Compliance for Deposit Operations
Customer Identification Program

Pennsylvania Association of Community Bankers

November 2020

Consultants to the Financial Industry
Young & Associates, Inc.
121 E. Main Street
P.O. Box 711
Kent, OH 44240
Phone: 330.678.0524
Fax: 330.678.6219
www.younginc.com

Table of Contents

Section 1:
Customer Identification Program
[31 C.F.R. § 1020.220]

Introduction

On May 1, 2003, the final rule of the Customer Identification Program was issued by the Financial Crimes Enforcement Network (FinCEN), United States Department of the Treasury; Office of the Comptroller of the Currency, Treasury; Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; Office of Thrift Supervision, Treasury; and the National Credit Union Administration (hereafter, the "Agencies"). Together, these Agencies jointly adopted a final rule to implement section 326 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (the Act).

The substantive requirements of the joint final rule were codified as part of Treasury's BSA regulations located in 31 C.F.R. § Chapter X. In addition, each of the Agencies concurrently published a provision in its own regulations to cross-reference this final rule in order to clarify the applicability of the final rule to the banks subject to its jurisdiction.

Section 2: Definitions [31 C.F.R § 1020.100]

Account [31 C.F.R § 1020.100(a)]

Account means 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.

Account *also includes* a relationship established to provide:

- a safety deposit box or other safekeeping services, or
- cash management, custodian, and trust services.

Account *does not* include:

- 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.

Bank [31 C.F.R § 1020.100(b)]

Bank means a bank, as that term is defined in § 1010.100(d), that is subject to regulation by a Federal Functional Regulator; and a credit union, private bank, and trust company, as set forth in § 1010.100(d), that does not have a Federal Functional Regulator.

Customer [31 C.F.R § 1020.100(c)]

Customer 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.

Customer *does not* include:

- a financial institution regulated by a Federal Functional Regulator;
- a bank regulated by a state bank regulator;

- companies that are publicly traded described in § 1020.315(b)(2) through (b)(4); 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.

Financial Institution [31 C.F.R § 1020.100(d)]

- For the purposes of § 1020.210, a financial institution defined in 31 U.S.C. 5312(a)(2) or (c)(1) that is subject to regulation by a Federal functional regulator or a self-regulatory organization.
- For the purposes of § 1020.220, financial institution is defined at 31 U.S.C. 5312(a)(2) and (c)(1).

Section 3: Customer Identification Program [31 C.F.R § 1020.220]

Minimum Requirements [31 C.F.R § 1020.220(a)]

In General [31 C.F.R § 1020.220(a)(1)]

A bank must implement a written Customer Identification Program (CIP) appropriate for its size and type of business that, at a minimum, includes each of the requirements of paragraphs (a)(1) through (5) of this section. If a bank is required to have an anti-money laundering compliance program under the regulations implementing 31 U.S.C. 5318(h), 12 U.S.C. 1818(s), or 12 U.S.C. 1786(q)(1), then the CIP must be a part of the anti-money laundering compliance program.

Discussion:

The rule requires each bank to maintain a CIP that is appropriate given the bank's size, location, and type of business. The rule also requires a bank's CIP to contain the statutorily prescribed procedures, describe these procedures, and detail certain minimum elements that each of the procedures must contain. In addition, the rule requires that the CIP be written and that it be approved by the bank's board of directors or a committee of the board.

The CIP must be incorporated into the bank's BSA compliance program and should not be a separate program. A bank's BSA compliance program must be written, approved by the board, and noted in the bank's minutes.

The board of directors' responsibility to oversee bank compliance with section 326 of the Act is a part of a board's conventional supervisory BSA compliance responsibilities that cannot be delegated to bank management. Therefore, a bank's board of directors must be responsible for approving a CIP described in detail sufficient for the board to determine that:

1. the bank's CIP contains the minimum requirements of this final rule; and
2. the bank's identity verification procedures are designed to enable the bank to form a reasonable belief that it knows the true identity of the customer.

Responsibility for the development, implementation, and day-to-day administration of the CIP may be delegated to bank management.

The rule requires that the CIP be a part of a bank's anti-money laundering program once a bank becomes subject to an anti-money laundering compliance program requirement.

