BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – Scoping and Planning

OBJECTIVE

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

PROCEDURES

To accomplish the goals of the BSA/AML examination, the examiner must determine the BSA/AML risk profile of the bank, as a part of the scoping and planning process. Whenever possible, the scoping and planning process should be completed before entering the bank. The scoping and planning process generally begins with an analysis of off-site monitoring information, prior examination reports and workpapers, request letter items completed by bank management, the bank's BSA/AML risk assessment, BSA-reporting databases, and independent reviews or audits.

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

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

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

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

1. Review prior examination or inspection reports, related workpapers, and management's responses to previously identified BSA violations, deficiencies, and recommendations. Discuss, as necessary, with the person(s) responsible for ongoing supervision of the bank or with the prior examiner in charge (EIC) any additional information or ongoing concerns that are not documented in the correspondence.

Consider reviewing news articles concerning or pertaining to the bank or its management.

2. Review the prior examination workpapers to identify the specific BSA/AML examination procedures completed, obtain BSA contact information, identify the report titles and formats the bank uses to detect unusual activity, identify previously noted high-risk banking operations, and review recommendations for the next examination.

3. As appropriate, contact bank management, including the BSA compliance officer, to discuss the following:

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

4. Send the request letter to the bank. Review the request letter documents provided by the bank. Refer to Appendix H ("Request Letter Items").

5. Read correspondence between the bank and its primary regulators, if not already completed by the examiner in charge, or other dedicated examination personnel. The examiner should become familiar with the following, as applicable:

   - Outstanding, approved, or denied applications.
   - Change of control documents, when applicable.
   - Approvals of new directors or senior management, when applicable.
   - Details of meetings with bank management.
   - Other significant activity affecting the bank or its management.

6. Review correspondence that the bank or the primary regulators has received from, or sent to, outside regulatory and law enforcement agencies relating to BSA/AML compliance. Communications, particularly those received from FinCEN, and the Internal Revenue Service (IRS) Detroit Computing Center may document matters relevant to the examination, such as the following:

   - Filing errors for Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs), and CTR exemptions.
   - Civil money penalties issued by or in process from FinCEN.
   - Law enforcement subpoenas or seizures.
   - Notification of mandatory account closures of non-cooperative foreign customers holding correspondent accounts as directed by the Secretary of the Treasury or the U.S. Attorney General.

7. Review the bank's BSA/AML risk assessment or internally identified high-risk banking operations (products, services, customers, and geographic locations). Determine whether the bank has offered any new product or services, or has targeted any new markets, since the previous examination. If the bank has not developed a risk assessment, or if the risk assessment is inadequate, the examiner must complete a risk assessment. Refer to Appendix J ("Quantity of Risk Matrix") when performing this analysis.

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

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

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

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

10. While OFAC regulations are not part of the BSA, evaluation of OFAC compliance is frequently included in BSA/AML examinations. It is not the federal banking agencies' primary role to identify OFAC violations, but rather to evaluate the sufficiency of a bank's implementation of policies, procedures, and processes to ensure compliance with OFAC laws and regulations. Examinations of an OFAC program for a large complex bank may be a review of a single business line. For these reviews, examiners will need to tailor the procedures that follow. To facilitate the examiner's understanding of the bank's risk profile and to adequately establish the scope of the OFAC examination, the examiner should complete the following steps:

- Review the bank's OFAC risk assessment. The risk assessment should consider the various types of products, services, customers, transactions and geographic locations in which the bank is engaged, including those that are processed by, through, or to the bank to identify potential OFAC exposure.
- Review the bank's independent testing of OFAC program.
- Review correspondence received from OFAC, and as needed, the civil penalties area on OFAC's web site to determine if the bank had any warning letters, fines or penalties imposed by OFAC since the most recent examination.
- Review correspondence between the bank and OFAC (e.g., periodic reporting of prohibited transactions and if applicable, annual OFAC reports on blocked property).

11. On the basis of the above procedures, develop an initial examination plan. The scoping and planning process should ensure that the examiner is aware of the bank's BSA/AML compliance program, OFAC program, compliance history, and risk profile (products, services, customers, and geographic locations).

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – BSA/AML Compliance Program

OBJECTIVE

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

PROCEDURES

1. Review the bank's written BSA/AML compliance program to ensure it contains the following required elements:

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

   In addition, a customer identification program (CIP) must be included as part of the BSA/AML compliance program.

Risk Assessment Link to the BSA/AML Compliance Program

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

Internal Controls

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

   - Identify high-risk banking operations (products, services, customers, and geographic locations); provide for periodic updates to the bank's risk profile; and provide for a BSA/AML compliance program tailored to manage risks.

- Inform the board of directors, or a committee thereof, and senior management, of compliance initiatives, identified compliance deficiencies, Suspicious Activity Reports (SARs) filed,[156] and corrective action taken.
- Identify a person or persons responsible for BSA/AML compliance.
- Provide for program continuity despite changes in management or employee composition or structure.
- Meet all regulatory requirements, meet recommendations for BSA/AML compliance, and provide for timely updates to implement changes in regulations.
- Implement risk-based customer due diligence (CDD) policies, procedures, and processes.
- Identify reportable transactions and accurately file all required reports, including SARs, Currency Transaction Reports (CTRs), and CTR exemptions. (Banks should consider centralizing the review and report-filing functions within the banking organization.)
- Provide for dual controls and the segregation of duties. Employees that complete the reporting forms (e.g., SARs, CTRs, and CTR exemptions) should not also be responsible for filing the reports or granting the exemptions.
- Provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity.
- Provide for adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity covered by the BSA and its implementing regulations.
- Train employees to be fully aware of their responsibilities under the BSA regulations and internal policy guidelines.
- Incorporate BSA compliance into job descriptions and performance evaluations of appropriate personnel.

