

**BANKER AS REGULATOR  
(INCLUDING PATRIOT ACT ISSUES)**

**MICHAEL D. CUDA**  
Winstead Sechrest & Minick  
1201 Elm Street, Suite 5400  
Dallas, Texas 75270

State Bar of Texas  
**2<sup>ND</sup> ANNUAL ADVANCED BUSINESS LAW COURSE**  
October 14-15, 2004  
Dallas

**CHAPTER 10**

MICHAEL D. CUDA  
Winstead Sechrest & Minick  
1201 Elm Street, Suite 5400  
Dallas, Texas 75270  
214.745.5233  
Fax: 214.745.5390

BIOGRAPHICAL INFORMATION

EDUCATION

B.A. in Political Philosophy, The University of Dallas  
M.B.A. summa cum laude, St. Edward's University  
J.D., magna cum laude, Texas Tech University School of Law

PROFESSIONAL ACTIVITIES

Shareholder, Winstead Sechrest & Minick, Dallas, Texas - Banking and Credit Transactions  
Member, City of Arlington, Texas Loan Review Board  
Member, Thrivent Financial Dallas-Tarrant Chapter Board of Directors  
Former member, Consumer Law Council, State Bar of Texas

LAW RELATED PUBLICATIONS, ACADEMIC APPOINTMENTS AND HONORS

Author/Speaker for the Advanced Real Estate Section of the State Bar of Texas  
Repeated Author/Speaker for the Texas Association of Bank Counsel on Various Topics  
Author/Speaker for the National Business Institute, Inc. regarding Texas Lending  
Author/Speaker for the Bank Law Institute regarding Banking Regulatory Issues  
Adjunct Professor of Law, Texas Tech University School of Law.  
Adjunct Professor of Law, University of Oklahoma School of Law.  
Adjunct Professor of Law, Texas Wesleyan University School of Law.

**TABLE OF CONTENTS**

- I. INTRODUCTION .....1
- II. THE USA PATRIOT ACT.....1
  - A. Background.....1
  - B. Customer Identification Program.....1
  - C. Examination Requests.....2
  - D. Case Law and Enforcement Actions.....2
- III. CREDIT AGREEMENT COVENANTS .....2
  - A. Affirmative Covenants.....2
    - 1. Corporate Existence and Due Qualification.....3
    - 2. Compliance with Laws.....3
    - 3. Compliance with Agreements.....3
  - B. Negative Covenants .....3
    - 1. Negative Pledges and Restrictions on Debt .....3
    - 2. Other Negative Covenants .....4
- IV. CONCLUSION.....4

## **BANKER AS REGULATOR (INCLUDING PATRIOT ACT ISSUES)**

### **I. INTRODUCTION**

It may strike bankers and their counsel as odd, but in many respects, bankers have become the regulators of their borrowers and customers. Partly as a result of federal and state regulatory requirements placed on financial institutions under the auspices of "safe and sound" banking practices and partly as a practical response to limiting the risky activities of a borrower to minimize loan losses, credit agreements have become a morass of direct or indirect regulatory references.

While most of the attendees of this conference are familiar with the fact that certain covenants are "standard" in a credit agreement and therefore do not raise a lot of objections, many of us may be less familiar with the statutory underpinnings that cause those "standard" provisions to be included on their documents. This article will attempt to explain some of those provisions, and the reasons they need to be included in a credit agreement.

### **II. THE USA PATRIOT ACT**

#### **A. Background**

The USA Patriot Act of 2001 (an acronym for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism") (the "Patriot Act") was signed into law on October 26, 2001 in rapid response to the terrorist attacks on the United States staged on September 11, 2001. The Patriot Act is composed of ten titles designed to provide stronger surveillance powers, enhance criminal laws against terrorism, improve intelligence and combat money laundering.<sup>1</sup> The provisions of the Patriot Act that likely most affect financial institutions are located in Title III, which change provisions of the Bank Secrecy Act as well as provide the Treasury Department and other federal agencies with enhanced authority to fight international money laundering.<sup>2</sup> Title III of the Patriot Act applies to all financial institutions.<sup>3</sup> Within Title III of the Patriot Act, effective dates vary, depending on the specific activity regulated. The Patriot Act itself does not have a specific overall implementation date, which would indicate that its provisions are effective immediately, other than those provisions with a specific implementation date.<sup>4</sup> Each of the implementation dates have now passed.<sup>5</sup>

Title III, Section 326 of the Patriot Act requires implementation of a Customer Identification Program ("CIP"). Full compliance with the Final CIP Regulations has been required since October 1, 2003.<sup>6</sup>

#### **B. Customer Identification Program**

The CIP is subsumed within the Bank Secrecy Act ("BSA") compliance program of each financial institution. Therefore, the nature of the program will vary by the relative size and sophistication of each financial institution. BSA policies are required to be approved by the board of directors of each financial institution, and such approval must be reflected in the board minutes.<sup>7</sup>

