- Existence of 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 low-risk situations when information is restricted, examiners may conduct U.S.-based examinations (see discussion below). In high-risk situations when adequate examinations (on-site or otherwise) cannot be effected, the agency may require the head office to take action to address the situation, which may include closing the foreign office.

U.S.-Based Examinations

U.S.-based, or off-site, examinations generally require greater confidence in the AML program at the foreign branch or office, as well as the ability to access sufficient records. Such off-site examinations should include discussions with senior bank management at the head and foreign 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[149] 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 management information systems (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 high-risk transactions or located in high-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, an enterprise-wide assessment of suspicious activities.

4. Review the bank's tiering or organizational structure report, which should include a list of all legal entities and the countries in which they are registered. Determine the locations of foreign branches and offices, including the foreign regulatory environment and the degree of access by U.S. regulators for on-site examinations and customer records.

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

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

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

8. Determine the involvement of the U.S. bank's head office in managing and monitoring foreign branches and offices. Conduct a preliminary evaluation of the

[149] Foreign offices include affiliates and subsidiaries.

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," page 146, 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 high-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.[150]

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.

[150] 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 management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors parallel banking relationships, particularly those that pose a high-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," page 146, 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 high-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 high 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 high risk may still require enhanced due diligence, 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[151] outlining each party's responsibilities. The service agreement may include the following:

- Products and services provided.
- Responsibility for recordkeeping (e.g., Currency Transaction Reports (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, management information systems, account monitoring, and reporting suspicious activities. Furthermore, while a domestic correspondent account may not be considered high risk, transactions through the account, which may be conducted on behalf of the respondent's customer, may be high risk. 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.

[151] 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 137 and 146, 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 management information systems (MIS) and internal risk rating factors, determine whether the bank has identified any domestic correspondent banking activities as high 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," page 146, for guidance.

Transaction Testing

5. On the basis of the bank's review of respondent accounts[152] with unusual or high-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.

[152] A respondent bank is any bank for which another bank establishes, maintains, administers, or manages a correspondent account relationship.

- Currency Transaction Reports (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[153] 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 New York Clearing House Association, L.L.C. (NYCH) and The Wolfsberg Group have published suggested industry standards and guidance for banks that provide foreign correspondent banking services.[154] Also, additional information relating to risk assessments and due diligence is contained in the core overview section, "Foreign Correspondent Account Recordkeeping and Due Diligence," page 106. The U.S. bank's policies, procedures, and processes should:

[153] Refer to the expanded overview section, "Payable Through Accounts," page 178, for additional information.

[154] 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/corresp-banking.html.

- 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 high-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 high 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 management information systems (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," page 146, 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 high-risk foreign correspondent financial institution account relationships. The high-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.

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 management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors high-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 (PTAs), 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 high in PTA accounts that are not adequately controlled.

Generally, a foreign financial institution requests a PTA for its customers that want to conduct banking transactions in the United States through the foreign financial institution's account at a U.S. bank. The foreign financial institution provides its customers, commonly referred to as "sub-accountholders," with checks that allow them to draw funds from the foreign financial institution's account at the U.S. bank.[155] The sub-accountholders, which may number several hundred or in the thousands for one PTA, all become signatories on the foreign financial institution's account at the U.S. bank. While payable through customers are able to write checks and make deposits at a bank in the United States like any other accountholder, they might not be directly subject to the bank's account opening requirements in the United States.

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

Risk Factors

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

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

expended to obtain or confirm information about the individual and business sub-accountholders that use the PTAs.

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

Risk Mitigation

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

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

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

- Roles and responsibilities of each party.
- Limits or restrictions on transaction types and amounts (e.g., currency deposits, funds transfers, check cashing).
- Restrictions on types of sub-accountholders (e.g., casas de cambio, finance companies, funds remitters, or other non-bank financial institutions).
- Prohibitions or restrictions on multi-tier sub-accountholders.[156]
- Access to the foreign financial institution's internal documents and audits that pertain to its PTA activity.

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

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

- 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 (PTAs), 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 enhanced due diligence 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).

   - Sub-accounts are not opened before the U.S. bank has reviewed and approved the customer information.

   - Master or sub-accounts can be closed if the information provided to the bank has been materially inaccurate or incomplete.

   - The bank can identify all signers on each sub-account.

2. From a review of management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors PTA accounts.

3. Determine whether the bank's system for monitoring PTA accounts 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 sub-accounts within each PTA.
   - The volume and dollar amount of monthly transactions for each sub-account.

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 sub-account 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," page 146, 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 sub-account 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 sub-accounts from being opened by casas de cambio, finance companies, funds remitters, or other non-bank financial institutions.
   - Prohibit multi-tier sub-accountholders.
   - Provide for proper controls over currency deposits and withdrawals by sub-accountholders and ensure that Currency Transaction Reports (CTRs) have been appropriately filed.
   - Provide for dollar limits on each sub-accountholder'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 sub-accountholders (e.g., directly or through a trusted third party).
- Require the foreign financial institution to monitor sub-account 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 sub-accountholder for credit to the customer's sub-account.

9. From the sample selected, review each sub-accountholder's identifying information and related transactions for a period of time as determined by the examiner. Evaluate PTA sub-accountholders' transactions. Determine whether the transactions are consistent with expected transactions or warrant further research. (The sample should include sub-accountholders 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,[157] to transport currency, monetary instruments, and other documents from outside the United States to a bank in the United States.[158] Pouches can be sent by another bank or individuals. Pouch services are commonly offered in conjunction with foreign correspondent banking services. Pouches can contain loan payments, transactions for demand deposit accounts, or other types of transactions.

Risk Factors

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

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

[157] 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.

[158] For additional guidance, refer to core overview section, "International Transportation of Currency or Monetary Instruments Reporting," page 134.

Risk Mitigation

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

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

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

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 management information systems (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," page 146, 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,[159] bearer securities, stored value cards, gems, art, illegal substances or contraband, or other items that should not ordinarily appear in a bank's pouch.

[159] Refer to the core examination procedures, "International Transportation of Currency or Monetary Instruments Reporting," page 136, 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, 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; on-line account opening; Internet banking transactions; and telephone banking. For example, credit cards, deposit accounts, mortgage loans, and funds transfers can all be initiated on-line, without face-to-face contact. Management needs to recognize this as a potentially high-risk area and develop adequate policies, procedures, and processes for customer identification and monitoring for specific areas of banking. Refer to the core examination procedures, "Customer Identification Program" (CIP), page 52, for further guidance. Additional information on e-banking is available in the FFIEC *Information Technology Examination Handbook.*[160]

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 management information systems for detecting unusual activity in high-risk accounts include ATM activity reports, funds transfer reports, new account activity reports, change of Internet address reports, Internet Protocol (IP) address reports, and reports to identify related or

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

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 on-line and should establish policies for when a customer should be required to open accounts on a face-to-face basis.[161] 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 an emerging technology that has made processing checks and monetary instruments (e.g., traveler's checks or money orders) more efficient. In broad terms, RDC provides a means of depositing checks into a bank account by scanning the checks and then transmitting the scanned or digitized image to a financial institution. This eliminates the need for face-to-face contact that results from in-person deposits, and reduces the cost and volume of paper associated with physically mailing or depositing checks or monetary instruments. Because the hardware needed to facilitate RDC transactions can be expensive, customers using the service are primarily business entities, although some banks also offer remote deposit services to their foreign correspondents.