Independent Testing (Audit)

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

5. Evaluate the qualifications of the person (or persons) performing the independent testing to ensure that the bank can rely upon the findings and conclusions.

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

    - BSA/AML risk assessment.
    - BSA/AML compliance program.

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

- BSA reporting and recordkeeping requirements.
- Customer Identification Program (CIP) implementation.
- The adequacy of CDD policies, procedures, and processes and whether they comply with internal requirements.
- Personnel adherence to the bank's BSA/AML policies, procedures, and processes.
- Appropriate transaction testing, with particular emphasis on high-risk operations (products, service, customers, and geographic locations).
- Training adequacy, including its comprehensiveness, accuracy of materials, the training schedule, and attendance tracking.

7. Through a verification of the auditor's reports and workpapers, determine whether the bank's audit review procedures confirm the integrity and accuracy of management information systems (MIS) used in the BSA/AML compliance program (e.g., MIS includes reports used to identify large currency transactions, aggregate daily currency transactions, funds transfer transactions, and monetary instrument sales transactions).

8. If an automated system is not used to identify or aggregate large transactions, determine whether the audit or independent review includes a sample test check of tellers' cash proof sheets, tapes, or other documentation to determine whether large currency transactions are accurately identified and reported.

9. Determine whether the audit's review of suspicious activity monitoring systems includes an evaluation of the system's ability to identify unusual activity. Ensure, through a validation of the auditor's reports and workpapers, that the bank's independent testing:

    - Reviews policies, procedures, and processes for suspicious activity monitoring.
    - Evaluates the system's methodology for establishing and applying expected activity or filtering criteria.
    - Evaluates the system's ability to generate monitoring reports.
    - Determines whether the system filtering criteria are reasonable.

10. Determine whether the audit's review of suspicious activity reporting systems includes an evaluation of the research and referral of unusual activity. Ensure, through a validation of the auditor's reports and workpapers, that the bank's independent testing includes a review of policies, procedures, and processes for referring unusual activity from all business lines (e.g. legal, private banking, foreign correspondent banking) to the personnel or department responsible for evaluating unusual activity.

11. Determine whether audit reviews the effectiveness of the bank's policy for reviewing accounts that generate multiple SAR filings.

12. Determine whether the audit tracks previously identified deficiencies and ensures management corrects them.

13. Review the audit scope, procedures, and workpapers, as applicable, to determine adequacy of the audit based on the following:

    - Overall audit coverage and frequency in relation to the risk profile of the bank.
    - Board reporting and supervision of, and its responsiveness to, audit findings.
    - Adequacy of transaction testing, particularly for high-risk banking operations and suspicious activity monitoring systems.
    - Competency of the auditors or independent reviewers regarding BSA/AML requirements.

BSA Compliance Officer

14. Determine whether the board of directors has designated a person or persons responsible for the overall BSA/AML compliance program. Determine whether the BSA compliance officer has the necessary authority and resources to effectively execute all duties.

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

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

Training

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

    - The importance the board of directors and senior management place on ongoing education, training, and compliance.
    - Employee accountability for ensuring BSA compliance.
    - Comprehensiveness of training, considering specific risks of individual business lines.
    - Training of personnel from all applicable areas of the bank.[157]
    - Frequency of training.
    - Coverage of bank policies, procedures, processes, and new rules and regulations.
    - Coverage of different forms of money laundering and terrorist financing as it relates to identification and examples of suspicious activity.
    - Penalties for noncompliance with internal policies and regulatory requirements.

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

18. As appropriate, conduct discussions with employees (e.g., tellers, funds transfer personnel, internal auditors, and loan personnel) to assess their knowledge of BSA/AML policies and regulatory requirements.

TRANSACTION TESTING

Transaction testing must include, at a minimum, either procedures detailed below (independent testing (audit)) or transaction testing procedures selected from within the core or expanded sections.

Independent Testing

19. Select a judgmental sample that includes transactions other than those tested by the independent auditor and determine whether independent testing:

    - Is comprehensive, adequate, and timely.
    - Has reviewed the accuracy of MIS used in the BSA/AML compliance program.
    - Has reviewed suspicious activity monitoring systems to include the identification of unusual activity
    - Has reviewed whether suspicious activity reporting systems include the research and referral of unusual activity.

Preliminary Evaluation

After the examiner has completed the review of all four required elements of the bank's BSA/AML compliance program, the examiner should document a preliminary evaluation of the bank's program. At this point, the examiner should revisit the initial examination plan, in order to determine whether any strengths or weaknesses identified during the review of the institution's BSA/AML compliance program warrant adjustments to the initial planned scope. Keep in mind, the examiner may complete the "Office of Foreign Assets Control" examination procedures on page 207. The examiner should document and support any changes to the examination scope, then proceed to the applicable core and, if warranted, expanded examination procedures. If there are no changes to the examination scope, the examiner should proceed to the core procedures "Developing Conclusions and Finalizing the Examination" on page 210.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – Customer Identification Program

OBJECTIVE

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

PROCEDURES

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

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

2. Determine whether the bank performed a risk analysis. Consider the types of accounts offered; methods of account opening; and the bank's size, location, and customer base.

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

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

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

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

TRANSACTION TESTING

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

    - Accounts opened for a customer that provides an application for a TIN or accounts opened with incomplete verification procedures.
    - New accounts opened using documentary methods and new accounts opened using nondocumentary methods.
    - Accounts identified as high risk by the bank or its regulator.[158]
    - Accounts opened by existing high-risk customers.
    - Accounts opened with exceptions.
    - Accounts opened by a third party (e.g., indirect loans).

