CUSTOMER IDENTIFICATION PROGRAM

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

Regulatory Requirements for Customer Identification Programs

This section outlines the regulatory requirements for banks in 12 CFR Chapters I through III and VII, and 31 CFR Chapter X regarding CIPs. Specifically, this section covers:

- 12 CFR 21.21(c)(2)
- 12 CFR 208.63(b)(2), 12 CFR 211.5(m)(2), 12 CFR 211.24(j)(2)
- 12 CFR 326.8(b)(2)
- 12 CFR 748.2(b)(2)
- 31 CFR 1020.220

A bank, including certain domestic subsidiaries,[1] must have a written CIP[2] 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,[3] which is subject to approval by the bank's board of directors.[4] Minor weaknesses, deficiencies, and technical violations alone are not indicative of an inadequate CIP.

Identity Verification Procedures

The CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable.[5] The procedures must enable the bank to form a reasonable belief that it knows the true identity of each customer and be based on the bank's assessment of relevant risks, including:

- The types of accounts maintained by the bank.
- The bank's methods of opening accounts.

---

[1] *See* OCC 12 CFR 5.34(e)(3) and 5.38(e)(3) (examination and supervision of operating subsidiaries of national banks and federal savings associations). *See also* FinCEN, Federal Reserve, FDIC, NCUA, OCC, OTS, Treasury (April 28, 2005), "Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act," Definition of "bank" FAQ #3. The FDIC will evaluate each subsidiary relationship in the context of the bank's safety and soundness before determining whether the CIP applies to the bank's subsidiaries. Wholly- or majority-owned credit union service organizations (CUSOs) may be considered subsidiaries of the credit union owner; however, as separate legal entities, the NCUA has no direct regulatory authority over CUSOs.

[2] 12 CFR 208.63(b)(2), 211.5(m)(2), and 211.24(j)(2) (Federal Reserve); 12 CFR 326.8(b)(2) (FDIC); 12 CFR 748.2(b)(2) (NCUA); 12 CFR 21.21(c)(2) (OCC); and 31 CFR 1020.220 (FinCEN).

[3] 12 CFR 208.63(b)(2), 211.5(m)(2), and 211.24(j)(2) (Federal Reserve); 12 CFR 326.8(b)(2) (FDIC); 12 CFR 748.2(b)(2) (NCUA); 12 CFR 21.21(c)(2) (OCC); and 31 CFR 1020.220 (FinCEN).

[4] 12 CFR 208.63(b), 211.5(m), and 211.24(j) (Federal Reserve); 12 CFR 326.8(b) (2) (FDIC); 12 CFR 748.2(b) (NCUA); 12 CFR 21.21 (OCC).

[5] 31 CFR 1020.220(a)(2).

- The types of identifying information available.
- The bank's size, location, and customer base.[6]

For purposes of the CIP rule, an "account" is a formal banking relationship established to provide or engage in services, dealings, or other financial transactions, including a deposit account, a transaction or asset account, a credit account, or other extension of credit. An account includes a relationship established to provide a safety deposit box or other safekeeping services, or cash management, custodian, and trust services.[7]

An account does not include:[8]

- A product or service where a formal banking relationship is not established with a person, such as check-cashing, wire transfer, or sale of a check or money order;
- An account that the bank acquires through an acquisition, merger, purchase of assets, or assumption of liabilities; or
- An account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974.