Risk Factors

RDC may expose banks to various risks, including money laundering, fraud, and compromised transmission of financial data. Inadequate controls could result in the transmission of fraudulent monetary instruments, exposing the bank to financial and reputational risks. Because RDC equipment is located outside of bank facilities, data and hardware security issues may increase.

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:

- Creating RDC customer parameters, which may include a list of acceptable industries approved for RDC services, standardizing underwriting criteria (e.g., credit history, financial statements, ownership structure of business, types of business customer), and setting maximums for large dollar items.

[161] For additional information, refer to *Authentication in an Internet Banking Environment* issued by the FFIEC, October 13, 2005.

- Obtaining expected account activity from the RDC customer, such as the anticipated RDC number volume, dollar volume, and type (e.g., payroll checks, third-party checks, traveler's checks).

- In contracts, requiring RDC customers to retain, protect, and ultimately destroy original documents. This may also include requirements that the RDC customer provide original documents to the bank when needed to facilitate investigations related to unusual transactions or poor quality transmissions, or to resolve disputes. Additional monitoring or review when significant changes occur in the type or volume of transactions, or when significant changes occur in the underwriting criteria that the bank relied on when establishing RDC services.

- Ensuring that RDC customers properly secure equipment and prevent inappropriate use, including establishing effective equipment security controls (e.g., passwords, dual control access).

- Using improved aggregation and monitoring capabilities as facilitated by the digitized data.

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 management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors high-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," page 146, 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 Customer Identification Program (CIP) 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 non-bank businesses that create, process, and distribute payments. The domestic and international expansion of the banking industry and non-bank financial services has increased the importance of electronic funds transfers, including funds transfers made through the wholesale payment systems. Additional information on the types of wholesale payment systems is available in the FFIEC *Information Technology Examination Handbook*.[162]

Funds Transfer Services

The vast majority of the value of U.S. dollar payments, or transfers, in the United States are 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 include automated clearing houses (ACHs), automated teller machines (ATMs), point-of-sale (POS) systems, telephone bill paying, home banking systems, debit cards, and stored value cards. Most of these retail transactions are initiated by customers rather than by banks or corporate users. These individual transactions may then be combined into larger wholesale transfers, which are the focus of this section.

The two primary domestic wholesale payment systems for interbank funds transfers are the Fedwire Funds Service (Fedwire®)[163] and the Clearing House Interbank Payments System (CHIPS).[164] The bulk of the dollar value of these payments is originated electronically to make large value, time-critical payments, such as the settlement of interbank purchases and sales of federal funds, settlement of foreign exchange transactions, disbursement or repayment of loans; settlement of real estate transactions or other financial market transactions; and purchasing, selling, or financing securities transactions. Fedwire and CHIPS participants facilitate these transactions on their behalf

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

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

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

and on behalf of their customers, including non-bank 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 (fax), 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.[165] 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.

[165] 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 off-shore 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 the following currencies: Australian dollar, Canadian dollar, Danish krone, euro, Hong Kong dollar, Japanese yen, New Zealand dollar, Norwegian krone, Singapore dollar, South African rand, South Korean won, Swedish krona, Swiss franc, UK pound sterling, and U.S. dollar, and is expected to add more currencies over time.

SWIFT

The SWIFT network is a messaging infrastructure,[166] not a payments system, that 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 foreign currencies occur 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.

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

[166] The Wolfsberg Group and The Clearing House Association LLC have issued a statement endorsing message standards to enhance the transparency of international funds transfers to promote the effectiveness of global AML and anti-terrorist financing programs. Refer to *Wolfsberg, Clearing House Statement on Payment Message Standards,* April 2007.

business.[167] 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.

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.

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.

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

[167] 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.

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

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

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

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 management information systems (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 in relation to the bank's size, its location, and the nature of its customer 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 suspicious activities, and for reporting of 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.
   - 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 high risk.
   - Frequent currency deposits and subsequent transfers, particularly to a larger institution or out of the country.

6. 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).

7. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," page 146, for guidance.

Transaction Testing

8. 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 high-risk funds transfer activities, which may include the following:

   - Funds transfers purchased with currency.
   - Transactions in which the bank is acting as an intermediary.
   - 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 high risk.
   - PUPID transactions.

9. 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. Identify any suspicious or unusual 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 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) transactions and management's ability to implement effective monitoring and reporting systems.*

The use of the ACH is growing rapidly due to the increased volume of electronic check conversion[168] and one-time ACH debits, reflecting the lower cost of ACH processing relative to check processing.[169] 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. The Federal Reserve Banks' FedACH system[170] is almost exclusively used for domestic payments, but can accommodate cross-border payments to Canada, Mexico, and some countries in Europe.

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.[171]

ACH Payment Systems

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

In general, an ACH transaction is a batch-processed, value-dated, electronic funds transfer between an originating and a receiving bank. An ACH credit transaction is

[168] 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.

[169] See www.nacha.org.

[170] The Federal Reserve Banks operate FedACH, a central clearing facility for transmitting and receiving ACH payments.

[171] See OCC Bulletin 2006-39 (September 1, 2006) at www.occ.gov/ftp/bulletin/2006-39.pdf.

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 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.

Third-Party Service Providers

A third-party service provider (TPSP) is an entity other than an Originator, ODFI, or RDFI that performs any functions on behalf of the Originator, the ODFI, or the RDFI with respect to the processing of ACH entries.[172] The National Automated Clearing House Association – The Electronic Payments Association (NACHA) Operating Rules define TPSPs and relevant subsets of TPSPs that include "Third-Party Senders" and "Sending Points."[173] 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

[172] 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 the expanded overview section, "Third-Party Payment Processors," page 209, for additional guidance.

[173] 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.

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, where 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.[174] 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.
- Because ACH processing is highly efficient and more automated than individual funds transfers, there are fewer opportunities for human review of individual transactions.

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 customer due diligence (CDD) information 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

[174] 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.

regulations. Banks may need to consider controls to restrict or refuse ACH services to potential originators 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 may need to more closely scrutinize transaction details for international ACH. The ODFI, if frequently involved in international ACH, may develop a separate process for reviewing international ACH transactions that minimizes disruption to general ACH processing, reconcilement, and settlement.