The mandatory provisions of any CIP, as incorporated through the BSA policy requirements, are internal policies, procedures and controls; designation of a compliance officer; continuing employee training; and an independent audit program.<sup>8</sup> Some of the factors that should be considered in developing these policies and procedures include the types of accounts maintained by the financial institution, the institution's method of opening accounts, the types of identifying information that are available and the size, location and customer base of the institution.<sup>9</sup>

In addition to developing the appropriate internal controls discussed above, a financial institution is required to gather customer information prior to opening any "account". For purposes of the Regulations, an "account" is "a formal banking relationship to provide or engage in services, dealing, or other financial transactions."<sup>10</sup> An "account" includes safe deposit boxes and other safekeeping services, cash management services and custodian and other trust services, but does not include accounts acquired by a financial institution and accounts for purposes of participating in an ERISA program.<sup>11</sup>

Once a financial institution has determined that a customer is opening an account, at a minimum, the institution must obtain the customer's name, date of birth (for individuals), address (principal place of business for corporations and other fictional entities) and an identification number (varies by individual or entity).<sup>12</sup> Based on the risk assessment, the institution may require additional information prior to opening the account.

After opening an account for a customer a financial institution must maintain records of the customer's account until five years after the account is closed and maintain the information related to customer verification until five years after the information is gathered and the record is made. Additionally, institutions must determine whether the customer appears on any federal government list of known or suspected terrorist organizations.<sup>13</sup> A financial institution is also required to provide its customer notice that it is requesting this information to verify their identity. The following language is suggested by the Federal Crimes Enforcement Network:

**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.<sup>14</sup>

The final rule does not alter a financial institution's ability to rely on other financial institutions to perform some or all of the elements of a CIP, and financial institutions are also allowed to rely on third parties to perform services on its behalf.<sup>15</sup> In fact, the financial institution compliance requirements under the Patriot Act have spawned a variety of service companies, such as Bridger Insight, that provide identity verification services and checks against all required terrorist watch lists, among other services.

### C. Examination Requests

Finally, the Bank Secrecy Examination Procedures memo outlines twelve items that it is suggested that examiners include in their request letter to financial institutions. These items include a copy of the institution's CIP; a written description of the institution's rationale for exempting existing customers; a copy of the board minutes approving the CIP; a copy of the audit policies and procedures covering the CIP; a copy of the CIP training program; a list of new accounts covering product lines and segregating new from existing customers; a list of accounts opened with a tax identification number; a list of accounts opening without verification or CIP compliance; a list of high-risk accounts pursuant to CIP procedures; a copy of the customer notice and timing; if a institution is relying on another institution for compliance, a list of such institutions, a statement of whether the institution is subject to this rulemaking together with a copy of any contract executed between the parties, a copy of the CIP of such institution and any certifications made by one party to the other; and finally, if the institution is relying on a third party for compliance, a list of names of the parties, a copy of any contracts between the parties, a copy of the CIP procedures used by the other party, and the institution's policies and procedures for ensuring adequate performance by the third party.<sup>16</sup>

### D. Case Law and Enforcement Actions

To the extent that a financial institution believes that money laundering may be occurring at the institution, it is required to report this information to its designated compliance officer. The compliance officer must then review the activities, and if the officer determines that a suspicious activity has occurred, the officer is required to file a Suspicious Activity Report (a "SAR"). A SAR is protected by a "safe harbor" for financial institutions so that these reports are not the subject of a defamation lawsuit by the institution's customers.

In *Whitney National Bank v. Karam*,<sup>17</sup> a SAR in connection with suspected illegal lending activity was filed and several customers of the institution sued for defamation. The plaintiff attempted to circumvent the safe harbor in their discovery request by seeking oral or written communications with law enforcement agencies with respect to their transactions at the institution. The institution sought and was granted protection from the discovery request. In particular, the Court ruled that the institution was not required to produce the "SAR itself; communications pertaining to a SAR or its contents; communications preceding the filing of a SAR and preparatory or preliminary to it; communications that follow the filing of a SAR and are explanations or follow-up discussions; or oral communications or suspected or possible violations that did not culminate in the filing of a SAR".<sup>18</sup>

In addition to the courts upholding the safe harbor for financial institutions filing a SAR, federal regulatory agencies have also actively sought enforcement of the regulations proscribed under the Patriot Act. In particular, on May 13, 2004, the OCC assessed a \$25 million civil penalty against Riggs Bank, N.A. for willful violations of the SAR and the Currency Transaction Reporting requirements of the BSA.<sup>19</sup> A consent order was also imposed requiring corrective action to comply with the BSA. The civil penalties and consent order arose out of Riggs' failure appropriately to assess their risk with respect to high-risk customers (foreign embassy account relationships with Saudi Arabia for example), inadequate collection of customer information, omissions to responses to regulators, ineffective independent testing, inadequate training, and other problems with their CIP.