The CIP rule applies to a customer,[9] which means:

- A person that opens a new account; and
- An individual who opens a new account for:
    - An individual who lacks legal capacity, such as a minor; or
    - An entity that is not a legal person, such as 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[10] or a person that has an existing account with the bank, provided that the bank has a reasonable belief that it knows the true identity of the person.[11] Also excluded from the definition of customer are financial institutions regulated by a federal functional regulator or a bank regulated by a state bank regulator, governmental entities, and publicly traded companies as described in 31 CFR 1020.315(b)(2) through (b)(4).[12]

---

[6] *Id*.
[7] 31 CFR 1020.100(a)(1).
[8] 31 CFR 1020.100(a)(2).
[9] 31 CFR 1020.100(b).
[10] FinCEN, Federal Reserve, FDIC, NCUA, OCC, OTS, Treasury (April 28, 2005), "Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act," Definition of "account" FAQ #1.
[11] 31 CFR 1020.100(b)(2)(iii). FinCEN, Federal Reserve, FDIC, NCUA, OCC, OTS, Treasury (April 28, 2005), "Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act," Person with an existing account FAQ #3. A bank can demonstrate that it has "a reasonable belief" by showing that prior to the issuance of the final CIP rule, it had comparable procedures in place to verify the identity of persons that 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.
[12] 31 CFR 1020.100(b)(2).

Customer Information Required

The CIP must contain account-opening procedures detailing the identifying information to obtain from each customer.[13] At a minimum, the bank must obtain the following identifying information from each customer before opening the account:

- Name,
- Date of birth for an individual,
- Address,[14] and
- Identification number.[15]

The CIP rule provides for an exception for opening an account for a customer who has applied for a tax identification number (TIN) and an alternative process for obtaining CIP identifying information for credit card accounts.

- The exception permits the bank to open an account for a customer who has applied for a TIN, but does not yet have a TIN. In this case, the bank's CIP must include procedures to confirm that the application was filed before the customer opens the account and to obtain the TIN within a reasonable period of time after the account is opened.[16]
- For a credit card account, the bank may also obtain CIP identifying information about the customer by acquiring it from a third-party source prior to extending credit to the customer.[17]

[13] 31 CFR 1020.220(a)(2)(i). Given the definition of customer, 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. In 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, as this person is defined as the customer.

[14] 31 CFR 1020.220(a)(2)(i)(A)(3). 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, or the residential or business street address of next of kin or of another contact individual. 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. FinCEN, Federal Reserve, FDIC, NCUA, OCC, OTS, Treasury (April 28, 2005), "Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act," Information required FAQ #1, further explains that for an individual, the description of the customer's physical location will suffice.

[15] An identification number for a U.S. person is a taxpayer identification number (TIN) (or evidence of an application for one consistent with 31 CFR 1020.220(a)(2)(i)(B)). An identification number for a non-U.S. person is one or more of the following: a TIN (or evidence of an application for one consistent with 31 CFR 1020.220(a)(2)(i)(B)); a passport number and country of issuance; an alien identification card number; or a number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard. When opening an account for a foreign business or enterprise that does not have an identification number, the bank must request alternative government-issued documentation certifying the existence of the business or enterprise. TINs are described in section 6109 of the Internal Revenue Code (26 USC 6109) and the IRS regulations implementing that section (26 CFR Part 301.6109-1) (e.g., Social Security number (SSN), individual taxpayer identification number (ITIN), or employer identification number (EIN)).

[16] 31 CFR 1020.220(a)(2)(i)(B).

[17] 31 CFR 1020.220(a)(2)(i)(C).

Based on its BSA/AML risk assessment, a bank may require identifying information, in addition to the required information, for certain customers or product lines.[18]

Customer Verification

The CIP must contain risk-based[19] procedures for verifying the identity of the customer within a reasonable period of time after the account is opened.[20] The verification procedures must use the "information obtained in accordance with [31 CFR 1020.220(a)(2)(i)]," namely the identifying information obtained by the bank.[21] 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.[22] The bank's procedures must describe when it uses documents, non-documentary methods, or a combination of both methods to verify the identity of its customers.[23]

Verification Through Documents

A bank relying on documents to verify a customer's identity must have procedures that set forth the documents that the bank will use.[24] The CIP rule gives examples of the types of documents that may be used to verify a customer's identity. The rule reflects the federal banking agencies' expectations that, for most customers who are individuals, banks review an unexpired government-issued form of identification evidencing a customer's nationality or residence and bearing 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. Given the availability of counterfeit and fraudulently obtained documents, a bank is encouraged to review more than a single document to ensure it can form a reasonable belief that it knows the true identity of the customer.