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," page 137, for additional guidance.) OFAC has clarified the application of its rules for domestic and cross-border ACH transactions and is working with industry to provide more detailed guidance on cross-border ACH.[175]

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 policies.

If an ODFI receives 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 mitigating 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.

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

With respect to OFAC screening, similar but somewhat more stringent OFAC obligations hold for cross-border ACH transactions. In the case of inbound cross-border ACH transactions, an RDFI is responsible for compliance with OFAC requirements. For outbound cross-border ACH transactions, 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.

Additional information on the types of retail payment systems (ACH payment systems) is available in the FFIEC *Information Technology Examination Handbook*.[176]

[176] 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) transactions and management's ability to implement effective monitoring and reporting systems.*

1. Review the policies, procedures, and processes related to ACH transactions. Evaluate the adequacy of the policies, procedures, and processes given the bank's ACH transactions 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 management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors high-risk customers using ACH transactions.

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

4. Determine whether the bank's system for monitoring customers, including third-party service providers (TPSP), using ACH transactions 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.
   - Monitoring ACH detail activity when the batch-processed transactions are separated for other purposes (e.g., processing errors).
   - Applying increased due diligence for international ACH transactions, including domestic transactions when the Originator is based in a foreign country or that are initiated by an international messaging system.
   - Identifying ACH transactions that the bank originates to foreign financial institutions, particularly to high-risk geographic locations.
   - Using methods to track, review, and investigate customer complaints regarding fraudulent or duplicate ACH transactions.

5. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," page 146, 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 high-risk customers, including TPSPs, with ACH transactions, which may include the following:

   - ACH transactions originating from or received by international parties.
   - ACH transactions originating from the Internet or via telephone, particularly those accounts 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 activity.
   - Customers who have been involved in the origination or receipt of duplicate or fraudulent ACH transactions.
   - 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 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 Customer Identification Program (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.

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

Stored value cards can operate in either an open or closed system.[177] Typically, open system cards may be reloaded, allowing the cardholder to add value. Closed system cards are usually limited to the initial value posted to the card, but some may allow the cardholder to add value. Additionally, funds can be prepaid on an open system card by one person, with someone else accessing the currency elsewhere through an ATM. Prepayment involves a transfer of funds to the card (e.g., telephone calling cards). Some domestic and offshore banks offer cards with currency access through ATMs internationally. Since stored value cards are easy to fund and transport without creating a paper trail, they are attractive for abuse by various illegal enterprises and money launderers. For example, drug dealers have been known to load currency onto prepaid cards and send the cards to their drug suppliers outside the country. Phone cards and other closed system prepaid cards can be purchased for currency and transferred from one person to another and resold. Often, a firm independent of a bank processes all card transactions through a "pooled" bank account held in the name of the firm managing the card program.[178]

Consumers use e-cash to access, store, and redeem funds that are maintained electronically. In addition, e-cash, in the form of payroll cards, is now offered by employers to their employees in place of a check to distribute wages. These payroll cards may also function as multi-purpose or general use reloadable cards (i.e., the cardholder can add value to the card at a variety of retail outlets using currency). The value of the funds stored on these cards can be transferred between cardholders using compatible electronic systems and networks, often without using banks.

---

[177] "Open" system cards can be used to connect to global debit and ATM networks; the cards can be used for purchases at any merchant or to access currency at any ATM that connects to global payment networks. "Closed" system cards are limited in that they 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 network that is limited geographically or otherwise (e.g., retail gift cards and mass transit system cards).

[178] Refer to the Money Laundering Threat Assessment Working Group, *U.S. Money Laundering Threat Assessment*, December 2005 and the National Drug Intelligence Center Assessment, *Prepaid Stored Value Cards: A Potential Alternative to Traditional Money Laundering Methods*, October 2006.

Using ATMs, point-of-sale devices, or special readers, stored monetary value is subtracted from the card or the value allocated to the card that is held in a pooled bank account. When the monetary value is depleted, the card is either discarded (disposable) or, in some instances, value is replenished (reloadable). 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*.[179]

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

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

Examination Procedures

Electronic Cash

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

1. Review the policies, procedures, and processes related to e-cash. Evaluate the adequacy of the policies, procedures, and processes given the bank's e-cash activities 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 management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors high-risk e-cash transactions.

3. Determine whether the bank's system for monitoring e-cash 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," page 146, for guidance.

Transaction Testing

5. On the basis of the bank's risk assessment of its e-cash 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 Customer Identification Program (CIP) 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.*

Non-bank or third-party payment processors (processors) are bank customers that provide payment-processing services to merchants and other business entities. Traditionally, processors contracted primarily with retailers that had physical locations in order to process the retailers' transactions. These merchant transactions primarily included credit card payments but also covered automated clearing house (ACH) transactions, remotely created checks,[180] and debit and stored value cards transactions. With the expansion of the Internet, retail borders have been eliminated. Processors may now service a variety of merchant accounts, including conventional retail and Internet-based establishments, prepaid travel, and Internet gaming enterprises.

Risk Factors

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

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

Risk Mitigation

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

- Reviewing the processor's promotional materials, including its web site, to determine the target clientele. (Businesses with elevated risk may include offshore companies,

[180] A remotely created check (sometimes called a "demand draft") is a check, 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 on-line, and therefore does not bear the customer's handwritten signature.

on-line gambling-related operations, and on-line payday lenders.) For example, a processor whose customers are primarily offshore would be inherently riskier than a processor whose customers are primarily restaurants.

- Determining whether the processor re-sells its services to a third party who may be referred to as an "agent or provider of Independent Sales Organization (ISO) opportunities" or "gateway" arrangements.[181]
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of its due diligence standards for new merchants.
- Identifying the processor's major customers.
- Reviewing corporate documentation including independent reporting services and, if applicable, documentation on principal owners.
- Visiting the processor's business operations center.

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

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

- Merchant base.
- Merchant activities.
- Average number of dollar volume and number of transactions.
- "Swiping" versus "keying" volume for credit card transactions.
- Charge-back history, including rates of return for ACH debit transactions and remotely created checks.

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

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 management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors processor relationships, particularly those that pose a high 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," page 146, 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 high-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.
   - 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 Currency Transaction Report (CTR) filing threshold.

Risk Mitigation

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

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

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.[182]

4. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," page 146, for guidance.

Transaction Testing

5. On the basis of the bank's risk assessment, as well as prior examination and audit reports, select a sample of monetary instrument transactions for both customers and noncustomers from:

[182] Money launderers are known to identify the ownership or source of illegal funds through the use of unique and unusual stamps.

