**Office of Thrift Supervision**
Department of the Treasury *Managing Director, Examinations, Supervision, and Consumer Protection*
1700 G Street, N.W., Washington, DC 20552 • (202) 906-7984

July 27, 2004

**MEMORANDUM FOR:** **CHIEF EXECUTIVE OFFICERS**

**FROM:** Scott M. Albinson

**SUBJECT:** Bank Secrecy Act/USA PATRIOT Act Examination Procedures—Customer Identification Programs

The USA PATRIOT Act (the Act) became law on October 26, 2001. The Act contains strong new measures to prevent, detect and prosecute terrorist financing and money laundering. Congress enacted the measures directly affecting savings associations as amendments to the Bank Secrecy Act (BSA) (31 CFR Part 103). A regulation implementing section 326 (Customer Identification Programs) (CIP) became effective October 1, 2003 (31 CFR 103.121). The implementing regulation requires each savings association to implement a written CIP appropriate for its size, location, and type of business that includes certain minimum requirements. The CIP must be incorporated into a savings association's anti-money laundering compliance program, which is subject to approval by the association's board of directors.

We have attached examination procedures to evaluate savings associations' compliance with the new CIP requirements. The procedures were developed in consultation with the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Comptroller of the Currency, and the National Credit Union Association. In addition, the procedures were designed to assist associations to implement the new requirements and facilitate a consistent supervisory approach among the banking agencies.

OTS is available to assist savings associations with the new requirements and procedures, and questions may be directed to your regional supervisory office. These and other BSA/USA PATRIOT Act resources are available at www.ots.treas.gov/bsa. Savings associations should also feel free to call our BSA/USA PATRIOT Act Hotline at (202) 906-6012.

Attachment

July 2004

# Bank Secrecy Act Examination Procedures for Customer Identification Programs

## Introduction

The Customer Identification Program (CIP) regulation,[1] 31 CFR 103.121, applies to federally regulated banks and savings associations (including Edge Act and Agreement corporations, and branches and agencies of foreign banks in the United States), credit unions, and nonfederally regulated private banks, trust companies, and credit unions (hereinafter, a bank or banks). All banks were required to comply with the CIP regulation for all accounts established on or after October 1, 2003.

31 CFR 103.121 implements section 326 of the USA PATRIOT Act and requires each bank to implement a written CIP appropriate for its size and type of business that includes certain minimum requirements. The CIP must be incorporated into the bank's anti-money-laundering compliance program, which is subject to approval by the bank's board of directors.[2]

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. These procedures must enable the bank to form a reasonable belief that it knows the true identity of each customer. Banks should conduct a risk assessment of their customer base and product offerings, and in determining the risks, consider the following factors:

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

An "account" pursuant to the CIP rule 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 other extension of credit. An account also includes a relationship established to provide a safe deposit box or other safekeeping services, or cash management, custodian, and trust services.

[1] The regulation was issued jointly by the Department of the Treasury, through the Financial Crimes Enforcement Network (FinCEN), together with the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, and the National Credit Union Administration (collectively, the agencies).

[2] Nonfederally regulated private banks, trust companies, and credit unions do not have anti-money-laundering program requirements; however, the institution's board must still approve the CIP.

An account does not include:

- Products or services 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;

- 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; and

- Accounts 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." A customer is a "person" (individual, corporation, partnership, or trust) 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.[3] 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.[4] In addition, excluded from the definition of "customer" are federally regulated financial institutions, banks regulated by a state bank regulator, governmental entities, and publicly traded companies (as described in 31 CFR 103.22(d)(2)(ii)-(iv)).

### *Customer Information Required*

The CIP must contain account-opening procedures detailing the identifying information it must obtain from each customer.[5] At a minimum, the bank must obtain the following basic information from the customer prior to opening the account[6]:

- Name;

- Date of birth, for individuals;

---

[3] 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.

[4] The bank may do so by showing that prior to 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, evidenced by such things as a history of account statements sent to the person, information sent to the IRS about the person's accounts without issue, loans made and repaid, or other services performed for the person over a period of time. This alternative, however, may not suffice for persons that the bank has deemed to be high risk.

[5] 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 should 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 behalf of whom the account is being opened.

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

- Address;[7] and
- Identification number.[8]

Based on its assessment of risk, 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, "using the information obtained in accordance with 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. The policy must also describe the documents it will use.

