Bank Secrecy Act / Anti-Money Laundering Examination Manual

Customer Identification Program — Overview

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

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

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

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

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

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

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

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

An account does not include:

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

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

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

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

Customer Information Required

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

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

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

Customer Verification

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

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

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

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

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

Verification Through Documents

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

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

Verification Through Nondocumentary Methods

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

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

Additional Verification for Certain Customers

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

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

Lack of Verification

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

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

Recordkeeping 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.[49] For credit cards, the retention period is five years after the account closes or becomes dormant.

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

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

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

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

Comparison with Government Lists

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

Adequate Customer Notice

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

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

Reliance on Another Financial Institution

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

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

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

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

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

Use of Third Parties

The CIP rule does not alter a bank's authority to use a third party, such as an agent or service provider, to perform services on its behalf. Therefore, a bank is permitted to arrange for a third party, such as a car dealer or mortgage broker, acting as its agent in connection with a loan, to verify the identity of its customer. The bank can also arrange for a third party to maintain its records. However, as with any other responsibility performed by a third party, the bank is ultimately responsible for that third party's compliance with the requirements of the bank's CIP. As a result, banks should establish adequate controls and review procedures for such relationships. This requirement contrasts with the reliance provision of the rule that permits the relied-upon party to take responsibility. Refer to "Reliance on Another Financial Institution," page 50.

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 (FAQs), which may be revised periodically. The FAQs and other related documents (e.g., the CIP rule) are available on FinCEN's and the federal banking agencies' web sites.

Examination Procedures

Customer Identification Program

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

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

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

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

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

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

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

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

Transaction Testing

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

   - Accounts opened for a customer that provides an application for a TIN or accounts opened with incomplete verification procedures.
   - New accounts opened using documentary methods and new accounts opened using nondocumentary methods.
   - Accounts identified as high risk.[52]
   - 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 new accounts, determine whether the bank has performed the following procedures:

   - Opened the account in accordance with the requirements of the CIP (31 CFR 103.121(b)(1)).
   - Formed a reasonable belief as to the true identity of a customer, including a 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)).

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

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

9. Evaluate the level of CIP exceptions to determine whether the bank is effectively implementing its CIP. A bank's policy may not allow staff to make or approve CIP exceptions. However, a bank may exclude isolated, 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 retain the identity information obtained at account opening for five years after the account closes. The bank must also maintain a description of documents relied on, methods used to verify identity, and resolution of discrepancies for five years after the record is made (31 CFR 103.121(b)(3)(ii)).

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