- 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," page 137, or "Customer Identification Program" (CIP), core examination procedures, page 52.[183] The bank accepting brokered deposits depends on the deposit broker to sufficiently perform required account opening procedures and to follow applicable BSA/AML compliance program requirements.

Risk Factors

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

Risk Mitigation

Banks that accept deposit broker accounts or funds should develop appropriate policies, procedures, and processes that establish minimum CDD procedures for all deposit brokers providing deposits to the bank. The level of due diligence a bank performs should be commensurate with its knowledge of the deposit broker and the deposit broker's known business practices and customer base.

In an effort to address the risk inherent in certain deposit broker relationships, banks may want to consider having a signed contract that sets out the roles and responsibilities of each party and restrictions on types of customers (e.g., nonresident or offshore customers,

[183] 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 sub-accountholder, it need only verify the identity of the named accountholder.

PEPs, or foreign shell banks). Banks should conduct sufficient due diligence on unknown, foreign, independent, or unregulated deposit brokers. To manage the BSA/AML risks associated with brokered deposits, the bank should:

- Determine whether the deposit broker is a legitimate business in all operating locations where the business is conducted.
- Review the deposit broker's business strategies, including targeted customer markets (e.g., foreign or domestic customers) and methods for soliciting clients.
- Determine whether the deposit broker is subject to regulatory oversight.
- Evaluate whether the deposit broker's BSA/AML 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 management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors deposit broker relationships, particularly those that pose a high 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," page 146, 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 high-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 Suspicious Activity Reports (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 high 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 (ATMs) 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.[184]

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*.[185]

Sponsoring Bank

Some electronic funds transfers (EFTs) or point-of-sale (POS) networks require an ISO to be sponsored by a member of the network (sponsoring bank). The sponsoring bank and the ISO are subject to all network rules. The sponsoring bank is also charged with ensuring the ISO abides by all network rules. Therefore, the sponsoring bank should conduct proper due diligence on the ISO and maintain adequate documentation to ensure that the sponsored ISO complies with all network rules.

Risk Factors

Most states do not currently register, limit ownership, monitor, or examine privately owned ATMs or their ISOs. While the provider of the ATM transaction network and the

[184] 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.

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

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:

- 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 Customer Identification Program 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 (ATMs) 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 management information systems (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 customer due diligence (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.[186] 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[187] in co-sponsorship with the bank. For example, a financial services corporation tailors a mutual fund product for sale at a specific bank. The product is sold exclusively at that bank and bears the name of both the bank and the financial services corporation.

Because of this co-branded relationship, responsibility for BSA/AML compliance becomes complex. As these accounts are not under the sole control of the bank or

[186] 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.

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

financial entity, responsibilities for completing Customer Identification Program (CIP), customer due diligence (CDD), and suspicious activity monitoring and reporting can vary. The bank should fully understand each party's contractual responsibilities and ensure adequate control by all parties.

Dual-Employee Arrangements

In a dual-employee arrangement, the bank and the financial services corporation such as an insurance agency or a registered broker/dealer have a common (shared) employee. The shared employee may conduct banking business as well as sell NDIP, or sell NDIP full-time. Because of this dual-employee arrangement, the bank retains responsibility over NDIP activities. Even if contractual agreements establish the financial services corporation as being responsible for BSA/AML, the bank needs to ensure proper oversight of its employees, including dual employees, and their compliance with all regulatory requirements.[188]

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.[189] In addition, the bank may also offer its own proprietary NDIPs, which can be created and offered by the bank, its subsidiary, or an affiliate.

---

[188] 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," page 45, for additional information.

[189] In certain circumstances, a bank may not be considered a broker, and an employee need not register as a broker/dealer. See 15 USC 78c(a)(4) for a complete list.

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

Risk Factors

BSA/AML risks arise because NDIP can involve complex legal arrangements, large dollar amounts, and the rapid movement of funds. NDIP portfolios managed and controlled directly by clients pose a greater money laundering risk than those managed by the bank or by the financial services provider. Sophisticated clients may create ownership structures to obscure the ultimate control and ownership of these investments. For example, customers can retain a certain level of anonymity by creating Private Investment Companies (PICs),[190] offshore trusts, or other investment entities that hide the customer's ownership or beneficial interest.

Risk Mitigation

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

Networking Arrangements

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

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

[190] Refer to expanded overview section, "Business Entities (Domestic and Foreign)," page 290, for additional guidance on PICs.

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

In-House Sales and Proprietary Products

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

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

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

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

4. Determine how the bank includes NDIP sales activities in its bank-wide or, if applicable, enterprise-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," page 146, 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 high 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

On November 3, 2005, FinCEN issued two final rules imposing AML obligations on insurance companies.[191] The rules impose AML compliance program requirements and Suspicious Activity Report (SAR) obligations on insurance companies similar to those that apply to banks. The insurance regulations apply only to insurance companies; there are no independent obligations for brokers and agents. However, the insurance company is responsible for the conduct and effectiveness of its AML compliance program, which includes agent and broker activities. The insurance regulations only apply to a limited range of products that may pose a high 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.[192] However, the bank may need to establish specific policies, procedures, and processes for

[191] 31 CFR 103.137 and 31 CFR 103.16.

[192] 70 *Federal Register* 66758 (November 3, 2005). See also 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.

its insurance sales in order to submit information to the insurance company for the insurance company's AML compliance.

Likewise, if a bank, as an agent of the insurance company, detects unusual or suspicious activity relating to insurance sales, it can file a joint SAR on the common activity with the insurance company.[193]

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).[194]
- Purchasing insurance products through unusual methods such as currency or currency equivalents.
- Buying products with insurance termination features without concern for the product's investment performance.

Risk Mitigation

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

[193] FinCEN has issued a Frequently Asked Questions document, *Anti-Money Laundering Program and Suspicious Activity Reporting Requirements for Insurance Companies* (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.

[194] 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.

- The identification of high-risk accounts.
- Customer due diligence, including enhanced due diligence 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 management information systems (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," page 146, 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 management information systems (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," page 146, 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 high-risk activity (e.g., funds transfers or monetary instruments purchases) and transactions from high-risk jurisdictions.

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

Lending Activities — Overview

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

Lending activities include, but are not limited to, real estate, trade finance,[195] cash-secured, credit card, consumer, commercial, and agricultural. Lending activities can include multiple parties (e.g., guarantors, signatories, principals, or loan participants).

Risk Factors

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

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

Risk Mitigation

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

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

[195] Refer to the expanded overview section, "Trade Finance Activities," page 241, for additional guidance.

business. For example, the bank can review loan reports such as early payoffs, past dues, fraud, or cash-secured.

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 management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors high-risk loan accounts.