## III. CREDIT AGREEMENT COVENANTS

### A. Affirmative Covenants.

Covenants are agreements or promises undertaken by a party to a contract to take (affirmative covenants) or not take (negative covenants) certain actions. In general, affirmative covenants focus on actions that a borrower would take in the normal course of business and negative covenants focus on actions that, if taken by the borrower, could significantly alter the structure of the borrower or its business operations.<sup>20</sup>

### 1. Corporate Existence and Due Qualification

Credit Agreements typically will require the borrower and each subsidiary of the borrower to maintain their corporate existence and good standing in each jurisdiction in which their respective activities require them to be organized and qualified. The purpose of this provision is to ensure that there is always a legal entity that is obligated to repay the loan.<sup>21</sup> This provision also requires the borrower and its subsidiaries to be qualified in foreign jurisdictions in which they are "doing business". Whether or not a borrower or its subsidiaries are doing business in a foreign jurisdiction may boil down to a facts and circumstances test. Nevertheless, it is important to a banker that a borrower or its subsidiaries are properly qualified in foreign jurisdictions because if there is not proper qualification, contracts entered into by the borrower or its subsidiaries in those jurisdictions may not be enforceable. This provision becomes increasingly more important as the volume of business that a borrower or its subsidiaries does in such jurisdiction grows.<sup>22</sup>

### 2. Compliance with Laws

A borrower and its subsidiaries are typically required to comply with all applicable laws, rules, regulations and orders. A great many additional references can be added to the litany of regulatory bodies and courts included in the covenant. This is an extremely broad provision that, stated as above, borrowers consistently argue is overbroad. Nevertheless, the covenant is designed to regulate the borrower's activities with respect to common and statutory corporate law, antitrust, antidiscrimination, environmental and licensing, federal, state and local tax laws, ERISA, the Foreign Corrupt Practices Act etc.<sup>23</sup> The more sophisticated the borrower, the more specific these "compliance with law" provisions become. Therefore, it is not unusual to see specific covenants with respect to ERISA, taxes, corporate law and environmental provisions. However, it is also important to have a catch-all provision, typically with a "compliance in all material respects" or "so as not to cause a material adverse effect" carve-out.

The purpose of all of the compliance with laws provisions, both general and specific, is to make sure that the borrower is taking all reasonable actions necessary to comply with laws. This gives lenders some additional assurance that the creditworthiness of the borrower will not be affected by fines and penalties, the revocation of a license or the placement of a lien on borrower assets, among other potential problems.<sup>24</sup> Consequently, it is generally appropriate to grant a borrower certain limitations on the scope of the general or specific covenants, as long as they remain financially sound even after a failure to comply with certain statutes or regulations.

### 3. Compliance with Agreements

Another area in which a lender "regulates" a borrower is in connection with third party agreements into which a borrower enters. The actual covenant can be drafted in the general or very specifically. To the extent that a borrower has one specific contract or customer that is very important to the business, it is appropriate to require performance under that contract or in that relationship in a covenant. If a borrower has a diversified series of contracts or customers, a general covenant is appropriate with a "material adverse effect" carve-out.

A subset of the compliance with agreements covenant that is typically set forth in a credit agreement is the requirement that a borrower pay and discharge as they become due, all material obligations. While this provision is just another form of a compliance with agreement covenant, a lender should know specifically that a borrower and its subsidiaries are paying its other creditors. The covenant itself is typically limited to material obligations. Exceptions, when appropriate, may be established for obligations whose validity or amount are being contested in good faith or for which the borrower has set aside adequate reserves.<sup>25</sup>

### B. Negative Covenants

As discussed above, negative covenants restrict a borrower's activities in order to accomplish the same goals as the affirmative covenants. Specifically, negative covenants establish guidelines for the business by prohibiting certain borrower actions, ensure that the business assumptions that the lender made in approving the loan remain in place and help the lender obtain information about the borrower.<sup>26</sup>

#### 1. Negative Pledges and Restrictions on Debt

A negative pledge is an agreement by a borrower and its subsidiaries not to encumber some or all of their assets. A negative pledge does not prohibit a borrower or its subsidiaries from incurring debt, which is a separate negative covenant. However, a negative pledge will limit the types of debt that a borrower can incur. The negative pledge covenant and the restriction on debt covenant are generally drafted with reference to one another. A typical provision may allow a borrower to grant liens on certain assets, but the restriction on debt covenant will limit the amount of debt that may secure the lien. Other types of debt and liens may be completely prohibited by the negative covenants.

While these provisions may not appear on their face to be "regulatory" in nature, like many of the affirmative covenants, they are designed to prevent a borrower from taking (or failing to take) actions that may compromise the borrower's ability to repay its obligations to the lender. However, these provisions become more regulatory in nature when you consider

prohibitions on debt and liens that historically have been treated as "off-balance sheet" items, such as financing leases. While the Securities and Exchange Commission are making a great deal of progress in reforming the accounting treatment of these and other items that have been open for manipulation, it is also appropriate for a lender either to prohibit debt that may not appear in a borrower's financial statements under Generally Accepted Accounting Principles or to require such items to be reported in the borrower's financial statements, regardless of GAAP treatment.