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

    - Opened the account in accordance with the requirements of the CIP (31 CFR 103.121(b)(1)).
    - Formed a reasonable belief as to the true identity of a customer, including a high-risk customer. (The bank should already have a reasonable belief as to the identity of an existing customer (31 CFR 103.121(b)(2)).
    - Obtained from each customer, before opening the account, the identity information required by the CIP (31 CFR 103.121(b)(2)(i)) (e.g., name, date of birth, address, and identification number).
    - Within a reasonable time after account opening, verified enough of the customer's identity information to form a reasonable belief as to the customer's true identity (31 CFR 103.121(b)(2)(ii)).
    - Appropriately resolved situations in which customer identity could not be reasonably established (31 CFR 103.121(b)(2)(iii)).
    - Maintained a record of the identity information required by the CIP, the method used to verify identity, and verification results (including results of discrepancies) (31 CFR 103.121(b)(3)).

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

- Compared the customer's name against the list of known or suspected terrorists or terrorist organizations, if applicable (31 CFR 103.121(b)(4)).
- Filed SARs, as appropriate.

9. Evaluate the level of CIP exceptions to determine whether the bank is effectively implementing its CIP. (A bank's policy may not allow staff to make or approve CIP exceptions. However, a bank may exclude isolated, non-systemic errors [such as an insignificant number of data entry errors] from CIP requirements without compromising the effectiveness of its CIP.) (31 CFR 103.121(b)(1)).

10. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit, select a sample of relationships with third parties the bank relies on to perform its CIP (or portions of its CIP) if applicable. If the bank is using the "reliance provision":

    - Determine whether the third party is a federally regulated institution subject to a final rule implementing the AML program requirements of 31 USC 5318(h).
    - Review the contract between the parties, annual certifications, and other information, such as the third party's CIP (31 CFR 103.121(b)(6)).
    - Determine whether reliance is reasonable. The contract and certification will provide a standard means for a bank to demonstrate that it has satisfied the "reliance provision," unless the examiner has reason to believe that the bank's reliance is not reasonable (e.g., the third party has been subject to an enforcement action for AML or BSA deficiencies or violations).

11. If the bank is using an agent or service provider to perform elements of its CIP, determine whether the bank has established appropriate internal controls and review procedures to ensure that its CIP is being implemented for third-party agent or service-provider relationships (e.g., car dealerships).

12. Review the adequacy of the bank's customer notice and the timing of the notice's delivery (31 CFR 103.121(b)(5)).

13. Evaluate the bank's CIP record retention policy and ensure that it corresponds to the regulatory requirements to maintain certain records. The bank must maintain a description of documents relied on, methods used to verify identity, resolution of discrepancies, and identity information for five years after the account closes (31 CFR 103.121(b)(3)(ii)).

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – Customer Due Diligence

OBJECTIVE

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

PROCEDURES

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

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

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

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

TRANSACTION TESTING

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

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – Suspicious Activity Reporting

OBJECTIVE

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

PROCEDURES

Review of Policies, Procedures, and Processes

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

    - Lines of communication for the referral of unusual activity to appropriate personnel.
    - Designation of individual(s) responsible for identifying, researching, and reporting suspicious activities.
    - Monitoring systems used to identify unusual activity.
    - Procedures to ensure the timely generation of, review of, and response to reports used to identify unusual activities.
    - Procedures for reviewing and evaluating the transaction activity of subjects included in law enforcement requests (e.g., criminal subpoenas, 314(a) requests, or national security letters (NSLs)) for suspicious activity. NSLs are highly confidential documents, and as such, examiners will not review or sample specific NSLs. Instead, examiners should evaluate the policies, procedures, and processes for:

        – Responding to NSLs.
        – Evaluating the account of the target for suspicious activity.
        – Filing Suspicious Activity Reports (SARs), if necessary.
        – Handling account closures.

    - Procedures for documenting decisions not to file a SAR.
    - Procedures for considering closing accounts as a result of continuous suspicious activity.
    - Procedures for completing, filing, and retaining SARs and their supporting documentation.

- Procedures for reporting SARs to the board of directors, or a committee thereof, and senior management.

Evaluating Suspicious Activity Monitoring Systems

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

Manual Transaction Monitoring

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

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

Automated Account Monitoring

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

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

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

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

Evaluating the SAR Decision-Making Process

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

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

11. Determine whether the bank's SAR decision process appropriately considers all available customer due diligence (CDD) information.

TRANSACTION TESTING

Evaluating SAR Quality

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

    - SARs contain accurate information.
    - SAR narratives are complete and thorough, and clearly explain why the activity is suspicious.
    - If SAR narratives from the BSA reporting database are blank or contain language, such as "see attached," ensure that the bank is not mailing attachments to the Internal Revenue Service (IRS) Detroit Computing Center.[159]

Testing the Suspicious Activity Monitoring System

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

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

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

    - Suspicious activity monitoring reports.
    - CTR download information.

[159] The IRS Detroit Computing Center is a central repository for the BSA reports that banks must file.

- High-risk banking operations (products, services, customers, and geographic locations).
- Customer activity.
- Subpoenas received by the bank.
- Decisions not to file a SAR.

14. For the customers selected previously, obtain the following information, if applicable:

    - Customer Identification Program (CIP) and account opening documentation.
    - CDD documentation.
    - Two to three months of account statements covering the total customer relationship and showing all transactions.
    - Sample items posted against the account (e.g., copies of checks deposited and written, debit/credit tickets, and funds transfer beneficiaries and originators).
    - Other relevant information, such as loan files and correspondence.