For a person other than an individual (such as a corporation, partnership, or trust), documents may include those 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.[25]

Verification Through Non-Documentary Methods

A bank using non-documentary methods to verify a customer's identity must have procedures that set forth the methods the bank uses.[26] Non-documentary methods may include contacting a customer; independently verifying the customer's identity through the comparison of information

[18] FinCEN, Federal Reserve, FDIC, NCUA, OCC, OTS, Treasury (April 28, 2005), "Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act," Definition of "customer" FAQs #7, 9, 10.
[19] 31 CFR 1020.220(a)(2).
[20] 31 CFR 1020.220(a)(2)(ii).
[21] *Id.*
[22] FinCEN, Federal Reserve, FDIC, NCUA, OCC, OTS, Treasury (April 28, 2005), "Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act," Customer verification FAQ #1.
[23] 31 CFR 1020.220(a)(2)(ii).
[24] 31 CFR 1020.220(a)(2)(ii)(A).
[25] 31 CFR 1020.220(a)(2)(ii)(A)(2).
[26] 31 CFR 1020.220(a)(2)(ii)(B).

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.[27]

If the bank uses non-documentary methods to verify a customer's identity, the bank's procedures must address situations in which 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; the customer opens the account without appearing in person at the bank; and where the bank is otherwise presented with circumstances that increase the risk that the bank will be unable to verify the true identity of a customer through documents.[28]

Additional Verification for Certain Customers

The CIP must address situations in which, 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 account, 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 documents or non-documentary methods.[29]

Lack of Verification

The CIP must also have procedures[30] for responding to circumstances in which the bank cannot form a reasonable belief that it knows the true identity of the customer. These procedures should describe:

- When 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; and
- When the bank should file a suspicious activity report (SAR) in accordance with applicable law and regulation.

Recordkeeping and Retention Requirements

The bank's CIP must include procedures for making and maintaining a record of all information obtained to identify and verify a customer's identity.[31] At a minimum, the bank must retain all identifying information (name, date of birth for an individual, address, identification number, and

[27] 31 CFR 1020.220(a)(2)(ii)(B)(1).
[28] 31 CFR 1020.220(a)(2)(ii)(B)(2).
[29] 31 CFR 1020.220(a)(2)(ii)(C).
[30] 31 CFR 1020.220(a)(2)(iii).
[31] 31 CFR 1020.220(a)(3).

any other identifying information obtained under 31 CFR 1020.220(a)(2)(i)[32]) at account opening for CIP purposes for a period of five years after the account is closed. For credit cards, the retention period is five years after the account is closed or becomes dormant.[33]

A bank may keep copies of identifying documents that it uses to verify a customer's identity; however, the CIP rule does not require it. A bank's verification procedures must 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. If the bank retains copies of identifying documents in lieu of a description, these documents must be retained in accordance with the general recordkeeping requirements in 31 CFR 1010.430, "Nature of Records and Retention Period." Nonetheless, a bank should not improperly use any document containing a picture of an individual, such as a driver's license, in connection with any aspect of a credit transaction.[34]

The bank must also keep a description of the following for five years after the record is made:[35]

- Any document that was relied on to verify identity, noting the type of document, any identification number contained in the document, the place of issuance, and, if any, the date of issuance and expiration date;
- The methods and the results of any measures undertaken to verify the identity of the customer using non-documentary methods or additional verification procedures for certain customers; and
- The resolution of any substantive discrepancy discovered when verifying the identifying information obtained.