## 2. Other Negative Covenants

Credit Agreements will contain a variety of other negative covenants that will limit a borrower and its subsidiaries from merging, dissolving, selling off a majority of their assets, entering into transactions with affiliates on non-market conditions, distributing dividends, making certain types of investments etc. Additionally, the borrower will be tested by certain financial covenants that allow a lender to determine the financial strength and stability of the borrower. While these provisions are not directly "regulatory" with respect to the borrower, they are regulatory with respect to a lender. Each lender is obligated by its own regulator to make loans in a safe and sound manner. While the safety and soundness obligation may not require every negative (or affirmative) covenant contained in a large syndicated credit facility, the further a lender deviates from these standards, the more open to criticism by its regulators it becomes. Additionally, a regulator's review of a defaulted loan is with 20-20 hindsight. Consequently, it is incumbent on a lender to reach an appropriate middle-ground with its borrowers regarding the nature and scope of all covenants.

## IV. CONCLUSION

In today's increasingly regulatory environment, a lender walks a fine line between "regulating" its customers, and creating an environment that discourages a customer, or borrower, from using a lender's institution. As we have seen, the USA PATRIOT Act has created significant new burdens on financial institutions to gather information on the customers, and monitor that information. It appears that regulatory examination information requests will require a financial institution to provide the basis for the scope of its CIP as well as all the analytical documentation related to the program's strengths and weaknesses after implementation. This is a regulatory requirement imposed on the financial institution, and it forces the financial institution to regulate its customers *i.e.* confirm that their customers are not engaging in money laundering or other prohibited activities.

In addition to some of these new "regulator" activities imposed on financial institutions, an institution, acting as a lender, must monitor its borrower's activities through covenants in order to assure borrower compliance with other laws and regulations. As borrowers and transactions have become more sophisticated, so have the covenants that "regulate" these activities. Finally, a lender's failure adequately to "regulate" its borrowers will draw attention from the lender's own regulators. Nevertheless, even though the cost of administering these "regulatory" activities is growing substantially, as we have seen in the Riggs case, the cost of non-compliance can be even more expensive.

<sup>1</sup> R. Ballieu, The USA PATRIOT Act: Complying with New Anti-Money Laundering Requirements, January 2002.

<sup>2</sup> *Id.* at 1.

<sup>3</sup> *Id.*

<sup>4</sup> *Id.* at 2.

<sup>5</sup> *Id.*

<sup>6</sup> See Generally, Guidance on Customer Identification Regulations, Financial Crimes Enforcement Network, FAQs: Final CIP Rule, January 2004; Bank Secrecy Act Examination Procedures for Customer Identification Programs, Financial Crimes Enforcement Network, January 28, 2004 (attached hereto for reference).

<sup>7</sup> *Id.*

<sup>8</sup> Bank Secrecy Act Examination Procedures for Customer Identification Programs, Financial Crimes Enforcement Network, January 28, 2004 at 1 - 3.

<sup>9</sup> *Id.* at 1..

<sup>10</sup> *Id.* at 2.

<sup>11</sup> *Id.*

<sup>12</sup> *Id.* at 3.

<sup>13</sup> *Id.* at 4-5.

<sup>14</sup> *Id.* at 5.

<sup>15</sup> *Id.* at 6.

<sup>16</sup> *Id.* at 7.

<sup>17</sup> 306 F.Supp. 2d 678 (S.D. Tex. 2004).

<sup>18</sup> *Id.* at 687.

<sup>19</sup> OCC NR 2004-34.

<sup>20</sup> Sandra Schnitzer Stern, Structuring and Drafting Commercial Loan Agreements § 5.01[1] (2004).

<sup>21</sup> *Id.* at 5.03[1].

<sup>22</sup> *Id.*

<sup>23</sup> *Id.* at 5.08[1].

<sup>24</sup> *Id.*

<sup>25</sup> *Id.* at 5.11.

<sup>26</sup> *Id.* at 6.01[1].



January 2004

# Guidance on Customer Identification Regulations

Financial Crimes Enforcement Network

## FAQs: Final CIP Rule

The staff of the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, and the United States Department of the Treasury ("Agencies") are issuing these frequently asked questions ("FAQs") regarding the application of 31 C.F.R. § 103.121. This joint regulation implements section 326<sup>1</sup> of the USA PATRIOT Act and requires banks, savings associations, credit unions and certain non-federally regulated banks ("bank") to have a Customer Identification Program ("CIP").

While the purpose of the FAQs document is to provide interpretive guidance with respect to the CIP rule, the Agencies recognize that this document does not answer every question that may arise in connection with the rule. The Agencies encourage banks to use the basic principles set forth in the CIP rule, as articulated in these answers, to address variations on these questions that may arise, and expect banks to design their own programs in accordance with the nature of their business.

The Agencies wish to emphasize that a bank's CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. It is critical that each bank develop procedures to account for all relevant risks including those presented by the types of accounts maintained by the bank, the various methods of opening accounts provided, the type of identifying information available, and the bank's size, location, and type of business or customer base. Thus, specific minimum requirements in the rule, such as the four basic types of information to be obtained from each customer, should be supplemented by risk-based verification procedures, where appropriate, to ensure that the bank has a reasonable belief that it knows each customer's identity.