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

4. If appropriate, refer to the core examination procedures, "Office of Foreign Assets Control," page 146, 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 high-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. Financial institutions can participate in trade financing by 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.** Issues the letter of credit on behalf of the Applicant and forwards it to the Advising Bank for notification to the Beneficiary. The Applicant is the Issuing Bank's customer, and both are usually located in the same country.
- **Confirming Bank.** Typically in the home country of the Beneficiary, at the request of the Issuing Bank, adds its commitment to honor draws made by the Beneficiary, provided the terms and conditions of the letter of credit are met.
- **Advising Bank.** An Issuing Bank's correspondent bank located near the Beneficiary's domicile, to which the Issuing Bank sends the letter of credit or notification of its issuance, with instructions to notify the Beneficiary. The Advising Bank advises the Beneficiary without taking other active engagement in the letter of credit. The Advising Bank is usually also the Confirming Bank.
- **Beneficiary (Drawer).** The seller or party to whom the letter of credit is addressed.

- **Negotiating Bank.** Usually the Beneficiary's bank. Agrees to purchase the draft and pay the Beneficiary after satisfying itself that documentary requirements have been met.

- **Accepting Bank.** Incurs a legal obligation to pay the draft at maturity. Drafts are drawn on the Accepting Bank that dates and signs the instrument.

- **Discounting Bank.** Discounts a draft for the Beneficiary after it has been accepted by an Accepting Bank.

- **Reimbursing Bank.** Authorized by the Issuing Bank to reimburse the Drawee Bank submitting claims under the letter credit.

- **Paying (Drawee) Bank.** As named in the letter of credit, the bank where drafts are to be paid. The Paying Bank is typically the Issuing Bank, but is often a branch or correspondent of the Issuing Bank. Once paid or accepted by the Paying or Drawee Bank, there is no recourse to the drawers.

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 involvement of multiple parties on both sides of any international trade transaction can make the process of due diligence more difficult. Also, since 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 fraudulently altered to hide the scheme. Variations on this theme include inaccurate or double invoicing, partial shipment of goods, and the use of fictitious goods. Illegal proceeds transferred in such transactions thereby appear sanitized and enter the realm of legitimate commerce.

The Applicant may substitute third-party nominees, such as shell companies, to disguise the Applicant's role in a trade finance agreement. This substitution results in a lack of transparency, effectively hiding the identity of the purchasing party, thus increasing the risk of money laundering activity.

Risk Mitigation

Sound customer due diligence (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 prospective import or export customers 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," page 56, 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.[196]

Banks taking other roles in the letter of credit process should complete due diligence that is commensurate with their roles in each transaction. Banks need to be aware that because of the frequency of transactions in which multiple banks are involved, Issuing Banks may not always have correspondent relationships with the Advising or Confirming Bank.

To the extent feasible, banks should review documentation, not only for compliance with the terms of the letter of credit, but also for anomalies or red flags that could indicate unusual or suspicious activity. Reliable documentation is critical in identifying potentially suspicious activity. When analyzing applicable trade transactions, banks should consider obtaining copies of official U.S. or foreign government import and export forms to assess the reliability of documentation provided.[197] 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 Suspicious Activity Report (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.

---

[196] Refer to *Trade Based Money Laundering*, June 23, 2006, at www.fatf-gafi.org/dataoecd/60/25/37038272.pdf.

[197] For instance, U.S. Customs and Border Protection Form 7501 (Entry Summary) (www.cbp.gov/linkhandler/cgov/toolbox/forms/7501.ctt/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.)

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," page 137, 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 overview section "Suspicious Activity Reporting," page 60, and expanded overview section, "Funds Transfers," page 192, for additional guidance.

Policies, procedures, and processes should also require a thorough review of all applicable trade documentation 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 management information systems 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 high-risk jurisdictions.
- Customers shipping items through high-risk jurisdictions, including transit through non-cooperative countries.
- Customers involved in potentially high-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 directs payment of proceeds to an unrelated third party.
- Shipment locations or description of goods not consistent with letter of credit.
- Documentation showing a higher or lower value or cost of merchandise than that which was declared to customs or paid by the importer.

- 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.

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 management information systems (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," page 146, 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 high net worth customers (e.g., estate planning, financial advice, lending, investment management, bill paying, mail forwarding, and maintenance of a residence). Private banking has become an increasingly important business line for large and diverse banking organizations and a source of enhanced fee income.

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

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

- Cash management (e.g., checking accounts, overdraft privileges, cash sweeps, and bill-paying services).
- Funds transfers.
- Asset management (e.g., trust, investment advisory, investment management, and custodial and brokerage services).[198]
- The facilitation of shell companies and offshore entities (e.g., Private Investment Companies (PICs), international business corporations (IBCs), and trusts).[199]
- Lending services (e.g., mortgage loans, credit cards, personal loans, and letters of credit).
- Financial planning services including tax and estate planning.

[198] For additional guidance, refer to the expanded overview and examination procedures, "Trust and Asset Management Services," pages 254 and 258, respectively.

[199] For additional guidance, refer to the expanded overview and examination procedures, "Business Entities (Domestic and Foreign)," pages 290 and 296, respectively.

- 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"[200] outlined, in part, the following vulnerabilities to money laundering:

- Private bankers as client advocates.
- Powerful clients including politically exposed persons, industrialists, and entertainers.
- A culture of confidentiality and the use of secrecy jurisdictions or shell companies.[201]
- A private banking culture of lax internal controls.
- The 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)," page 120. 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.

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

[201] Refer to the expanded overview section, "Business Entities (Domestic and Foreign)," page 290, 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 (PEPs).[202]

- **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

Customer due diligence (CDD) is essential when establishing any customer relationship and it is critical for private banking clients.[203] Banks should take reasonable steps to establish the identity of their private banking clients and, as appropriate, the beneficial owners of accounts. Adequate due diligence should vary based on the risk factors identified previously. Policies, procedures, and processes should define acceptable CDD for different types of products (e.g., PICs), services, and accountholders. As due

[202] Refer to the core overview section, "Private Banking Due Diligence Program (Non-U.S. Persons)," page 120, and to the expanded overview section, "Politically Exposed Persons," page 264, for additional guidance.

[203] Due diligence policies, procedures, and processes are required for private banking accounts for non-U.S. persons by section 312 of the Patriot Act. Refer to the core overview section, "Private Banking Due Diligence Program (Non-U.S. Persons)," page 120, for additional guidance.

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[204] and to determine whether the account is maintained for non-U.S. persons.[205]

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

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

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, banks may choose to maintain (or have an independent third party maintain) bearer shares for new clients, or those without well-established relationships with the institution. For well-known, long-time customers, banks may find that periodically re-certifying beneficial ownership is effective. The best underlying control associated with these types of structures is a strong CDD program through which banks

[204] 31 CFR 103.121(b)(2)(ii)(C).