15. Review the selected accounts for unusual activity. If the examiner identifies unusual activity, review customer information for indications that the activity is typical for the customer (i.e., the sort of activity in which the customer is normally expected to engage). When reviewing for unusual activity, consider the following:

    - For individual customers, whether the activity is consistent with CDD information (e.g., occupation, expected account activity and sources of funds and wealth).
    - For business customers, whether the activity is consistent with CDD information (e.g., type of business, size, location, and target market).

16. Determine whether the manual or automated suspicious activity monitoring system detected the activity that the examiner identified as unusual.

17. For transactions identified as unusual, discuss the transactions with management. Determine whether the account officer demonstrates knowledge of the customer and the unusual transactions. After examining the available facts, determine whether management knows of a reasonable explanation for the transactions.

18. Determine whether the bank has failed to identify any reportable suspicious activity.

19. From the results of the sample, determine whether the manual or automated suspicious activity monitoring system effectively detects unusual or suspicious activity. Identify the underlying cause of any deficiencies in the monitoring systems (e.g., inappropriate filters, insufficient risk assessment, or inadequate decision-making).

Evaluating the SAR Decision Process

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

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

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

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – Currency Transaction Reporting

OBJECTIVE

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

PROCEDURES

1. Determine whether the bank's policies, procedures, and processes adequately address the preparation, filing, and retention of Currency Transaction Reports (CTRs).

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

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

TRANSACTION TESTING

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

    - CTRs are completed in accordance with FinCEN instructions.
    - CTRs are filed for large currency transactions identified by tellers' cash proof sheets, automated large currency transaction systems, or other types of aggregation systems that cover all relevant areas of the bank, unless an exemption exists for the customer.
    - CTRs are filed accurately and completely within 15 calendar days after the date of the transaction (25 days if filed magnetically or electronically).
    - The bank's independent testing confirms the integrity and accuracy of the management information systems (MIS) used for aggregating currency transactions. If not, the examiner should confirm the integrity and accuracy of the MIS. The examiner's review should confirm that tellers do not have the capability to override cash aggregation systems.

- Discrepancies exist between the bank's records of CTRs and the CTRs reflected in the download from the BSA reporting databases.
- The bank retains copies of CTRs for five years from the date of the report (31 CFR 103.27(a)(3)).

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – Currency Transaction Reporting Exemptions

OBJECTIVES

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

PROCEDURES

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

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

2. Determine whether the bank files the form TD F 90-22.53 (Designation of Exempt Person) with the Internal Revenue Service (IRS) to exempt a customer from CTR reporting as defined in 31 CFR 103.22. The form should be filed within 30 days of the first reportable transaction that was exempted.

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

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

Under the regulation, the definition of exempt persons includes "non-listed businesses" and "payroll customers" as defined in 31 CFR 103.22(d)(2)(vi)-(vii). Nevertheless, several businesses remain ineligible for exemption purposes; refer to 31 CFR 103.22(d)(6)(viii) and the "Currency Transaction Reporting Exemptions" overview of this manual.

4. Determine whether the bank files a TD F 90-22.53 with the IRS to exempt a customer, as identified by management, from CTR reporting.

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

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

   - Have frequent[160] currency transactions in excess of $10,000 (withdrawals to pay domestic employees in currency in the case of a payroll customer).
   - Be incorporated or organized under the laws of the United States or a state, or registered as and eligible to do business within the United States or a state.
   - Maintain a transaction account at the bank for at least 12 months.

7. Determine whether the bank's policies, procedures, and processes ensure that the TD F 90-22.53 is filed on or before March 15 of the second year from the date of the original filing and biennially thereafter (for 31 CFR 103.22(d)(2)(vi)-(vii) exemptions only). Ascertain whether filings include both a notification of any change in control relative to the exempt persons and a certification by the bank that it maintains a system for reporting suspicious activity.

TRANSACTION TESTING

8. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of Designation of Exempt Person forms (TD F 90-22.53) from the bank to test compliance with the regulatory requirements (e.g., only eligible businesses are exempted, adequate supporting documentation is maintained, and biennial filings are timely).

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

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – Information Sharing

OBJECTIVE

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

PROCEDURES

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

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

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

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

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

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

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

   - Copies of section 314(a) requests.
   - A log that records the tracking numbers and includes a sign-off column.
   - Copies of the cover page of the requests, with a financial institution sign-off, that the records were checked, the date of the search and search results (e.g., positive/negative).
   - For positive matches, copies of the form returned to FinCEN and the supporting documentation should be retained.

Voluntary Information Sharing (Section 314(b))

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

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

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

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

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

10. Through a review of the financial institution's documentation (including account analysis) on a sample of the information shared and received, evaluate how the financial institution determined whether a Suspicious Activity Report (SAR) was warranted. The financial institution is not required to file SARs solely on the basis of information obtained through the voluntary information sharing process. In fact, the information obtained through the voluntary information sharing process may enable

the financial institution to determine that no SAR is required for transactions that may have initially appeared suspicious. The financial institution should have considered account activity in determining whether a SAR was warranted.

TRANSACTION TESTING

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

    - The financial institution's policies, procedures, and processes enable it to search all of the records identified in the General Instructions for section 314(a) requests. Such processes may be electronic, manual, or both.
    - The financial institution searches appropriate records for each information request received. For positive matches:

        – Verify that a response was provided to FinCEN within the designated time period (31 CFR 103.100(b)(2)(ii)).
        – Review the financial institution's documentation (including account analysis) to evaluate how the financial institution determined whether a SAR was warranted. Financial institutions are not required to file SARs solely on the basis of a match with a named subject; instead, account activity should be considered in determining whether a SAR is warranted.