The Agencies note that the CIP, while important, is only one part of a bank's BSA/AML compliance program. Adequate implementation of a CIP, standing alone, will not be sufficient to meet a bank's other obligations under the BSA, regulations promulgated by its primary Federal regulator, such as Suspicious Activity Reporting requirements, or regulations promulgated by the Office of Foreign Assets Control.

---

<sup>1</sup> Section 326 of the Act adds a new subsection (l) to 31 U.S.C. § 5318 of the Bank Secrecy Act ("BSA").

Finally, these FAQs have been designed to help banks comply with the requirements of the CIP rule. They do not address the applicability of any other Federal or state laws.

### **31 C.F.R. § 103.121(a)(1) -- Definition of "account"**

**1. The CIP rule applies to a "customer," which is generally "a person that opens a new account." (Emphasis added.) At what point does the CIP rule apply when the account is a loan? When is the account opened?**

"Customer" does not include a person who does not receive banking services, such as a person whose loan application is denied. See 68 FR 25090, 25093 (May 9, 2003). Therefore, when the account is a loan, the account is opened when the bank enters into an enforceable agreement to provide a loan to the customer.

**2. Are loan participations purchased from third parties and loans purchased from a car dealer or mortgage broker within the exclusion from the definition of "account" for loans acquired through an acquisition, merger, purchase of assets, or assumption of liabilities?**

Yes, this exclusion is intended to cover loan participations purchased from third parties and loans purchased from a car dealer or mortgage broker. If, however, the bank is extending credit to the borrower using a car dealer or mortgage broker as its agent, then it must ensure that the dealer or broker is performing the bank's CIP.

### **31 C.F.R. § 103.121(a)(2) -- Definition of "bank"**

**1. Is the CIP rule applicable to a bank's foreign subsidiaries?**

No. The CIP rule does not apply to any part of the bank located outside of the United States. Nevertheless, as a matter of safety and soundness, banks are encouraged to implement an effective CIP throughout their operations, including in their foreign offices, except to the extent that the requirements of the rule would conflict with local law.

### **31 C.F.R. § 103.121(a)(3) -- Definition of "customer"**

**1. Who is the "customer" when an account is opened by an individual who has power-of-attorney for a competent person who is the named owner of the account?**

The CIP rule provides that a "customer" generally is "a person that opens a new account." 31 C.F.R. § 103.121(a)(3)(i)(A). When an account is opened by an individual who has power-of-attorney for a competent person, the individual with a power-of-attorney is merely an agent acting on behalf of the person that opens the account. Therefore, the "customer" will be the named owner of the account rather than the individual with a power-of-attorney over the account. By contrast, an individual with power-of-attorney will be the "customer" if the account is opened for a person who lacks legal capacity. 31 C.F.R. § 103.121(a)(3)(i)(B)(1).

**2. Is a person who becomes co-owner of an existing deposit account a “customer” to whom the CIP rule applies?**

Yes, a person who becomes the co-owner of an existing deposit account is a “customer” subject to the CIP rule because that person is establishing a new account relationship with the bank.

**3. Is a new borrower who is substituted for an existing borrower through an assumption of a loan a “customer” to whom the CIP rule applies?**

Yes, a new borrower who is substituted for an existing borrower through an assumption of a loan is a “customer” because the new borrower is establishing a new account relationship with the bank.

**4. The CIP rule requires a bank to verify the identity of each “customer.” Under the CIP rule, a “customer” generally is defined as “a person that opens a new account.” If a pension plan administrator chooses to remove a former employee from the plan pursuant to section 657(c) of the Economic Growth and Tax Relief Reconciliation Act of 2001 (EGTRRA), it is required by law to transfer these funds to a financial institution. In addition, an administrator of a terminated plan may remove former employees that it is unable to locate, by transferring their benefits to a financial institution. Would a plan administrator or the former employee be a bank “customer” where funds are transferred to a bank and an account established in the name of the former employee, in either of these situations?**

In either situation, the administrator has no ownership interest in or other right to the funds, and therefore, is not the bank’s “customer.” Nor would we view the administrator as acting as the customer’s agent when the administrator transfers the funds of former employees in these situations. A customer relationship arises and the requirements of the rule are implicated when the former employee “opens” an account. While the former employee has a legally enforceable right to the funds that are transferred to the bank, the employee has not exercised that right until he or she contacts the bank to assert an ownership interest. Thus, in light of the requirements imposed on the plan administrator under EGTRRA, as well as the requirements in connection with plan terminations, the former employee will not be deemed to have “opened a new account” for purposes of the CIP rule until he or she contacts the bank to assert an ownership interest over the funds, at which time a bank will be required to implement its CIP with respect to the former employee.

This interpretation applies only to (1) transfers of funds as required under section 657(c) of EGTRRA, and (2) transfers to banks by administrators of terminated plans in the name of participants that they have been unable to locate, or who have been notified of termination but have not responded, and should not be construed to apply to any other transfer of funds that may constitute opening an account.