Identity Verification Procedures [31 C.F.R § 1020.220(a)(2)]

The CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practical. The procedures must enable the bank to form a reasonable belief that it knows the true identity of each customer. These procedures must be based on the bank's assessment of the relevant risks, including those presented by the various types of accounts maintained by the bank, the various methods of opening accounts provided by the bank, the various types of identifying

information available, and the bank's size, location, and customer base. At a minimum, these procedures must contain the elements described in this paragraph (a)(2).

Customer information required [31 C.F.R § 1020.220(a)(2)(i)]

(A) In general. The CIP must contain procedures for opening an account that specify the identifying information that will be obtained from each customer. Except as permitted by paragraphs (a)(2)(i)(B) and (C) of this section, the bank must obtain, at a minimum, the following information from the customer prior to opening an account:

1. Name;
2. Date of birth, for an individual;
3. Address, which shall be:
   a. For an individual, a residential or business street address;
   b. For an individual who does not have a residential or business street 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; or
   c. 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; and
4. Identification number, which shall be:
   a. For a U.S. person, a taxpayer identification number; or
   b. For a non-U.S. person, one or more of the following:
      i a taxpayer identification number;
      ii passport number and country of issuance;
      iii alien identification card number; or
      iv 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.

(B) Exception for persons applying for a taxpayer identification number. Instead of obtaining a taxpayer identification number from a customer prior to opening the account, the CIP may include procedures for opening an account for a customer that has applied for, but has not received, a taxpayer identification number. In this case, the CIP must include procedures to confirm that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.

(C) Credit card accounts. In connection with a customer who opens a credit card account, a bank may obtain the identifying information about a customer required under paragraph (a)(2)(i)(A) by acquiring it from a third-party source prior to extending credit to the customer.

The rule includes an exception for credit card accounts only, which would allow a bank broader latitude to obtain some information from the customer opening a credit card account, and the remaining information from a third party source, such as a credit reporting agency, prior to extending credit to a customer.

Customer Verification [31 C.F.R § 1020.220(a)(2)(ii)]

The CIP must contain procedures for verifying the identity of the customer, using information obtained in accordance with paragraph (a)(2)(i) of this section, within a reasonable time after the account is opened. The procedures must describe when the bank will use documents, non-documentary methods, or a combination of both methods as described in this paragraph (a)(2)(ii).

(A) Verification through documents. For a bank relying on documents, the CIP must contain procedures that set forth the documents that the bank will use. These documents may include:

(1) For an individual, unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and

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

(B) Verification through non-documentary methods. For a bank relying on non-documentary methods, the CIP must contain procedures that describe the non-documentary methods the bank will use.

(1) These 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.

(2) The bank's non-documentary procedures must 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; 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.

Discussion

Recognizing that some accounts are opened by telephone, by mail, and over the Internet, the rule provides that a bank's CIP also must contain procedures describing what non-documentary methods the bank will use to verify identity and when the bank will use these methods (whether in addition to, or instead of, relying on documents).

Non-documentary verification methods that a bank may use include contacting a customer after the account is opened; obtaining a financial statement; comparing the identifying information provided by the customer against fraud and bad check databases to determine whether any of the information is associated with known incidents of fraudulent behavior

(negative verification); comparing the identifying information with information available from a trusted third party source, such as a credit report from a consumer reporting agency (positive verification); and checking references with other financial institutions. The bank also may wish to analyze whether there is logical consistency between the identifying information provided, such as the customer's name, street address, ZIP code, telephone number, date of birth, and social security number (logical verification).

The rule adopts general principles plus examples. Therefore, the final rule states that for a bank relying on non-documentary verification methods, the CIP must contain procedures that describe the non-documentary methods the bank will use. One method is "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," rather than verifying "documentary information" through such sources.

(C) Additional verification for certain customers. The CIP must address situations where, based on the bank's 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 the verification methods described in paragraphs (a)(2)(ii)(A) and (B) of this section.

Lack of Verification [31 C.F.R § 1020.220(a)(2)(iii)]

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

(A) When the bank should not open an account;

(B) The terms under which a customer may use an account while the bank attempts to verify the customer's identity;

(C) When the bank should close an account, after attempts to verify a customer's identity have failed; and

(D) When the bank should file a Suspicious Activity Report in accordance with applicable law and regulation.

Discussion

A bank's CIP should include procedures for responding to circumstances in which the bank cannot form a reasonable belief that it knows the true identity of the customer. There are some exceptions to this basic rule. For example, a bank may maintain an account at the direction of a law enforcement or intelligence agency, even though the bank does not know the true identity of the customer. However, the rule text itself states that the procedures should describe the following:

- When a bank should not open an account for a potential customer;
- 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 in accordance with applicable law and regulation.