[205] Refer to the core examination procedures, "Private Banking Due Diligence Program (Non-U.S. Persons)," page 125, for additional guidance.

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.

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

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 management information systems (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," page 146, 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 (PEPs).
   - Private Investment Companies (PICs), international business corporations (IBCs), and shell companies.

- Offshore entities.
- Cash-intensive businesses.
- Import or export companies.
- Customers from or doing business in a high-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[206] services, and management's ability to implement effective due diligence, monitoring, and reporting systems.*

Trust[207] accounts are generally defined as a legal arrangement in which one party (the trustor or grantor) transfers ownership of assets to a person or bank (the trustee) to be held or used for the benefit of others. These arrangements include the broad categories of court-supervised accounts (i.e., executorships and guardianships), personal trusts (i.e., living trusts, trusts established under a will, and charitable trusts), and corporate trusts (i.e., bond trusteeships).

Unlike trust arrangements, agency accounts are established by contract and governed by contract law. Assets are held under the terms of the contract, and legal title or ownership does not transfer to the bank as agent. Agency accounts include custody, escrow, investment management,[208] and safekeeping relationships. Agency products and services may be offered in a traditional trust department or through other bank departments.

Customer Identification Program

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

For purposes of the CIP, the bank is not required to search the trust, escrow, or similar accounts to verify the identities of beneficiaries, but instead is only required to verify the identity of the named accountholder (the trust). In the case of a trust account, the customer is the trust whether or not the bank is the trustee for the trust. However, the CIP rule also provides that, based on the bank's risk assessment of a new account opened by a customer that is not an individual, the bank may need "to obtain information about" individuals with authority or control over such an account, including signatories, in order

[206] Asset management accounts can be trust or agency accounts and are managed by the bank.

[207] 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).

[208] 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.

to verify the customer's identity.[209] 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.[210]

Risk Factors

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

- Personal and court-supervised accounts.
- Trust accounts formed in the private banking department.
- Asset management and investment advisory accounts.
- Global and domestic custody accounts.
- Securities lending.
- Employee benefit and retirement accounts.
- Corporate trust accounts.
- Transfer agent accounts.
- Other related business lines.

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

[210] *Id.*

As in any account relationship, money laundering risk may arise from trust and asset management activities. When misused, trust and asset management accounts can conceal the sources and uses of funds, as well as the identity of beneficial and legal owners. Customers and account beneficiaries may try to remain anonymous in order to move illicit funds or avoid scrutiny. For example, customers may seek a certain level of anonymity by creating Private Investment Companies (PICs),[211] offshore trusts, or other investment entities that hide the true ownership or beneficial interest of the trust.

Risk Mitigation

Management should develop policies, procedures, and processes that enable the bank to identify unusual account relationships and circumstances, questionable assets and sources of assets, and other potential areas of risk (e.g., offshore accounts, PICs, asset protection trusts (APTs),[212] agency accounts, and unidentified beneficiaries). While the majority of traditional trust and asset management accounts will not need enhanced due diligence, management should be alert to those situations that need additional review or research.

Customer Comparison Against Lists

The bank must 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 (PEPs), doing business with or located in a jurisdiction designated as "primary money laundering concern" under section 311 of the Patriot Act, or match OFAC lists.[213] 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," page 87, and expanded overview section, "Politically Exposed Persons," page 264, for additional guidance.

Circumstances Warranting Enhanced Due Diligence

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

[211] For additional guidance on PICs, refer to the expanded overview section, "Business Entities (Domestic and Foreign)," page 290.

[212] 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.

[213] Management and examiners should be aware that OFAC list-matching is not a BSA requirement. However, since trust systems are typically separate and distinct from bank systems, verification of these checks on the bank system is not sufficient to ensure that these checks are also completed in the trust and asset management department. 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," page 137, for additional guidance.

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

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

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

- The bank is entering into a relationship with a new customer.
- The account principals or beneficiaries reside in a foreign jurisdiction, or the trust or its funding mechanisms are established offshore.
- Assets or transactions are atypical for the type and character of the customer.
- The account type, size, assets, or transactions are atypical for the bank.
- International funds transfers are conducted, particularly through offshore funding sources.
- Accounts are funded with easily transportable assets such as gemstones, precious metals, coins, artwork, rare stamps, or negotiable instruments.
- Accounts or relationships are maintained in which the identities of the principals, or beneficiaries, or sources of funds are unknown or cannot easily be determined.
- Accounts benefit charitable organizations or other non-governmental organizations (NGOs) that may be used as a conduit for illegal activities.[214]
- Interest on lawyers' trust accounts (IOLTA) holding and processing significant dollar amounts.
- Account assets that include PICs.
- PEPs are parties to any accounts or transactions.

[214] For additional guidance, refer to the expanded overview section, "Non-Governmental Organizations and Charities," page 287.

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[215] 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," page 15, 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 management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors trust and asset management relationships, particularly those that pose a high risk for money laundering.

4. Determine how the bank includes trust and asset management relationships in a bank-wide or, if appropriate, enterprise-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," page 146, for guidance.

[215] 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 high-risk trust and asset management services relationships. Include relationships with grantors and co-trustees, if they have authority or control, as well as any high-risk assets such as Private Investment Companies (PICs) or asset protection trusts. From the sample selected, perform the following examination procedures:

   - Review account opening documentation, including the Customer Identification Program (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 (NRAs) 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,[216] or (ii) has not been issued an alien registration receipt card, also known as a green card. The Internal Revenue Service (IRS) determines the tax liabilities of a foreign person and officially defines the person as a "resident" or "nonresident."

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

Risk Factors

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

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

secrecy laws of that country. Since the NRA is expected to reside outside of the United States, funds transfers or the use of foreign automated teller machines (ATMs) may be more frequent. The BSA/AML risk may be further heightened if the NRA is a politically exposed person (PEP). Refer to the expanded examination procedures, "Politically Exposed Persons," page 268, for further information.

Risk Mitigation

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

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

NRA customers may request W-8 status for U.S. tax withholding. In such cases, the NRA customer completes a W-8 form, which attests to the customer's foreign and U.S. tax-exempt status. While it is an 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.[217]

The bank's Customer Identification Program (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)," page 120, and the expanded overview and examination procedures, "Politically Exposed Persons," page 264.

[217] Additional information can be found at www.irs.gov/formspubs. See also 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 (NRAs) 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 management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors high-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," page 146, 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 high-risk NRA accounts. Include the following risk factors:

   - An account for resident or citizen of a high-risk jurisdiction.
   - Account activity is substantially currency based.
   - An NRA or foreign individual who uses a wide range of bank services, particularly correspondent services.
   - An NRA or foreign individual for whom the bank has filed a Suspicious Activity Report (SAR).

