Office of Thrift Supervision
Department of the Treasury

Scott M. Albinson
Managing Director

1700 G Street, N.W., Washington, DC 20552 • (202) 906-7984

May 9, 2003

MEMORANDUM FOR: CHIEF EXECUTIVE OFFICERS

FROM: Scott M. Albinson

SUBJECT: Customer Identification Program Implementation

This CEO Memorandum provides you with additional detail on Treasury's final regulation on Section 326: Customer Identification Program (CIP), published on May 9, 2003. 68 Fed. Reg. 25090 (May 9, 2003) (copy attached.) This Memorandum includes two staff guidance pieces that will help answer questions and provide a framework for achieving compliance with the new regulation. It supplements our March 20, 2002 staff summary of the USA PATRIOT Act and our August 5, 2002 update.

We urge all OTS regulated institutions to carefully review the new requirements of the final regulation. The final regulation includes important changes from the proposed regulation as a result of the comments received by us and the other federal banking agencies. We also urge all thrifts to read the preamble to better understand the intent of the regulatory requirements. Treasury will codify this regulation under its BSA authority, 31 CFR Part 103. OTS regulated institutions are obligated to comply with all regulations promulgated under 31 CFR Part 103.
12 CFR § 563.177.

The CIP regulation is effective October 1, 2003. The regulation requires that, by the effective date, your Board of Directors approve your CIP, you include your CIP in your overall BSA/Anti-Money Laundering policies and procedures, and you fully implement this new integrated program.

OTS will review for compliance with the new regulation during examinations beginning October 1, 2003. OTS is developing revised BSA/AML examination procedures that incorporate USA PATRIOT Act requirements and will publish those procedures before the compliance deadline. In the meantime, please make use of the attached USA PATRIOT Act Preparedness Check-up to assist you in adapting your current policies and procedures to the new requirements.

If you have any questions concerning the final regulation or any other BSA/USA PATRIOT Act related issue, please contact your OTS regional office or consult our new BSA/PATRIOT Act web resource page at www.ots.treas.gov/BSA. You may also call and leave a message on our specially created USA PATRIOT Act phone line, (202) 906-6012.

Attachments

Federal Register

Friday,

May 9, 2003

Part II

Department of the Treasury

31 CFR Part 103

Office of the Comptroller of the Currency

12 CFR Part 21

Office of Thrift Supervision

12 CFR Part 563

Federal Reserve System

12 CFR Parts 208 and 211

Federal Deposit Insurance Corporation

12 CFR Part 326

National Credit Union Administration

12 CFR Part 748

Commodity Futures Trading Commission

17 CFR Parts 1 and 42

Securities and Exchange Commission

17 CFR Part 270 and 31 CFR Part 103

Transactions and Customer Identification Programs; Final Rules and Proposed Rule

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Part 21

[Docket No. 03–08]

RIN 1557–AC06

FEDERAL RESERVE SYSTEM

12 CFR Parts 208 and 211

[Docket No. R–1127]

FEDERAL DEPOSIT INSURANCE CORPORATION

12 CFR Part 326

DEPARTMENT OF THE TREASURY

Office of Thrift Supervision

12 CFR Part 563

[Docket No. 2003–16]

NATIONAL CREDIT UNION ADMINISTRATION

12 CFR Part 748

RIN 3133

DEPARTMENT OF THE TREASURY

31 CFR Part 103

RIN 1506–AA31

Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks

AGENCIES: The Financial Crimes Enforcement Network, 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; National Credit Union Administration.

ACTION: Joint final rule.

SUMMARY: The Department of the Treasury, through the Financial Crimes Enforcement Network (FinCEN), together with the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), and the National Credit Union Administration (NCUA) (collectively, the Agencies), have 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). Section 326 requires the Secretary of the Treasury (Secretary) to jointly prescribe with each of the Agencies, the Securities and Exchange Commission (SEC), and the Commodity Futures Trading Commission (CFTC), a regulation that, at a minimum, requires financial institutions to implement reasonable procedures to verify the identity of any person seeking to open an account, to the extent reasonable and practicable; maintain records of the information used to verify the person's identity; and determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency. This final regulation applies to banks, savings associations, credit unions, private banks, and trust companies.

DATES: *Effective Date:* This rule is effective June 9, 2003.

Compliance Date: Each bank must comply with this final rule by October 1, 2003.

FOR FURTHER INFORMATION CONTACT:

OCC: Office of the Chief Counsel at (202) 874–3295.

Board: Enforcement and Special Investigations Sections at (202) 452–5235, (202) 728–5829, or (202) 452–2961.

FDIC: Special Activities Section, Division of Supervision and Consumer Protection, and Legal Division at (202) 898–3671.

OTS: Compliance Policy Division at (202) 906–6012.

NCUA: Office of General Counsel at (703) 518–6540; or Office of Examination and Insurance at (703) 518–6360.