#### *Verification Through Documents*

A bank using documentary methods to verify a customer's identity must have procedures that set forth the documents that the bank will use. The CIP rule gives examples of types of documents that have long been considered primary sources of identification and reflects the agencies' expectations that banks will obtain an unexpired government-issued form of identification from most customers evidencing nationality or residence and bearing a photograph or similar safeguard, such as 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 obtain 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 that the bank will use. Nondocumentary methods may include contacting a customer;

---

[7] For an individual: a residential or business street 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.

[8] An identification number for a U.S. person is a taxpayer identification number (TIN) (or evidence of an application for one), and for a non-U.S. person is one or more of the following: a TIN; passport number and country of issuance; alien identification card number; or 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 U.S.C. 6109) and the Internal Revenue Service regulations implementing that section (e.g., social security number or employer identification number).

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 situations where 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 subsequently verify it); 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.

*Additional Verification*

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 the 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 that respond to 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; and
- When the bank should file a Suspicious Activity Report (SAR) in accordance with applicable law and regulation.

***Recordkeeping Requirements and Retention***

The CIP must include recordkeeping procedures. At a minimum, the bank must retain the identifying information (name, address, date of birth for an individual, tax identification number (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 upon 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 terrorist or terrorist organizations.[9] Banks will be contacted by Treasury in consultation with their functional regulator when a list is issued. At such time when a list is issued, 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 describe generally the bank's identification requirements and must be provided in a manner that is reasonably designed so that a customer is able to view it or is otherwise given notice prior to account opening. Sample language as follows 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 it is addressed in the CIP and the following criteria are met:

- The relied-upon financial institution is subject to an anti-money-laundering program rule (31 USC 5318(h)) and is regulated by a federal functional regulator.[10]

- The customer has an account at the bank and the other functionally regulated financial 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 anti-money-laundering program, and that it will perform (or its agent will perform) the specified requirements of the bank's CIP.

[9] As of the date of these procedures, there are no designated government lists to verify specifically for CIP purposes. Customer comparisons to lists required by the Office of Foreign Assets Control (OFAC) and the USA PATRIOT Act section 314(a) requests remain separate and distinct requirements.

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

### *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, for example, to arrange for a car dealer or mortgage broker, acting as its agent in connection with a loan, to verify the identity of its customer, or it can arrange for a third party to maintain its records. However, as with any other responsibility performed by a third party the bank ultimately is 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 is in contrast with the reliance provision of the rule, which 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 Bank Secrecy Act or other anti-money-laundering rules, particularly with respect to provisions concerning information that must be obtained, verified, or maintained in connection with any account or transaction.

The Department of Treasury and the agencies have provided financial institutions with Frequently Asked Questions (FAQs). Please note that this document may be revised periodically. The reader can find this and other related documents (e.g., the CIP rule) on FinCEN's Web site: http://www.fincen.gov.

## Request Letter Items

It is suggested that examiners request the following items to facilitate the examination. Of interest are items since the last Bank Secrecy Act (BSA)/Anti-Money-Laundering (AML) examination or the Customer Identification Program (CIP) regulation's required compliance date (October 1, 2003).

1. A copy of the bank's CIP that covers all of its products and services and all the requirements, as set forth in the regulation.

2. A written description of the bank's rationale for exempting existing customers from its CIP.

3. A copy of the board minutes approving the CIP (or approving the BSA program that includes the CIP).

4. A copy of the bank's audit procedures and a copy of any audit reports covering the bank's CIP.

5. A copy of the bank's CIP training program (or BSA training program, if it includes the CIP program).

6. A list of new accounts covering all product lines (including accounts opened by third parties) and segregating existing customer accounts from new customers for [examiner to insert a period of time appropriate for the size/complexity of the bank].

7. A list of any accounts opened with an application for a tax identification number (TIN).

8. A list of any accounts opened where verification has not been completed or opened with exceptions to the CIP (making or approving exceptions cannot be allowed by policy; however, isolated, nonsystemic errors (such as an insignificant number of data entry errors) may be deemed as not compromising the program's effectiveness).

9. A list of accounts identified as high risk for CIP by the bank (for example, foreign private banking and trust accounts, accounts of senior foreign political officials, offshore accounts, and out-of-area and non-face-to-face accounts).

10. A copy of the customer notice(s) and description of its timing and delivery, by product.

11. If the bank is using the "reliance provision" to rely on another financial institution to perform some or all of its CIP on any new accounts, indicate the name of the institution, designate if the institution is subject to a rule implementing the AML compliance program requirements of 31 USC 5318(h) and is regulated by a federal functional regulator. Provide the following: copies of any contracts signed between the parties, a copy of the CIP or procedures used by the other party, and any certifications made by the other party.