Comparison with Government Lists

The CIP must include procedures for determining whether the customer appears on any list of known or suspected terrorists or terrorist organizations issued by any federal government agency and designated as such by Treasury in consultation with the federal functional regulators.[36] The procedures must require the bank to make such a determination within a reasonable period of time after the account is opened, or earlier, if required by another federal law or regulation or federal directive issued in connection with the applicable list. The procedures must also require the bank to follow all federal directives issued in connection with such lists.[37] Banks will

[32] FinCEN, Federal Reserve, FDIC, NCUA, OCC, OTS, Treasury (April 28, 2005), "Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act," Retention of records FAQ #2.
[33] 31 CFR 1020.220(a)(3).
[34] FinCEN, Federal Reserve, FDIC, NCUA, OCC, OTS, Treasury (April 28, 2005), "Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act," Required records FAQ #2.
[35] 31 CFR 1020.220(a)(3)(i)(B)-(D).
[36] 31 CFR 1020.220(a)(4).
[37] *Id*.

receive notification by way of separate guidance regarding the list that must be consulted for purposes of this provision.[38]

As of the publication date of this Manual, no designated government lists for CIP purposes exist. Checking of customers against Office of Foreign Assets Control (OFAC) lists and 31 CFR 1010.520 (commonly referred to as section 314(a) requests) remain separate and distinct requirements.

Adequate Customer Notice

The CIP must include procedures for providing bank customers with adequate notice that the bank is requesting information to verify their identities.[39] Notice is adequate if the bank generally describes the identification requirements of the CIP rule and provides the notice in a manner reasonably designed to ensure that a customer is able to view or otherwise receive the notice before the account is opened.[40] Depending on the manner in which an account is opened, examples of adequate notice may include posting a notice in the lobby or on the bank's website, including a notice with account application documents, or providing other written or oral notice. The sample language below is provided in the regulation:[41]

> **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

The bank's CIP may include procedures specifying when a bank will rely on the performance by another financial institution (including an affiliate) of any procedures of the bank's CIP with respect to any customer of the bank that is opening, or has opened, an account or has established a similar formal banking or business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions, provided that:

- Such reliance is reasonable under the circumstances;
- The other, relied-upon financial institution is subject to a rule implementing 31 USC 5318(h) and is regulated by a federal functional regulator;[42] and

[38] OCC, Federal Reserve, FDIC, OTS, NCUA, FinCEN (May 9, 2003), "Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks," 68 Fed. Reg. 25090, 25103.
[39] 31 CFR 1020.220(a)(5)(i).
[40] 31 CFR 1020.220(a)(5)(ii).
[41] 31 CFR 1020.220(a)(5)(iii).
[42] 31 CFR 1010.100(r). Federal functional regulator means: Federal Reserve, FDIC, NCUA, OCC, U.S. Securities and Exchange Commission (SEC), or U.S. Commodity Futures Trading Commission (CFTC).

- 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.[43]

Exemptions

The appropriate federal functional regulator, with the concurrence of FinCEN on behalf of the Secretary of the Treasury, may, by order or regulation, exempt any bank or type of account from the requirements of this section.[44] The federal banking agencies, with FinCEN's concurrence, have granted a CIP exemption for loans extended by banks and their subsidiaries to all customers to facilitate purchases of property and casualty insurance policies (referred to as premium finance loans).[45] The federal banking agencies found that the exemption is consistent with the purposes of the BSA, based on FinCEN's determination that premium finance loans present a low risk of money laundering or terrorist financing (ML/TF), and that this exemption is consistent with safe and sound banking.

Other Legal Requirements

Nothing in the CIP rule relieves a bank of its obligation to comply with any other provision of the BSA, including provisions concerning information that must be obtained, verified, or maintained in connection with any account or transaction.[46]

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 may 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.[47] The bank can also arrange for a third party to maintain its records. However, as with other responsibilities performed by a third party, the bank is ultimately responsible for compliance with the requirements of the CIP rule. Examiners should refer to their agency's relevant guidance and requirements for such third-party relationships.[48]