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

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – Purchase and Sale of Monetary Instruments

OBJECTIVE

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

PROCEDURES

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

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

    - If so, determine whether the bank maintains the required records for sales of monetary instruments to nondepositors.
    - If not permitted, determine whether the bank allows sales on an exception basis.

TRANSACTION TESTING

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

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

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – Funds Transfers

OBJECTIVE

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

PROCEDURES

1. 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.

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

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

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

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

TRANSACTION TESTING

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

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

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – Foreign Correspondent Account Recordkeeping and Due Diligence

OBJECTIVE

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

PROCEDURES

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

Foreign Shell Bank Prohibition and Foreign Correspondent Account Recordkeeping

2. If so, review the bank's policies, procedures, and processes. At a minimum policies, procedures, and process should accomplish the following:

   - Prohibit dealings with foreign shell banks and specify the responsible party for obtaining, updating, and managing certifications or information for foreign correspondent accounts.
   - Identify foreign correspondent accounts and address the sending, tracking, receiving, and reviewing of certification requests or requests for information.
   - Evaluate the quality of information received in responses to certification requests or requests for information.
   - Determine whether and when a Suspicious Activity Report (SAR) should be filed.
   - Maintain sufficient internal controls.
   - Provide for ongoing training.
   - Independently test the bank's compliance with 31 CFR 103.177.

3. Determine whether the bank has on file a current certification or current information (that would otherwise include the information contained within a certification) for each foreign correspondent account to determine whether the foreign correspondent is not a foreign shell bank (31 CFR 103.177(a)).

4. If the bank has foreign branches, determine whether the bank has taken reasonable steps to ensure that any correspondent accounts maintained for its foreign branches are not used to indirectly provide banking services to a foreign shell bank.

Special Due Diligence Program for Foreign Correspondent Accounts

5. Determine whether the bank has implemented due diligence policies, procedures, and controls for correspondent accounts established, maintained, administered, or managed in the United States for foreign financial institutions. Policies, procedures, and controls should incorporate existing sound practices or have a supported rationale for not including a particular sound practice.

6. Review policies, procedures, and processes governing the risk assessment of correspondent accounts with foreign financial institutions. Verify that the following factors have been considered, as appropriate, as criteria in the risk assessment:

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

7. Verify that policies, procedures, and processes are sufficient to identify foreign banks that meet the statutory criteria for enhanced due diligence (31 USC 5318(i)(2)).

8. For foreign financial institutions subject to enhanced due diligence, evaluate the criteria that the bank uses to conduct enhanced scrutiny of any accounts held by such banks to guard against money laundering.

9. Review the bank's policies, procedures, and processes for determining whether foreign correspondent banks subject to enhanced due diligence maintain correspondent accounts for other foreign financial institutions (i.e., nested correspondent accounts), and if so, determine that the bank's policies, procedures, and processes include reasonable steps to ascertain:

    - The identity of the other foreign financial institutions for which the foreign financial institution maintains correspondent accounts.
    - Information relevant to assessing and minimizing risks associated with the foreign bank's correspondent accounts for other foreign financial institutions.

10. Determine whether policies, procedures, and processes require the bank to identify accounts with any foreign bank subject to enhanced due diligence whose shares are not publicly traded. For such accounts, evaluate the bank's policies, procedures, and processes to determine each owner's interest.

TRANSACTION TESTING

Foreign Shell Bank Prohibition and Foreign Correspondent Account Recordkeeping

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

    - Whether certifications and information on the accounts are complete and reasonable.
    - Whether the bank has adequate documentation to evidence that it does not maintain accounts for, or indirectly provide services to, foreign shell banks.
    - For account closures, whether closures were made within a reasonable time period and that the relationship was not re-established without sufficient reason.
    - Whether there are any federal law enforcement requests for information regarding foreign correspondent accounts. If so, ascertain that requests were met in a timely manner.
    - Whether the bank received any official notifications to[161] close a foreign financial institution account. (If so, ascertain that the accounts were closed within ten business days.)
    - Whether the bank retains, for five years from the date of account closure, the original of any document provided by a foreign financial institution, as well as the original or a copy of any document relied on in relation to any summons or subpoena of the foreign financial institution issued under 31 CFR 103.185.

Special Due Diligence Program for Foreign Correspondent Accounts

12. From a sample selected, determine whether the bank consistently follows its general due diligence policies, procedures, and processes for correspondent accounts. Expand the sample to include correspondent accounts maintained for foreign financial institutions other than foreign banks (such as money transmitters) as appropriate.

13. From the original sample, determine whether the bank has implemented enhanced due diligence procedures for higher risk foreign banks operating under:

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

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

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

    - Ascertain, for any such foreign bank whose shares are not publicly traded, the identity of each of the owners of the foreign bank, and the nature and extent of the ownership interest of each such owner.
    - Conduct enhanced scrutiny of any accounts held by such banks to guard against money laundering.
    - Ascertain whether such foreign bank provides correspondent accounts to other foreign banks (i.e. nested correspondent accounts) and, if so, to ascertain the identity of those foreign banks and conduct due diligence as appropriate.

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

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

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

OBJECTIVE

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

PROCEDURES

1. Determine whether the bank engages in private banking activity with non-U.S. persons.

2. Determine whether the bank has implemented due diligence policies, procedures, and controls for private banking accounts established, maintained, administered, or managed in the United States for non-U.S. persons. Determine whether those controls comply with existing sound practices (or have a supported rationale for not including a particular sound practice).

3. Review policies, procedures, and controls the bank uses to ascertain the identity of the nominal and beneficial owners of, and the source of funds deposited into, private banking accounts for non-U.S. persons.