12. If the bank is using a third party such as an agent or service provider to perform some or all of its CIP on any new accounts, indicate the name of the party, a copy of any contracts signed between the parties, a copy of the CIP or procedures used by the other party, and the bank's policies and procedures for ensuring adequate performance by the third party.

## Examination Procedures

In accordance with agency guidelines, examiners should determine which procedures should be completed by focusing on the areas of particular risk. Examiners should base the selection of procedures on the adequacy of the bank's compliance management system and level of risk identified. Examiners may complete the procedures in two phases in large, complex banks (evaluating policies and audit first, followed by the remaining procedures). The procedures outlined below are designed to help examiners determine whether banks have implemented adequate CIPs to comply with this regulation.

1. Evaluate the bank's CIP to ensure that it addresses the regulatory requirements. Determine whether the bank performed a risk analysis, taking into consideration the types of accounts offered, methods of account opening, and the bank's size, location, and customer base. Determine also if it designed an appropriate program. The program should be in writing and included within the bank's BSA program (12 CFR 563.177). The program should include, at a minimum, the following:

    a) Procedures for obtaining the required identifying information (including name, address, TIN, and date of birth for individuals) and risk-based identity verification procedures (including procedures that address situations where verification cannot be performed).

    b) Procedures for complying with recordkeeping requirements.

    c) Procedures for checking new accounts against prescribed government lists, if applicable.

    d) Procedures for providing adequate customer notice.

    e) Procedures covering reliance on another financial institution or another third party, if applicable.

    f) Procedures for determining whether and when a SAR(s) should be filed.

    g) Adequate internal controls, training, and procedures to ensure that the financial institution monitors and independently tests its compliance with the regulation.

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

3. Unless reviewed during the BSA program examination (12 CFR 563.177), review minutes and verify that the board approved the CIP, either separately or as part of the BSA program (31 CFR 103.121(b)(1); 12 CFR 563.177(b)(2)).

4. Evaluate the bank's audit and training programs to ensure that the CIP is adequately incorporated (31 CFR 103.121(b)(1); 12 CFR 563.177(b)(2)).

5. Evaluate the bank's systems and controls to check all new accounts against prescribed government lists for suspected terrorists or terrorist organizations on a timely basis in the event such lists are issued (31 CFR 103.121(b)(4)).

6. Based on 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*

   a) Opened with an application for a TIN or opened with incomplete verification procedures,

   b) Opened using documentary methods and accounts opened using nondocumentary methods,

   c) Identified as high risk by the bank or the regulator[11],

   d) Opened by existing high-risk customers,

   e) Opened with exceptions, and

   f) Opened by a third party (e.g., indirect loans).

7. From the above sample of accounts, determine whether the bank:

   a) Opened the account in accordance with the requirements of the CIP (31 CFR 103.121(b)(1)).

   b) Formed a reasonable belief as to the customer's true identity, including high-risk customers, or had already done so on an existing customer (31 CFR 103.121(b)(2)).

   c) Obtained from each customer, prior to opening the account, the identity information required by the CIP (31 CFR 103.121(b)(2)(i)).

   d) Verified, within a reasonable time of account opening, 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)).

[11] High-risk accounts may include for example, foreign private banking and trust accounts, accounts of senior foreign political officials, offshore accounts, and out-of-area and non-face-to-face accounts.

e) Resolved situations appropriately where customer identity could not be reasonably established (31 CFR 103.121(b)(2)(iii)).

f) Maintained a record of the identity information required by the CIP and a record of the method used to verify identity and verification results (including results of discrepancies) (31 CFR 103.121(b)(3)).

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

h) Filed SARs, as appropriate (12 CFR 563.180).

8. Evaluate the level of exceptions to determine whether the bank is effectively implementing its CIP (making or approving exceptions cannot be allowed by policy, however, isolated, nonsystemic errors [such as an insignificant number of data entry errors] may be deemed as not compromising the program's effectiveness) (31 CFR 103.121(b)(1)).

9. Based on a risk assessment, prior examination reports, and a review of the bank's audit, select a sample of relationships with third parties upon whom the bank relies or uses to perform its CIP (or portions of the CIP), if applicable.

   If the bank is using the "reliance provision:"

   a) Determine whether the third party is a federally regulated financial institution subject to the BSA/AML program requirements of 31 USC 5318(h).

   b) Review the contract between the parties, annual certifications, and other information, such as the third party's CIP (31 CFR 103.121(b)(6)).

   c) 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).

   If the bank is using an agent or service provider to perform elements of its CIP, determine whether its oversight over such a third party is adequate as follows:

   a) 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).

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

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