**5. A bank is an agent for a (bank) credit card issuer. The cards are co-branded, the two banks share in the revenue from the cards issued. However, the issuer approves the credit**

**card applications and handles collections. Is a person who obtains a credit card a customer of the agent bank or the card issuer?**

A person who receives a credit card is receiving an extension of credit from, and therefore is establishing an account with, the issuing bank. The agent bank is compensated by the issuing bank and not by the customer. For these reasons, the issuing bank is responsible for ensuring that its CIP applies to the customer. However, the agent bank may perform parts of the CIP on behalf of the issuing bank. As with any other responsibility performed by an agent, the issuing bank ultimately is responsible for the agent's compliance with the requirements of the CIP rule. See 68 FR 25090, 25104 (May 9, 2003). Alternatively, the issuing bank may *rely* upon the agent bank to perform elements of its CIP, provided that the issuing bank is able to satisfy the requirements of the reliance provision, 31 C.F.R. § 103.121(b)(6), including the requirement that the person be a customer of both the issuing and agent bank.

### **31 C.F.R. § 103.121(a)(3)(ii)(C) – Person with an existing account**

**1. A loan and a time deposit are each an “account” for purposes of the CIP rule. How do the requirements of the CIP rule apply to a loan that is renewed, or a certificate of deposit that is rolled over?**

The CIP rule applies to a “customer,” generally, “a person that opens a *new* account.” 31 C.F.R. § 103.121(a)(3)(i). (Emphasis added.) “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. 31 C.F.R. § 103.121(a)(1)(i). For purposes of the CIP rule, each time a loan is renewed or a certificate of deposit is rolled over, the bank establishes another formal banking relationship and a *new* account is established. However, the rule provides that the term “customer” does not include 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. 31 C.F.R. § 103.121(a)(3)(ii)(C). In each of these cases, the customer has an *existing* account. Therefore, as long as the bank has a reasonable belief that it knows the person's true identity, the bank need not perform its CIP when a loan is renewed or certificate of deposit is rolled over. However, if a new customer is added to the loan or deposit account, the bank would need to satisfy the CIP rule with respect to that new account relationship.

**2. Does the exclusion from the definition of “customer” in 31 C.F.R. § 103.121(a)(3)(ii)(C) for a person with an existing account extend to a person who has had an account with the bank in the last twelve months but who no longer has an account?**

No, this provision only excludes from the definition of “customer” a person that at the time a new account is opened currently “has an existing account with the bank,” and only if the bank has a reasonable belief that it knows the true identity of the person. Therefore, for example, when a person has a deposit account and subsequently obtains a loan, the person has an existing account with the bank. Conversely, a person would not be deemed to have an existing account at the bank if the person had a loan, paid it off, and twelve months later obtains a new loan.

**3. How can a bank demonstrate that it has “a reasonable belief that it knows the true identity of a person with an existing account” with respect to persons that had accounts with the bank as of October 1, 2003?**

Among the ways a bank can demonstrate that it has “a reasonable belief” is 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.

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.

**4. Can a bank exclude from the definition of “customer” a person that has an existing account with its affiliate?**

No, a person that has an existing account with a bank affiliate does not qualify as “a person who has an existing account with the bank” within the meaning of 31 C.F.R. § 103.121(a)(3)(ii)(C). However, the bank may be able to *rely* on its affiliate to perform elements of its CIP, as provided in 31 C.F.R. § 103.121(b)(6).

**31 C.F.R. § 103.121(b)(2)(i) -- Information required**

**1. What address should be obtained for customers who live in rural areas who do not have a residential or business address or the residential or business address of next of kin or another contact individual? For example, is a rural route number acceptable?**

Yes, the number on the roadside mailbox on a rural route is acceptable as an address. A rural route number, unlike a post office box number, is a description of the approximate area where the customer can be located. In the absence of such a number, and in the absence of a residential or business address for next of kin or another contact individual, a description of the customer’s physical location will suffice.

**2. Can a bank open an account for a U.S. person that does not have a taxpayer identification number?**

No, the bank cannot unless the customer has applied for a taxpayer identification number, the bank confirms that the application was filed before the customer opened the account, and the bank obtains the taxpayer identification number within a reasonable period of time after the account is opened. Note, however, that a bank does not need to obtain a taxpayer identification number when opening a new account for a customer that has an existing account, as long as the bank has a reasonable belief that it knows the true identity of the customer. A bank may also open an account for a person who lacks legal capacity with the identifying information, including taxpayer identification number, of an individual who opens an account for that person.

## 31 C.F.R. § 103.121(b)(2)(ii) – Customer verification

### **1. Must a bank verify the accuracy of all of the identifying information it collects in connection with 31 C.F.R. § 103.121(b)(2)(i)?**

The final rule provides that a bank's CIP must contain procedures for verifying the identity of the customer, "using the information obtained in accordance with paragraph (b)(2)(i)," namely the identifying information obtained by the bank. 31 C.F.R. § 103.121(b)(2)(ii). A bank need not establish the accuracy of every element of identifying information obtained but must do so for enough information to form a reasonable belief it knows the true identity of the customer. See 68 FR 25090, 25099 (May 9, 2003).