4. Review policies, procedures, and controls governing risk assessment of private banking accounts for non-U.S. persons. Verify that the following factors have been considered, as appropriate, as criteria in the risk assessment:

    - Nature of customer's business (i.e., source of wealth).
    - Purpose of an account and anticipated activity.
    - Customer history.
    - The private banking customer's location of domicile and business.
    - Other available information on the private banking customer.

5. Review the bank's policies, procedures, and controls for performing enhanced scrutiny as required by statute for a private banking account that is requested,

maintained by, or on behalf of a senior foreign political figure or any immediate family member or close associate of a senior foreign political figure.[162]

TRANSACTION TESTING

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

    - Whether the bank's procedures comply with internal policies and statutory requirements.
    - Whether the bank has followed its procedures governing risk assessment of private banking accounts for non-U.S. persons.
    - Whether the bank performs enhanced scrutiny of PEP accounts, consistent with its policy and statutory requirements.

7. On the basis of procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with private banking due diligence programs.

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

[162] As necessary, refer to the expanded procedures section "Politically Exposed Persons" (PEPs), on page 259 for additional guidance.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – Special Measures

OBJECTIVE

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

PROCEDURES

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

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

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

TRANSACTION TESTING

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

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

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

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

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – Foreign Bank and Financial Accounts Reporting

OBJECTIVE

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

PROCEDURES

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

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

TRANSACTION TESTING

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

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – International Transportation of Currency or Monetary Instruments Reporting

OBJECTIVE

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

PROCEDURES

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

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

TRANSACTION TESTING

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

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

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – Office of Foreign Assets Control

OBJECTIVE

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

PROCEDURES

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

2. Regarding the risk assessment, review the bank's OFAC program. Consider the following:

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

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

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

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

TRANSACTION TESTING

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

    - Sample new accounts (e.g., deposit, loan, trust, safe deposit, investments, credit cards, and foreign office accounts,) and evaluate the filtering process used to search the OFAC database (e.g., the timing of the search), and documentation maintained evidencing the searches.
    - Sample appropriate transactions that may not be related to an account (e.g., funds transfers, monetary instrument sales and check cashing transactions), and evaluate the filtering criteria used to search the OFAC database, the timing of the search, and documentation maintained evidencing the searches.
    - If the bank uses an automated system to conduct searches, assess the timing of when updates are made to the system, and when the most recent OFAC changes were made to the system. Also, evaluate whether all of the bank's databases are run against the automated system, and the frequency upon which searches are made. If there is any doubt regarding the effectiveness of the OFAC filter, then run tests of the system by entering test account names that are the same as or similar to those recently added to the OFAC list to determine whether the system identifies a potential hit.
    - If the bank does not use an automated system, evaluate the process used to check the existing customer base against the OFAC list and the frequency of such checks.
    - Review a sample of potential OFAC matches and evaluate the bank's resolution and blocking/rejecting processes.
    - Review a sample of reports to OFAC and evaluate their completeness and timeliness
    - If the bank is required to maintain blocked accounts, select a sample and evaluate that the bank maintains adequate records of amounts blocked and ownership of blocked funds, that the bank is paying a commercially reasonable rate of interest on all blocked accounts, and that it is accurately reporting required information annually (by September 30th) to OFAC. Test the controls in place to verify that the account is blocked.
    - Pull a sample of false hits (potential matches) to check their handling; the resolution of a false hit should take place outside of the business line.

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

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

9. Discuss OFAC related examination findings with bank management.

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Core Examination Procedures – Developing Conclusions and Finalizing the Examination

OBJECTIVE

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

PROCEDURES

Examiners should formulate and state an overall conclusion about the adequacy of the bank's BSA/AML compliance program, as required by statute. In formulating overall conclusions, the examiner does not need to review every procedure at each examination. For procedures completed, identify violations and deficiencies, formulate conclusions, recommend corrective actions, and write comments. During discussions with management about examination conclusions, examiners should include discussions of both strengths and weaknesses of the bank's BSA/AML compliance.

Formulating Conclusions

1. Accumulate all pertinent findings from the BSA/AML examination procedures performed. Evaluate the thoroughness and reliability of any self-assessment conducted by the bank. Determine whether the following requirements are met:

    - The BSA/AML compliance program is effectively monitored and supervised in relation to the bank's risk profile.
    - The board of directors and senior management are aware of BSA/AML regulatory requirements, effectively oversee BSA/AML compliance, and commit, as necessary, to corrective actions (e.g., audit and regulatory examinations).
    - BSA/AML policies, procedures, and processes are adequate to ensure compliance with applicable laws and regulations and appropriately address high-risk operations (products, services, customers, and geographic locations).
    - Internal controls ensure compliance with the BSA and provide sufficient risk management, especially for high-risk operations (products, services, customers, and geographic locations).
    - Independent testing (audit) is appropriate and adequately tests for compliance with required laws, regulations, and policies.
    - The designated person responsible for coordinating and monitoring day-to-day compliance is competent and has the necessary resources.

- Personnel are sufficiently trained to adhere to legal, regulatory, and policy requirements.
- Information and communication policies, procedures, and processes are adequate and accurate.

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

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

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

4. Develop findings and conclusions and discuss them with the examiner in charge (EIC) or examiner responsible for reviewing the bank's overall BSA/AML compliance.

5. Identify actions needed to correct outstanding deficiencies or violations, as appropriate, including the possibility of, among other things, requiring the bank to conduct more detailed risk assessments or taking formal enforcement action.

6. Discuss findings with management and obtain a commitment for improvements or corrective action, if needed. Document these discussions.