Treasury: Office of the Chief Counsel (FinCEN) at (703) 905–3590; Office of the General Counsel (Treasury) at (202) 622–1927; or the Office of the Assistant General Counsel for Banking & Finance (Treasury) at (202) 622–0480.

SUPPLEMENTARY INFORMATION:

I. Background

A. Section 326 of the USA PATRIOT Act

On October 26, 2001, President Bush signed into law the USA PATRIOT Act, Pub. L. 107–56. Title III of the Act, captioned ''International Money Laundering Abatement and Anti-terrorist Financing Act of 2001,'' adds several new provisions to the Bank Secrecy Act (BSA), 31 U.S.C. 5311 *et seq.* These provisions are intended to facilitate the prevention, detection, and prosecution of international money laundering and the financing of terrorism.

Section 326 of the Act adds a new subsection (l) to 31 U.S.C. 5318 of the BSA that requires the Secretary to prescribe regulations ''setting forth the minimum standards for financial institutions and their customers regarding the identity of the customer that shall apply in connection with the opening of an account at a financial institution.''

Section 326 applies to all ''financial institutions.'' This term is defined very broadly in the BSA to encompass a variety of entities, including commercial banks, agencies and branches of foreign banks in the United States, thrifts, credit unions, private banks, trust companies, investment companies, brokers and dealers in securities, futures commission merchants, insurance companies, travel agents, pawnbrokers, dealers in precious metals, check-cashers, casinos, and telegraph companies, among many others. *See* 31 U.S.C. 5312(a)(2) and (c)(1)(A).

For any financial institution engaged in financial activities described in section 4(k) of the Bank Holding Company Act of 1956 (section 4(k) institutions), the Secretary is required to prescribe the regulations issued under section 326 jointly with each of the Agencies, the SEC, and the CFTC (the Federal functional regulators).

Section 326 of the Act provides that the regulations must require, at a minimum, financial institutions to implement reasonable procedures for (1) verifying the identity of any person seeking to open an account, to the extent reasonable and practicable; (2) maintaining records of the information used to verify the person's identity, including name, address, and other identifying information; and (3) determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency. In prescribing these regulations, the Secretary is directed to take into consideration the various types of accounts maintained by various types of financial institutions, the various methods of opening accounts, and the various types of identifying information available.

B. Overview of Comments Received

On July 23, 2002, Treasury and the Agencies published a joint notice of proposed rulemaking in the **Federal Register** (67 FR 48290) applicable to (a) any financial institution defined as a ''bank'' in 31 CFR 103.11(c) [1] and

[1] This definition includes banks, savings associations, credit unions, Edge Act and Agreement corporations, and branches and agencies of foreign banks.

subject to regulation by one of the Agencies; and (b) any foreign branch of an insured bank. On the same date, Treasury separately published an identical, proposed rule for credit unions, private banks, and trust companies that do not have a Federal functional regulator (67 FR 48299).[2] Treasury and the Agencies proposed general standards that would require each bank to design and implement a customer identification program (CIP) tailored to the bank's size, location, and type of business. The proposed rule also included certain specific standards that would be mandated for all banks.[3]

Treasury and the Agencies collectively received approximately five hundred comments in response to these proposed rules (collectively referred to as the ''proposal'' or the ''proposed rule'' for ''banks''), although some commenters sent copies of the same letter to Treasury and to each of the Agencies. The majority of comments received by Treasury and the Agencies were from banks, savings associations, credit unions, and their trade associations. Most of these commenters agreed with the largely risk-based approach set forth in the proposal that allowed each bank to develop a CIP based on its specific operations.

Some commenters, however, criticized the specific requirements in the proposed rule and suggested that Treasury and the Agencies issue a final rule containing an entirely risk-based approach without any minimum identification and verification requirements. According to some of these commenters, such a thoroughly risk-based approach would give banks appropriate discretion to focus their efforts and finite resources on specific, high-risk accounts most likely to be used by money-launderers and terrorists.

Other commenters, especially those representing credit card banks and credit card issuers, asserted that the proposed minimum identification and verification requirements should be eliminated because they did not take into account the unique nature of credit card operations. They warned that these requirements, if implemented, would have a chilling effect on credit practices important to U.S. consumers and would impose significant compliance costs on their industry with little benefit to law enforcement.

By contrast, some smaller banks criticized the flexibility of the proposal and stated that a risk-based approach would leave too much room for interpretation by the Agencies. These commenters urged Treasury and the Agencies to issue a final rule establishing more specific requirements. For example, some commenters suggested that the rule prescribe risk assessment levels for each customer type and type of account, along with a specific description of acceptable forms of identification and methods of verification appropriate for each bank's size and location.

While commenters representing various segments of the industry differed on the approach that should be taken in the final rule, the vast majority concluded that Treasury and the Agencies had underestimated the compliance burden that would be imposed by certain elements of the proposal. Commenters were especially concerned about the proposed requirements that banks verify the identity of signatories on accounts, keep copies of documents used to verify a customer's identity, and retain identity verification records for five years after an account is closed.