### **2. Can a bank use an employee identification card as the sole means to verify a customer's identity?**

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' expectation that banks will obtain government-issued identification from most customers. 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.

### **3. Can a bank use an electronic credential, such as a digital certificate, as a non-documentary means to verify the identity of a customer that opens an account over the Internet or through some other purely electronic channel?**

A bank may obtain an electronic credential, such as a digital certificate, as one of the methods it uses to verify a customer's identity. However, the CIP rule requires the bank to have a reasonable belief that it knows the true identity of the customer. Therefore, for example, the bank is responsible for ensuring that the third party uses the same level of authentication as the bank itself would use. See also FFIEC guidance titled "Authentication in an Electronic Banking Environment" (July 30, 2001).

### **4. How should a bank verify the identity of a partnership that opens a new account when there are no documents or non-documentary methods that will establish the identity of the partnership?**

A bank opening an account for such a partnership must undertake additional verification by obtaining information about the identity of any individual with authority or control over the partnership account, in order to verify the partnership's identity, as described in 31 C.F.R. § 103.121(b)(2)(ii)(C).

**5. How should a bank verify the identity of a sole proprietorship that opens a new account, (such as an account titled in the name of an individual “doing business as” a sole proprietorship) when there are no documents or non-documentary methods that will establish the identity of the sole proprietorship?**

In some states, sole proprietorships are required to file “fictitious” or “assumed name certificates.” Banks may choose to use these certificates as a means to verify the identity of a sole proprietorship, if appropriate. However, when there are no documents or non-documentary methods that will establish the identity of the sole proprietorship, the bank must undertake additional verification by obtaining information about the sole proprietor or any other individual with authority or control over the sole proprietorship account -- such as the name, address, date of birth, and taxpayer identification number of the sole proprietor, or any other individual with authority or control over the account -- in order to verify the sole proprietorship’s identity, as described in 31 C.F.R. § 103.121(b)(2)(ii)(C).

**31 C.F.R. § 103.121(b)(3)(i) – Required records**

**1. Would it be acceptable to retain a description of the non-documentary customer verification method used (such as a consumer credit report or an inquiry to a fraud detection system) in a general policy or procedure instead of recording the fact that a particular method was used on each individual customer's record?**

Yes, provided that the record cross-references the specific provision(s) of the risk-based procedures contained in the bank’s CIP used to verify the customer’s identity.

**2. Can a bank keep copies of documents provided to verify a customer’s identity, in addition to the description required under 31 C.F.R. § 103.121(b)(3)(i)(B), even if it is not required to do so?**

Yes, a bank may keep copies of identifying documents that it uses to verify a customer’s identity. 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 documents for other purposes, for example, to facilitate investigating potential fraud. (These documents should be retained in accordance with the general recordkeeping requirements in 31 C.F.R. § 103.38.) Nonetheless, a bank should be mindful that it must 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.

**31 C.F.R. § 103.121(b)(3)(ii) – Retention of records**

**1. Does the original information obtained during account opening have to be retained or can the bank satisfy the recordkeeping requirement by just keeping updated information about the customer, i.e., the customer’s current address?**

The CIP rule requires that a bank retain the identifying information obtained about the customer *at the time of account opening* 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. 31 C.F.R. § 103.121(b)(3)(ii). Updated information serves valuable, but different, purposes.

**2. If the bank requires a customer to provide more identifying information than the minimum during the account opening process, does it have to keep this information for more than five years?**

The bank must keep for five years after the account is closed, or in the case of credit card accounts, five years after the account is closed or becomes dormant, all identifying information it gathers about the customer to satisfy the requirements of § 103.121(b)(2)(i) of the CIP rule. 31 C.F.R. § 103.121(b)(3)(ii). This would include any identifying information, the bank will use, at the time the account is opened, to establish a reasonable belief it knows the true identity of the customer. So, for example, if the bank obtains other identifying information at account opening in addition to the minimal information required, such as the customer's phone number, then the bank must keep that information.

**3. How does the record retention period apply to a customer who simultaneously opens multiple accounts in the bank?**

If several accounts are opened for a customer simultaneously, all identifying information about a customer obtained under 31 C.F.R. § 103.121(b)(2)(i) must be retained for five years after the last account is closed or, in the case of credit card accounts, five years after the last account is closed or becomes dormant. All remaining records must be kept for five years after the records are made.

#### **31 C.F.R. § 103.121(b)(4) – Section 326 List**

**1. Has a list of known or suspected terrorists or terrorist organizations been designated for purposes of the CIP rule?**

No such list has been designated to date. Banks will be contacted by their functional regulators when a list is issued. As of the time of publication, lists published by OFAC have not been designated as lists for purposes of the CIP rule. Of course, banks are separately obligated to check these lists in accordance with OFAC's regulations.