---

[43] 31 CFR 1020.220(a)(6).
[44] 31 CFR 1020.220(b).
[45] Federal Reserve, FDIC, NCUA, OCC, FinCEN (October 5, 2020), "Order granting an exemption from customer identification program requirements implementing section 326 of the USA PATRIOT Act, 31 U.S.C. 5318(l), for loans extended by banks (and their subsidiaries) subject to the jurisdiction of the Federal Banking Agencies to all customers to facilitate purchases of property and casualty insurance policies."
[46] 31 CFR 1020.220(c).
[47] Such third-party arrangements are contemplated in FinCEN, Federal Reserve, FDIC, NCUA, OCC, OTS, Treasury (April 28, 2005), "Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act," Customer notice FAQ #2.
[48] Federal Reserve (December 5, 2013), SR 13-19 "Guidance on Managing Outsourcing Risk." FDIC (June 6, 2008), FIL-44-2008 "Guidance for Managing Third-Party Risk." NCUA (December 2007), "Evaluating Third Party Relationships." OCC (October 30, 2013), Bulletin 2013-29 "Third Party Relationships: Risk Management Guidance;" and OCC (March 5, 2020), Bulletin 2020-10 "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29."

Additional Resources

The U.S. Department of the Treasury, FinCEN, and the federal banking agencies have issued Frequently Asked Questions (FAQs), which may be revised periodically.[49] FinCEN and the federal banking agencies have issued interagency guidance to issuing banks on applying CIP requirements to holders of prepaid cards.[50] There is also guidance encouraging banks to use non-documentary verification methods permitted by the CIP requirements for customers who cannot provide standard identification documents because of the effects of natural disasters.[51] The FAQs, guidance, exceptive relief, and other related documents (e.g., the CIP rule) are available on the websites of FinCEN and the federal banking agencies.

Examiner Assessment of the CIP Process

Examiners should assess the adequacy of the bank's policies, procedures, and processes (internal controls) related to the bank's CIP. Specifically, examiners should determine whether these internal controls are designed to mitigate and manage ML/TF and other illicit financial activity risks and comply with CIP requirements. Examiners may review other information, such as recent independent testing or audit reports, to aid in their assessment of the bank's CIP.

Examiners should also consider general internal controls concepts, such as dual controls, segregation of duties, and management approval for certain actions, as they relate to the bank's CIP. Other internal controls may include BSA compliance officer or other senior management approval for staff actions that deviate from the bank's CIP policies, procedures, and processes. When assessing internal controls and CIP compliance, examiners should keep in mind that the bank may have limited instances of noncompliance with the CIP rule (such as isolated or technical violations) or minor deviations from the bank's CIP policies, procedures, and processes without resulting in an inadequate CIP.

Examiners should determine whether the bank's internal controls for CIP are designed to assure ongoing compliance with the requirements and are commensurate with the bank's size or complexity and organizational structure. More information can be found in the *Assessing the BSA/AML Compliance Program - BSA/AML Internal Controls* section of this Manual.

[49] FinCEN, Federal Reserve, FDIC, NCUA, OCC, OTS, Treasury (April 28, 2005), "Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act."
[50] Federal Reserve, FDIC, FinCEN, NCUA, and OCC (March 21, 2016), "Interagency Guidance to Issuing Banks on Applying Customer Identification Program Requirements to Holders of Prepaid Cards."
[51] FDIC (August 29, 2017), FIL-38-2017 "Meeting the Financial Needs of Customers Affected by Hurricane Harvey and its Aftermath." Federal Reserve (March 29, 2013), SR 13-6 "Supervisory Practices Regarding Banking Organizations and their Borrowers and Other Customers Affected by a Major Disaster or Emergency." NCUA (December 14, 2017), SL No. 17-02 "Examiner Guidance for Institutions Affected by a Major Disaster." OCC (November 14, 2012), NR 2012-164 "Agencies Issue Supplemental Statement on Supervisory Practices Regarding Financial Institutions and Borrowers Affected by Hurricane Sandy."