The rule does not specifically require a bank to close the account of a customer whose identity the bank cannot verify, but instead leaves this determination to the discretion of the bank. There is no statutory basis to create a safe harbor that would shield banks from state regulatory or borrower liability if a bank should choose to close a customer's account. Any such closure should be consistent with the bank's existing procedures for closing accounts in accordance with its risk management practices.

A bank must also comply with other applicable laws and regulations, such as the adverse action provisions under ECOA and the FCRA, when determining not to open an account because it cannot establish a reasonable belief that it knows the true identity of the customer.

Recordkeeping [31 C.F.R § 1020.220(a)(3)]

The CIP must include procedures for making and maintaining a record of all information obtained under the procedures implementing paragraph (a) of this section.

(i) ***Required records.*** At a minimum, the record must include:

(A) All identifying information about a customer obtained under paragraph (a)(2)(i) of this section;

(B) A description of any document that was relied upon under paragraph (a)(2)(ii)(A) of this section 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;

(C) A description of the methods and the results of any measures undertaken to verify the identity of the customer under paragraph (a)(2)(ii)(B) or (C) of this section; and

(D) A description of the resolution of any substantive discrepancy discovered when verifying the identifying information obtained.

Nothing in the rule modifies, limits, or supersedes section 101 of the Electronic Signatures in Global and National Commerce Act, Pub. L. 106-229, 114 Stat. 464 (15 U.S.C. 7001) (E-Sign Act). Thus, a bank may use electronic records to satisfy the requirements of this final rule, as long as the records are accurate and remain accessible in accordance with 31 C.F.R. § 1010.430(d).

(ii) ***Retention of Records.*** The bank must retain the information in paragraph (a)(3)(i)(A) of this section for five years after the date the account is closed or, in the case of credit card accounts, five years after the account is closed or becomes dormant. The bank must retain the information in paragraphs (a)(3)(i)(B), (C), and (D) of this section for five years after the record is made.

Comparison with Government Lists [31 C.F.R § 1020.220(a)(4)]

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. 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.

At this time, there are no designated lists. Banks will receive notification by way of separate guidance regarding the lists that must be consulted for purposes of this provision.

Customer Notice [31 C.F.R § 1020.220(a)(5)]

(i) **Customer Notice.** The CIP must include procedures for providing bank customers with adequate notice that the bank is requesting information to verify their identities.

(ii) **Adequate Notice.** Notice is adequate if the bank generally describes the identification requirements of this section and provides the notice in a manner reasonably designed to ensure that a customer is able to view the notice, or is otherwise given notice, before opening an account. For example, depending upon the manner in which the account is opened, a bank may post a notice in the lobby or on its Web site, include the notice on its account applications, or use any other form of written or oral notice.

(iii) **Sample Notice.** If appropriate, a bank may use the following sample language to provide notice to its customers:

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 [31 C.F.R § 1020.220(a)(6)]

The 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:

a. Such reliance is reasonable under the circumstances;

b. The other financial institution is subject to a rule implementing 31 U.S.C. 5318(h) and is regulated by a Federal functional regulator; and

c. 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.

Exemptions [31 C.F.R § 1020.220(b)]

The appropriate Federal functional regulator, with the concurrence of the Secretary, may, by order or regulation, exempt any bank or type of account from the requirements of this section. The Federal functional regulator and the Secretary shall consider whether the exemption is consistent with the purposes of the Bank Secrecy Act and with safe and sound banking, and may consider other appropriate factors. The Secretary will make these determinations for any bank or type of account that is not subject to the authority of a Federal functional regulator.

Other Requirements Unaffected [31 C.F.R § 1020.220(c)]

Nothing in this section relieves a bank of its obligation to comply with any other provision in this part, including provisions concerning information that must be obtained, verified, or maintained in connection with any account or transaction.

Discussion

The proposal provided that nothing in § 1020.220 shall be construed to relieve a bank of its obligations to obtain, verify, or maintain information in connection with an account or transaction that is required by another provision in part 1020. For example, if an account is opened with a deposit of more than $10,000 in cash, the bank opening the account must comply with the customer identification requirements in § 1020.220, as well as with the provisions of § 1010.311, which require that certain information concerning the transaction be reported by filing a Currency Transaction Report (CTR).