#### **31 C.F.R. § 103.121(b)(5) – Customer notice**

**1. Does a bank have to provide notice to all owners of a joint account?**

Yes, notice must be provided to all owners of a joint account. In addition, notice must be provided "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." 31 C.F.R. § 103.121(b)(5)(ii). The Agencies agree that a bank may satisfy this requirement by directly providing the notice to any one accountholder of a joint account for delivery to the other owners of the account. Similarly, the bank may open a joint account using information about each of the accountholders obtained from one accountholder, acting on behalf of the other joint accountholders.

**2. How should a bank provide notice to its customer when it engages in indirect lending through a third party such as a mortgage broker or car dealer?**

When a mortgage broker or car dealer is acting as the bank's agent in connection with a loan, the bank may delegate to its agent the obligation to perform the requirements of the bank's CIP rule. In contrast to the reliance provision in the CIP rule, the bank is ultimately responsible for its agent's compliance with the rule. Depending upon the manner in which the account is opened, the agent can provide notice to the bank's customer, for example, by posting a sign, printing the notice on the loan application given to the customer, orally providing the notice, or by providing the notice in any manner that is reasonably designed to ensure that the customer is given notice before opening an account.

**31 C.F.R. § 103.121(b)(6) -- Reliance**

**1. Where a bank is entitled to "rely" on another financial institution to perform its CIP, whose CIP must the relied-upon financial institution implement?**

The reliance provision does not impose on the other financial institution the obligation to duplicate the procedures in the bank's CIP. The reliance provision permits a bank to rely on another financial institution to perform any of the procedures of the bank's CIP, meaning, any of the elements that the CIP rule requires to be in a bank's CIP: (1) identity verification procedures, which include collecting the required information from customers and using some or all of that information to verify the customers' identities; (2) keeping records related to the CIP; (3) determining whether a customer appears on a designated list of known or suspected terrorists or terrorist organizations; and (4) providing customers with adequate notice that information is being requested to verify their identities.

Note that a bank can only use the reliance provision when the other financial institution is regulated by a Federal functional regulator and is subject to a general BSA compliance program rule, they share the customer, the bank can show its reliance upon the other financial institution's performance of an element of the bank's CIP was reasonable under the circumstances, and the requisite contract is signed and certifications provided.

**2. When a longstanding customer of another financial institution (including an affiliate) opens a new account at the bank, can a bank rely on the other financial institution's verification of the identity of the customer performed before a CIP procedure was required?**

A bank that is subject to the CIP rule may rely on another financial institution's verification of the identity of the customer if the requirements of the reliance provision are satisfied. The bank would have to be able to demonstrate that such reliance upon the other financial institution's verification of the identity of the customer is reasonable under the circumstances. For example, the bank could do so by reviewing the relied-upon institution's procedures to ensure that they were adequate although the institution was not yet subject to a CIP rule when it verified the customer's identity.

**In addition, even when a bank is relying on the verification of identity performed by another institution, the bank would continue to be responsible for complying with all remaining requirements of the CIP rule, namely, the requirement that it keep records, provide customer notice, and as soon as a section 326 list has been designated, check the list when a new account is opened.**

**Bank Secrecy Act Examination Procedures**  
**for**  
**Customer Identification Programs**

**Introduction**

The Customer Identification Program (CIP) regulation,<sup>1</sup> 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 non-federally 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.<sup>2</sup>

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.

---

<sup>1</sup> 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).

<sup>2</sup> Non-federally 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" 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.

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.<sup>3</sup> 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.<sup>4</sup> 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.<sup>5</sup> At a minimum, the bank must obtain the following basic information from the customer prior to opening the account<sup>6</sup>:

---

<sup>3</sup> 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.

<sup>4</sup> 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.

<sup>5</sup> 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.

- Name;
- Date of birth, for individuals;
- Address;<sup>7</sup> and
- Identification number.<sup>8</sup>

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, non-documentary 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.

---

<sup>6</sup> For credit card customers, the bank may obtain identifying information from a third-party source prior to extending credit.

<sup>7</sup> 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.

<sup>8</sup> 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).

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 Non-documentary Methods*

Banks are not required to use non-documentary methods to verify a customer's identity. However, a bank using non-documentary methods to verify a customer's identity must have procedures that set forth the methods that the bank will use. Non-documentary 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 non-documentary 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 non-documentary 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.<sup>9</sup> 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."

---

<sup>9</sup> 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.

### ***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 U.S.C. 5318(h)) and is regulated by a federal functional regulator<sup>10</sup>.
- 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.

### ***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)

---

<sup>10</sup> 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.

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, non-systemic 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 U.S.C. 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 208.63). 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 208.63), 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 208.63(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 208.63(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 non-documentary methods,

- c) Identified as high-risk by the bank or the regulator<sup>11</sup>,
- 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)).
- 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 208.62).

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, non-systemic 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 U.S.C. 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).

---

<sup>11</sup> 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.

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:

- d) 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)).