6. From the sample selected, perform the following examination procedures:

- Review the customer due diligence information, including Customer Identification Program 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" (PEPs), and management's ability to implement effective risk-based due diligence, monitoring, and reporting systems. If the relationship is a private banking account [218] refer to core overview section, "Private Banking Due Diligence Program (Non-U.S. Persons)," page 120, 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 and their associates. Because the risks presented by PEPs will vary, 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.[219] 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.[220] 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.

---

[218] 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.

[219] *Guidance on Enhanced Scrutiny for Transactions that may Involve the Proceeds for Foreign Official Corruption* issued by the U.S. Treasury, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision, and the Department of State, January 2001.

[220] 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.[221] Titles alone may not provide sufficient information to determine if an individual is a PEP, since governments are organized differently from jurisdiction to jurisdiction.

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.
- The nature of the title (e.g., honorary or salaried).
- Level of authority over government activities or other officials.
- Access to significant government assets or funds.

In determining the acceptability of high-dollar or high-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 high-dollar or high-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 high-risk determination; it is only one factor the bank should consider in assessing the risk of a relationship.

Ascertaining whether a customer has a close association with a senior foreign political figure can be difficult, although focusing on those relationships that are "widely and publicly known" provides a reasonable limitation on expectations to identify close associates as PEPs. However, banks that have actual knowledge of a close association should consider their customer a PEP, even if such association is not otherwise widely or publicly known. Banks are expected to follow reasonable steps to ascertain the status of an individual, and the federal banking agencies and FinCEN recognize that these steps may not uncover all close associations.

[221] 71 *Federal Register* 495–515.

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 geographic locations involved and the individual's position or authority. 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 reputation 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 control or influence over state-owned government or corporate accounts.

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 high-risk products and services are critical, as this 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.
- Seek information directly from the individual regarding possible PEP status.
- Identify the accountholder's country of residence.
- Obtain information regarding employment or other sources of funds.
- Check references, as appropriate, to determine whether the individual is or has been a PEP.
- Identify the source of wealth.
- Obtain information on immediate family members or close associates having transaction authority over 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 against reasonably accessible public databases (e.g., government databases, major

news publications, free commercial databases available on the Internet, and fee-based databases, 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)," page 120, 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" (PEPs), and management's ability to implement effective risk-based due diligence, monitoring, and reporting systems. If the relationship is a private banking account [222] refer to core overview section, "Private Banking Due Diligence Program (Non-U.S. Persons," page 120, 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 money laundering 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 management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors PEP relationships, particularly those that pose a high risk for money laundering.

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 the core examination procedures, "Office of Foreign Assets Control," page 146, 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:

[222] 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.
- 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 (PEPs) in certain circumstances.[223]

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 high risk.
- Substantial currency transactions take place in the accounts.

[223] For additional guidance, refer to the expanded overview section, "Politically Exposed Persons," page 264.

- 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.[224] 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.

[224] For additional guidance, refer to the core section overview, "Private Banking Due Diligence Program (Non-U.S. Persons)," page 120.

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 management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors embassy and foreign consulate accounts, particularly those that pose a high 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," page 146, 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.

Non-Bank Financial Institutions — Overview

Objective. *Assess the adequacy of the bank's systems to manage the risks associated with accounts of non-bank financial institutions (NBFIs), and management's ability to implement effective monitoring and reporting systems.*

NBFIs are broadly defined as institutions other than banks that offer financial services. The Patriot Act has defined a variety of entities as financial institutions.[225] 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 (MSBs).[226]
- 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

[225] Refer to Appendix D ("Statutory Definition of Financial Institution") for guidance.

[226] 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 has issued guidance stating that certain businesses that cash their own checks do not meet the definition of a "check casher." *See* FIN-2006-G005, *Frequently Asked Questions — Businesses Cashing Their Own Checks*, March 31, 2006, at www.fincen.gov.

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.[227] 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.[228] Existing FinCEN regulations require certain MSBs to register with FinCEN.[229] 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:

- 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.

[227] 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.

[228] *See* 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).

[229] *See* 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. *See* FIN-2006-G006, *Registration and De-Registration of Money Services Businesses*, February 3, 2006, at www.fincen.gov.

- 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 low 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, enhanced due diligence (EDD) policies, procedures, and controls.

The factors below, while not all inclusive, may reduce or mitigate the risk in some MSB accounts:

- The MSB is registered with FinCEN and licensed with the appropriate state(s), if required.
- The MSB confirms it is subject to examination for AML compliance by the Internal Revenue Service (IRS) or the state(s), if applicable.
- The MSB affirms the existence of a written BSA/AML program and provides the BSA officer's name and contact information.
- The MSB has an established banking relationship and/or account activity consistent with expectations.
- The MSB is an established business with an operating history.
- The MSB is a principal with one or a few agents, or is acting as an agent for one principal.
- The MSB provides services only to local residents.
- Most of the MSB's customers conduct routine transactions in low dollar amounts.
- The expected (low-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

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[230] are:

- Apply the bank's Customer Identification Program.[231]
- 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 enhanced due diligence 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.

[230] 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.

[231] See 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).

- Conduct onsite visits.
- Review list of agents, including locations, within or outside the United States, that will be receiving services directly or indirectly through the MSB account.
- 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

Non-Bank Financial Institutions

Objective. *Assess the adequacy of the bank's systems to manage the risks associated with accounts of non-bank financial institutions (NBFIs), and management's ability to implement effective monitoring and reporting systems.*

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 management information systems (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 (MSBs) 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 high-risk NBFI accounts. From the sample selected, perform the following examination procedures:

   - Review account opening documentation and ongoing due diligence information.
   - Review account statements and, as necessary, specific transaction details. Compare expected transactions with actual activity.
   - Determine whether actual activity is consistent with the nature of the customer's business and identify any unusual or suspicious activity.

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

Professional Service Providers — Overview

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

A professional service provider acts as an intermediary between its client and the bank. Professional service providers include lawyers, accountants, investment brokers, and other third parties that act as financial liaisons for their clients. These providers may conduct financial dealings for their clients. For example, an attorney may perform services for a client, or arrange for services to be performed on the client's behalf, such as settlement of real estate transactions, asset transfers, management of client monies, investment services, and trust arrangements.

A typical example is interest on lawyers' trust accounts (IOLTA). These accounts contain funds for a lawyer's various clients, and act as a standard bank account with one unique feature: The interest earned on the account is ceded to the state bar association or another entity for public interest and pro bono purposes.

Risk Factors

In contrast to escrow accounts that are set up to serve individual clients, professional service provider accounts allow for ongoing business transactions with multiple clients. Generally, a bank has no direct relationship with or knowledge of the beneficial owners of these accounts, who may be a constantly changing group of individuals and legal entities.