CUSTOMER IDENTIFICATION PROGRAM EXAMINATION AND TESTING PROCEDURES

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

1. Verify that the bank has a written CIP appropriate for its size and type of business. The written program must be included within the bank's BSA/AML compliance program and must contain procedures that address:

   - Obtaining the required identifying information (including name, date of birth for an individual, address, and identification number).
   - Verifying the identity of each customer to the extent reasonable and practicable through risk-based procedures.
   - Responding to circumstances in which the bank cannot form a reasonable belief that it knows the true identity of a customer, including determining when a suspicious activity report (SAR) should be filed.
   - Complying with recordkeeping requirements.
   - Timely checking of new accounts against prescribed government lists, if applicable.
   - Providing adequate customer notice.
   - Relying on another financial institution that has an AML compliance program and is regulated by a federal functional regulator, if applicable.

2. Verify that the bank establishes appropriate controls and review procedures for its relationships with third parties, if applicable. If the bank is using a third party, such as an agent or service provider, to perform elements of its CIP, determine whether the bank has procedures in place to monitor for and ensure adequate performance.

3. Determine whether the bank's CIP appropriately considers the types of accounts maintained; methods of account opening; the types of identifying information available; and the bank's size, location, and customer base.

4. 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 as indicated by the bank's risk assessment (e.g., consumers and businesses, loans and deposits, credit card relationships, and accounts opened via U.S. mail and online). The sample should also, on a risk basis, include the following:

   - New accounts opened using the exception for customers that have applied for a TIN.
   - New accounts opened using documentary methods, and new accounts opened using non-documentary methods.
   - New accounts identified by the bank as higher risk.

- New accounts opened with incomplete verification information, if applicable.
- New accounts opened by a third party as the bank's agent (e.g., indirect loans), if applicable.

5. From the previous sample of new accounts, determine whether the bank has performed the following procedures:
   - Opened the account in accordance with the bank's policies, procedures, and processes for CIP.
   - Obtained from each customer, before opening the account, the identifying information required by the CIP: name, date of birth (for an individual), address, and identification number.
   - Verified the identity of the customer at account opening, or within a reasonable time after account opening, to the extent reasonable and practicable.
   - Appropriately resolved situations in which customer identity could not be reasonably verified and filed SARs, as appropriate.
   - Made and maintained a record of the identifying information required by the CIP regulations; a description of any document that was relied upon to verify identity; the methods and results of any measures undertaken to verify identity using non-documentary methods or additional verification procedures; and verification results (including results of substantive discrepancies).
   - Compared the customer's name against any list of known or suspected terrorists or terrorist organizations, if applicable.
6. Review the adequacy of the bank's customer notice and the timing of the notice's delivery.
7. If the bank relies on other financial institutions to perform its CIP (or portions of its CIP), select a sample of new accounts opened under the reliance provision.
   - Determine whether the bank's customer is opening or has opened an account at, or has established a similar formal banking or business relationship with, the other financial institution to provide or engage in services, dealings, or other financial transactions.
   - Determine whether the other 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.
   - Review the contract between the parties, annual certifications, and other information, such as the other financial institution's CIP.
   - Determine whether reliance is reasonable. The contract and certification 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 other financial institution has been subject to an enforcement action for AML or BSA deficiencies or violations).

8. Review the internal controls in place for CIP. Determine whether the bank's internal controls are designed to assure ongoing compliance with CIP requirements and are commensurate with the bank's size or complexity and organizational structure.

9. Review any identified instances of noncompliance with the CIP rule and any deviations from the bank's CIP policies, procedures, and processes to determine whether the bank is effectively implementing its CIP. In making this determination, examiners should keep in mind that the bank may have limited instances of noncompliance with the CIP rule (such as isolated or technical violations) or minor deviations from the bank's CIP policies, procedures, and processes without resulting in an inadequate CIP.

10. On the basis of examination and testing procedures completed, form a conclusion about the adequacy of policies, procedures, and processes the bank has developed to meet BSA regulatory requirements associated with CIP.