Preparing the BSA/AML Comments for the Report of Examination

7. Draw a conclusion regarding the adequacy of the bank's BSA/AML compliance program. Discuss the effectiveness of each of these elements of the bank's BSA/AML compliance program. Indicate whether the BSA/AML compliance program meets all the regulatory requirements by providing the following:

   - A system of internal controls.
   - Independent testing for compliance.

- A specific person to coordinate and monitor the BSA/AML compliance program.
- Training of appropriate personnel.

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

The examiner should ensure that workpapers are prepared in sufficient detail to support issues discussed in the report of examination (ROE). **The examiner does not need to provide a written comment on every one of items 8 through 15, as follows.** Written comments should cover only areas or subjects pertinent to the examiner's findings and conclusions. All significant findings must be included in the ROE. To the extent that the following items are discussed in the workpapers, but not the ROE, the examiner should ensure that the workpapers thoroughly and adequately document each review, as well as any other aspect of the bank's BSA/AML compliance program that merits attention, but may not rise to the level of being included in the ROE. As applicable, the examiner should prepare a discussion of the following items.

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

9. If the bank maintains any foreign correspondent or private banking accounts, describe whether the bank's due diligence policies, procedures, and processes meet regulatory requirements under section 312 of the Patriot Act (31 USC 5318(i)).

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

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

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

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

13. If applicable, describe whether the bank's policies, procedures, and processes for Currency Transaction Report (CTR) exemptions meet regulatory reporting requirements, appropriately grant exemptions, and use the correct forms.

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

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

Preparing an Appropriate Supervisory Response

16. Identify violations and assess the severity of those violations. As appropriate, record violations in internal databases or the ROE.

17. On the basis of overall findings and conclusions, confer with the EIC to formulate appropriate ratings.

18. As appropriate, discuss recommendations for supervisory actions with the EIC, supervisory management, and legal staff.

19. Organize and reference workpapers.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Examination Procedures – Enterprise-Wide BSA/AML Compliance Program

OBJECTIVE

Assess the holding companies' and lead financial institution's[163] program for BSA/AML compliance.

PROCEDURES

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. 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 legal entities, functional lines of business, or product lines. (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 and identification of 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

[163] 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.

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 or lead financial institution board of directors, a board committees 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,[164] review the holding company's or the lead financial institution's procedures for monitoring and filing SARs. Refer to the core overview and procedures sections for "Suspicious Activity Reporting" on pages 40 and 183, respectively.

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

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

[164] 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 to file a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury, as required by 12 CFR 225.4(f). Certain savings and loan holding companies, and their non-depository subsidiaries, are required to file SARs pursuant to Treasury regulations. In addition, savings and loan holding companies, if not required, are strongly encouraged to file SARs in appropriate circumstances.

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

1. Review the policies, procedures, and processes 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. Ensure that 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 "Office of Foreign Assets Control" procedures on page 207.

TRANSACTION TESTING

5. On the basis of the bank's review of respondent accounts 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 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 individual customers to a correspondent bank for credit to the customer's account at the correspondent bank. Determine whether Currency Transaction Reports (CTRs) are properly filed.

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

1. Review the policies, procedures, and processes related to foreign correspondent financial institution account relationships. Evaluate the adequacy of the policies, procedures, and processes. Ensure that 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 client referral guidelines are covered under the contractual arrangement. If the U.S. bank does not have a standardized agreement, refer to the transaction testing 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 "Office of Foreign Assets Control" procedures on page 207.

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 as designated by the U.S. bank, including correspondent accounts for small financial institutions. From the sample selected perform the following 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with foreign correspondent financial institution relationships.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure that 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 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with U.S. dollar drafts.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure that 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 has 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 that 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 "Office of Foreign Assets Control" procedures on page 207.

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-accountholder's 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with PTAs.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure that 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 "Office of Foreign Assets Control" procedures on page 207.

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,[165] bearer securities, stored value cards, gems, art, illegal substances or contraband, or other items that should not ordinarily appear in a bank's pouch.

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

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

[165] Refer to core procedures section "International Transportation of Currency or Monetary Instruments Reporting," on page 206 for additional guidance.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

1. Review the policies, procedures, and processes related to foreign branches and offices[166] to evaluate their adequacy given the activity in relation to the bank's risk, and ensure that 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 organizational structure 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.

[166] This includes affiliates and subsidiaries.

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

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

8. Determine the involvement of the U.S. bank's head office in managing and monitoring foreign branches and offices. Conduct a preliminary evaluation of the foreign branches or offices through discussions with senior management at the U.S. bank's head office (e.g., operations, customers, 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 "Office of Foreign Assets Control" procedures on page 207.

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 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.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure that 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 "Office of Foreign Assets Control" procedures on page 207.

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 on the basis of the size, nature, and type of the transactions between the institutions.

8. On the basis of 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 arms-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.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Examination Procedures – Electronic Banking

OBJECTIVE

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

PROCEDURES

1. Review the policies, procedures, and processes related to e-banking. Evaluate the adequacy of the policies, procedures, and processes given the bank's e-banking activities and the risks they present. Ensure that 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 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 "Office of Foreign Assets Control" procedures on page 207.

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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with e-banking relationships.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure that 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 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 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.

5. Determine the bank's procedures for 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).

6. If appropriate, refer to the "Office of Foreign Assets Control" procedures on page 207.

TRANSACTION TESTING

7. 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.

8. 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.

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure that 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 "Office of Foreign Assets Control" procedures on page 207.

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 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with e-cash relationships.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure that 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 "Office of Foreign Assets Control" procedures on page 207.

