Customer Identification Program Examination and Testing Procedures

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

| **Procedure** | **Comments** |
| --- | --- |
| 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.
 |  |
| 1. 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.
 |  |
| 1. 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.
 |  |
| 1. 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.
 |  |
| 1. 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.
 |  |
| 1. Review the adequacy of the bank’s customer notice and the timing of the notice’s delivery.
 |  |
| 1. 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).
 |  |
| 1. 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.
 |  |
| 1. 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.
 |  |
| 1. 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.
 |  |