As with any account that presents third-party risk, the bank could be more vulnerable to potential money laundering abuse. Some potential examples of abuse could include:

- Laundering illicit currency.
- Structuring currency deposits and withdrawals.
- Opening any third-party account for the primary purpose of masking the underlying client's identity.

As such, the bank should establish an effective due diligence program for the professional service provider as summarized below.

Risk Mitigation

When establishing and maintaining relationships with professional service providers, banks should adequately assess account risk and monitor the relationship for suspicious or unusual activity. At account opening, the bank should have an understanding of the intended use of the account, including anticipated transaction volume, products and services used, and geographic locations involved in the relationship. As indicated in the core overview section, "Currency Transaction Reporting Exemptions," page 81,

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 management information systems (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," page 146, 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 high-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.

Non-Governmental Organizations and Charities — Overview

Objective. *Assess the adequacy of the bank's systems to manage the risks associated with accounts of non-governmental organizations (NGOs) and charities, and management's ability to implement effective due diligence, monitoring, and reporting systems.*

NGOs are private nonprofit organizations that pursue activities intended to serve the public good. NGOs may provide basic social services, work to relieve suffering, promote the interests of the poor, bring citizen concerns to governments, encourage political participation, protect the environment, or undertake community development to serve the needs of citizens, organizations, or groups in one or more of the communities that the NGO operates. An NGO can be any nonprofit organization that is independent from government.

NGOs can range from large regional, national, or international charities to community-based self-help groups. NGOs also include research institutes, churches, professional associations, and lobby groups. NGOs typically depend, in whole or in part, on charitable donations and voluntary service for support.

Risk Factors

Since NGOs can be used to obtain funds for charitable organizations, the flow of funds both into and out of the NGO can be complex, making them susceptible to abuse by money launderers and terrorists. The U.S. Treasury issued guidelines to assist charities in adopting practices to reduce the risk of terrorist financing or abuse.[232]

Risk Mitigation

To assess the risk of NGO customers, a bank should conduct adequate due diligence on the organization. In addition to required Customer Identification Program (CIP) information, due diligence for NGOs should focus on other aspects of the organization, such as the following:

- Purpose and objectives of their stated activities.
- The geographic locations served (including headquarters and operational areas).
- The organizational structure.
- The donor and volunteer base.

[232] *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.

- Funding and disbursement criteria (including basic beneficiary information).
- Recordkeeping requirements.
- Its affiliation with other NGOs, governments, or groups.
- Internal controls and audits.

For accounts that bank management considers to be high risk, stringent documentation, verification, and transaction monitoring procedures should be established. NGO accounts that are at higher risk for BSA/AML concerns include those operating or providing services internationally, conducting unusual or suspicious activities, or lacking proper documentation. Enhanced due diligence for these accounts should include:

- Evaluating the principals.
- Obtaining and reviewing the financial statements and audits.
- Verifying the source and use of funds.
- Evaluating large contributors or grantors of the NGO.
- Conducting reference checks.

Examination Procedures

Non-Governmental Organizations and Charities

Objective. *Assess the adequacy of the bank's systems to manage the risks associated with accounts of non-governmental organizations (NGOs) and charities, and management's ability to implement effective due diligence, monitoring, and reporting systems.*

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 management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors high-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," page 146, 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 high-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[233] business entity that may pose heightened risks.[234] 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.[235]

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

[233] 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.

[234] 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. *See* FIN-2006-G014, *Potential Money Laundering Risks Related to Shell Companies*, November 2006, at www.fincen.gov.

[235] *See* GAO, *Company Formations — Minimal Ownership Information is Collected and Available*, GAO-06-376, April 2006, at www.gao.gov. For additional information, refer to *Failure to Identify Company Owners Impedes Law Enforcement*, Senate Hearing 109-845, held on November 14, 2006, at www.senate.gov/~govt-aff/index.cfm?Fuseaction=Hearings.Detail&HearingID=406, 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 www.senate.gov/~govt-aff/index.cfm?FuseAction=Hearings.Detail&HearingID=385.

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 (IBCs) and Private Investment Companies (PICs) opened in offshore financial centers (OFCs). 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.[236]

[236] 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.[237] 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.[238] 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.[239]

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).

[237] 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.

[238] *Failure to Identify Company Owners Impedes Law Enforcement. See* Senate Hearing 109-845 held on November 14, 2006.

[239] 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 high-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 Customer Identification Program (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. Since 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, banks may choose to maintain (or have an independent third party maintain) bearer shares for new clients, or those without well-established relationships with the institution. For 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 high-risk transactions in these accounts, such as activity that has no business or apparent lawful purpose, funds transfer activity to and from high-risk jurisdictions, currency intensive transactions, and frequent changes in the ownership or control of the nonpublic 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 management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors high-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," page 146, 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 high-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 high 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 (ATMs).
- Vending machine operators.
- Parking garages.

Risk Factors

Some businesses and entities may be misused by money launderers to legitimize their illicit proceeds. For example, a criminal may own a cash-intensive business, such as a restaurant, and use it to launder currency from illicit criminal activities. The restaurant's currency deposits with its bank do not, on the surface, appear unusual since the business is legitimately a cash-generating entity. However, the volume of currency in a restaurant used to launder money will most likely be higher in comparison with similar restaurants in the area. The nature of cash-intensive businesses and the difficulty in identifying unusual activity may cause these businesses to be considered high risk.

Risk Mitigation

When establishing and maintaining relationships with cash-intensive businesses, banks should establish policies, procedures, and processes to identify high-risk relationships; assess AML risks; complete due diligence at account opening and periodically throughout the relationship; and include such relationships in appropriate monitoring for unusual or suspicious activity. At the time of account opening, the bank should have an understanding of the customer's business operations; the intended use of the account; including anticipated transaction volume, products, and services used; and the geographic locations involved in the relationship.

When conducting a risk assessment of cash-intensive businesses, banks should direct their resources to those accounts that pose the greatest risk of money laundering or terrorist financing. The following factors may be used to identify the risks:

- The purpose of the account.
- The volume, frequency, and nature of currency transactions.
- Customer history (e.g., length of relationship, Currency Transaction Report (CTR) filings,[240] and Suspicious Activity Report (SAR) filings).
- The primary business activity, products, and services offered.
- The business or business structure.
- Geographic locations and jurisdictions of operations.
- The availability of information and cooperation of the business in providing information.

For those customers deemed to be particularly high risk, bank management may consider implementing sound practices, such as periodic on-site visits, interviews with the business's management, or closer reviews of transactional activity.

[240] As discussed in the core overview section, "Currency Transaction Reporting Exemptions," page 81, 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 management information systems (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," page 146, 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 Customer Identification Program (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.