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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with processor accounts.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure 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.[167]

4. If appropriate, refer to the "Office of Foreign Assets Control" procedures on page 207.

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

TRANSACTION TESTING

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

    - Monetary instrument sales records.
    - Copies of cleared monetary instruments purchased with currency.

6. From the sample selected, analyze transaction information to determine whether amounts, the frequency of purchases, and payees are consistent with expected activity for customers or noncustomers (e.g., payments to utilities, household purchases). Identify any suspicious or unusual activity.

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure that 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 "Office of Foreign Assets Control" procedures on page 207.

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), ensure that 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with deposit brokers.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure that 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.

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 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 ATM machines, 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with ISOs.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure that 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 "Office of Foreign Assets Control" procedures on page 207.

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 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with NDIP sales activities.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Examination Procedures – Insurance

OBJECTIVE

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

PROCEDURES

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 and the risks they present. Ensure that 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 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 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 "Office of Foreign Assets Control" procedures on page 207.

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 insurance products. From the sample selected, perform the following 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with insurance sales.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure that 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 "Office of Foreign Assets Control" procedures on page 207.

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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 the represent. Ensure that 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 "Office of Foreign Assets Control" procedures on page 207.

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 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with lending relationships.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

1. Review the policies, procedures, and processes related to trade finance activities. Evaluate the adequacy of the policies, procedures, and processes given the bank's trade finance activities and the risks they represent. Ensure that 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 trade finance activities, particularly those that pose a higher risk for money laundering.

3. 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.

4. If appropriate, refer to the "Office of Foreign Assets Control" procedures on page 207.

TRANSACTION TESTING

5. On the basis of the bank's risk assessment of its trade finance activities, as well as prior examination and audit reports, select a sample of trade finance accounts. From the sample selected, review documentation for unusual and suspicious activities (e.g., letters of credit and irregular pricing of goods).

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

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure that 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 conditions and to detect any inappropriate activities.

6. If appropriate, refer to the "Office of Foreign Assets Control" procedures on page 207.

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), shell corporations, and nominee accounts.
    - 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 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with private banking relationships.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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[168] services, and management's ability to implement effective due diligence, monitoring, and reporting systems.

PROCEDURES

If this is a stand-alone trust examination, refer to the core procedures section "Scoping and Planning" page 170, 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 represent. Ensure that 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

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

adequate given the bank's size, complexity, location, and types of customer relationships.

6. If appropriate, refer to the "Office of Foreign Assets Control" procedures on page 207.

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 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with trust and asset management relationships.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure that 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 on the basis of 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 the "Office of Foreign Assets Control" procedures on page 207.

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 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with NRA accounts.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Examination Procedures – Politically Exposed Persons

OBJECTIVE

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

PROCEDURES

1. Review the policies, procedures, and processes related to PEPs. Evaluate the adequacy of the policies, procedures, and processes given the bank's PEP activities and the risks they present. Ensure that controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. Review the procedures for opening PEP accounts. Identify senior management's role in the approval and ongoing 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 "Office of Foreign Assets Control" procedures on page 207.

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 procedures:

    - 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with PEPs.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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). Ensure that 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 "Office of Foreign Assets Control" procedures on page 207.

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 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with embassy and foreign consulate accounts.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure that 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 bank's size, complexity, location, and types of customer relationships.

Money Services Businesses

5. Consistent with the interagency guidance released on April 26, 2005, determine if the bank has policies, procedures, and processes in place for accounts opened or maintained for money services businesses to:

   - Confirm FinCEN registration, if required.
   - Confirm state licensing, if applicable.
   - Confirm agent status, if applicable.
   - Conduct a risk assessment to determine the level of risk associated with each account and whether further due diligence is required.

6. Determine whether the bank's policies, procedures, and processes to assess risks posed by money services business 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 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with NBFI relationships.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

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. Ensure that 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 "Office of Foreign Assets Control" procedures on page 207.

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 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with professional service provider relationships.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded 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.

PROCEDURES

1. Review the policies, procedures, and processes related to NGOs. Evaluate the adequacy of the policies, procedures, and processes given the bank's NGOs accounts and the risks they represent. Ensure that 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 "Office of Foreign Assets Control" procedures on page 207.

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 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with NGO accounts.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

Expanded Examination Procedures – Corporate Entities (Domestic and Foreign)

OBJECTIVE

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

PROCEDURES

1. Review the bank's policies, procedures, and processes related to corporate entities. Evaluate the adequacy of the policies, procedures, and processes given the bank's transactions with corporate entities and the risks they present. Ensure that 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 corporate entities. Determine whether the policies adequately assess the risk between different account types. For example, determine whether policies differentiate between U.S. corporate entities and foreign corporate entities.

3. Determine how the bank identifies and, as necessary, completes additional due diligence on corporate 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 corporate entity accounts.

5. Determine whether the bank's system for monitoring corporate entities for suspicious activities and for reporting of suspicious activities, is adequate given the activities associated with corporate entities.

6. If appropriate, refer to the "Office of Foreign Assets Control" procedures on page 207.

TRANSACTION TESTING

7. On the basis of the bank's risk assessment of its accounts with corporate entities, as well as prior examination and audit reports, select a sample of these accounts. Include the following risk factors:

- An entity incorporated 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 corporate entity whose bearer shares 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 corporate entities.
- Corporate 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 corporate 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with corporate entity relationships.

PROCEDURES FOR EVALUATING BANK SECRECY ACT ANTI-MONEY LAUNDERING COMPLIANCE

Expanded 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.

PROCEDURES

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. Ensure that 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 "Office of Foreign Assets Control" procedures on page 207.

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 procedures:

    - Review account opening documentation including Customer Identification Program 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 procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with cash-intensive businesses and entities.