Bank Secrecy Act
Anti-Money Laundering
Examination Manual

Core Overview - Customer Identification Program

OBJECTIVE

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

OVERVIEW

As of October 1, 2003, all banks and their operating subsidiaries must have a written CIP. The CIP rule implements section 326 of the Patriot Act and requires each bank to implement a written CIP that is appropriate for its size and type of business and that includes certain minimum requirements. The CIP must be incorporated into the bank's BSA/AML compliance program, which is subject to approval by the bank's board of directors.

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

- The types of accounts offered by the bank.
- The bank's methods of opening accounts.
- The types of identifying information available.
- The bank's size, location, and customer base.

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

An account does not include:

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

CUSTOMER INFORMATION REQUIRED

The CIP rule applies to a "customer." A customer is a "person" (an individual, a corporation, partnership, a trust, an estate, or any other entity recognized as a legal person) who opens a new account, an individual who opens a new account for another individual who lacks legal capacity, and an individual who opens a new account for an entity that is not a legal person (e.g., a civic club). A customer does not include a person who does not receive banking services, such as a

person whose loan application is denied. The definition of "customer" also does not include an existing customer as long as the bank has a reasonable belief that it knows the customer's true identity. Excluded from the definition of customer are federally regulated banks, banks regulated by a state bank regulator, governmental entities, and publicly traded companies (as described in 31 CFR 103.22(d)(2)(ii) through (iv)).

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

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

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

CUSTOMER VERIFICATION

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

Verification Through Documents

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

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

Verification Through Non-documentary Methods

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

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

Additional Verification for Certain Customers

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

Lack of Verification

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

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

RECORDKEEPING REQUIREMENTS AND RETENTION

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

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

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

COMPARISON WITH GOVERNMENT LISTS

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

ADEQUATE CUSTOMER NOTICE

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

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

RELIANCE ON ANOTHER FINANCIAL INSTITUTION

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

- The relied-upon financial institution is subject to a final rule implementing the AML program requirements of 31 USC 5318(h) and is regulated by a federal functional regulator.
- The customer has an account or is opening an account at the bank and at the other functionally regulated institution.
- Reliance is reasonable, under the circumstances.
- The other financial institution enters into a contract requiring it to certify annually to the bank that it has implemented its AML program, and that it will perform (or its agent will perform) the specified requirements of the bank's CIP.

USE OF THIRD PARTIES

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

OTHER LEGAL REQUIREMENTS

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

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

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 non-documentary methods.
- Accounts identified as high risk by the bank or its regulator.
- 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)).
- 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 SAR', 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.

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.

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.

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.

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 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.
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.

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.

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 non-customers. 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.

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.

Expanded Examination Procedures – Non-deposit Investment Products

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with both networking and in-house non-deposit 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 customers 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.

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 (non-depositors).
   - If so, determine whether the bank maintains the required records for sales of monetary instruments to non-depositors.
   - 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.