Some commenters also suggested that banks be given greater flexibility when dealing with established customers and urged that banks be permitted to rely on identification and verification of customers performed by a third party, including an affiliate. Other commenters asked for additional guidance regarding the lists of known and suspected terrorists and terrorist organizations that must be checked, and regarding what will be deemed adequate notice to customers for purposes of complying with the final rule. Many commenters requested that the final rule contain a delayed implementation date that would provide banks with the time needed to design a customer identification program, obtain board approval, alter existing policies and procedures, forms and software, and train staff.

Several comments were received from companies engaged in the sale of technology or services that could be used to identify and verify customers, retain records, and check lists of known and suspected terrorists and terrorist organizations. Many of these companies recommended that the proposed rule be modified to make clear that use of specific products and services would be permissible. Some of these commenters urged that the rule require banks to authenticate any documents obtained to verify the identity of the customer through the use of automated document authentication technology.

A small number of comments were received from individuals. Some of these individuals criticized the proposed requirement that banks obtain a social security number from persons opening an account as an infringement upon individual liberty and privacy. Some individuals were concerned that this requirement would expose them to an added risk of identity theft. Other individuals supported the proposal and concluded that its verification requirements might diminish instances of identity theft and fraud. A few commenters suggested that the government develop a separate national identification number or require that social security cards bear photographs and or other safeguards.

A variety of commenters applauded the efforts of Treasury and the Federal functional regulators to devise a uniform set of rules that apply to banks, broker-dealers, mutual funds, futures commission merchants, and introducing brokers.[4] They noted that, without uniformity, customers of financial institutions may seek to open accounts with institutions that customers perceive to have less robust customer identification requirements. These commenters also suggested revisions that would enhance the uniformity of the rules.

Treasury and the Agencies have modified the proposed rule in light of the comments received. A discussion of the comments, and the manner in which the proposed rule has been modified, follows in the section-by-section analysis.

In addition, as suggested by a number of commenters, Treasury and the Agencies expect to issue supplementary guidance following issuance of the final rule.

C. Joint Issuance by Treasury and the Agencies

The final rule implementing section 326 is being issued jointly by Treasury, through FinCEN, and by the Agencies. It applies to (1) a ''bank,'' as defined in 31 CFR 103.11(c), that is subject to regulation by one of the Agencies, and (2) to any non-Federally insured credit union, private bank or trust company that does not have a Federal functional regulator (collectively referred to in the final rule as ''a bank'').

[2] In the preamble for this proposed rule, Treasury explained that a single final regulation would be issued for all financial institutions defined as ''banks'' under 31 CFR 103.11(c), with modifications to accommodate certain differences between Federally regulated and non-Federally regulated banks. *See* 67 FR 48299, 48300.

[3] At the same time, Treasury also published (1) together with the SEC, proposed rules for broker-dealers (67 FR 48306) and mutual funds (67 FR 48318); and (2) together with the CFTC, proposed rules for futures commission merchants and introducing brokers (67 FR 48328).

[4] *See* footnote 3, *supra.*

The substantive requirements of this joint final rule are being codified as part of Treasury's BSA regulations located in 31 CFR part 103. In addition, each of the Agencies is concurrently publishing a provision in its own regulations [5] to cross-reference this final rule in order to clarify the applicability of the final rule to the banks subject to its jurisdiction.

Regulations governing the applicability of section 326 to certain financial institutions that are regulated by the SEC and the CFTC are the subject of separate rulemakings. Treasury, the Agencies, the SEC, and the CFTC consulted extensively in the development of all joint rules implementing section 326 of the Act. All of the participating agencies intend the effect of the rules to be uniform throughout the financial services industry. Treasury intends to issue separate rules under section 326 for certain non-bank financial institutions that are not regulated by one of the Federal functional regulators.

The Secretary has determined that the records required to be kept by section 326 of the Act have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, to protect against international terrorism.

In addition, Treasury, under its own authority, is issuing conforming amendments to 31 CFR 103.34, which imposes requirements concerning the identification of bank customers.

D. Compliance Date

Nearly all commenters on the proposed rule requested that banks be given adequate time to develop and implement the requirements of any final rule implementing section 326 of the Act. These commenters stated that if the proposed rule were implemented, banks would be required, among other things, to revise existing account opening policies and procedures, obtain board approval, train staff, update forms, purchase new or updated software for customer verification and checking of government lists, and purchase new equipment for copying or scanning and storing records. Commenters requested a delayed effective or compliance date, but, given the variety of banks that would be covered by the final rule, there was no consensus regarding the amount of time that would be necessary to comply with the final rule. The transition periods suggested by commenters ranged from 60 days to two years from the date a final rule is published.

The final rule modifies various aspects of the proposal and eliminates some of the requirements that commenters identified as being most burdensome. Nonetheless, Treasury and the Agencies recognize that some banks will need time to develop a CIP, obtain board approval, and implement the CIP, which will include various measures, such as training of staff, reprinting forms, and developing new software. Accordingly, although this final rule will be effective 30 days after publication, banks are provided with a transition period to implement the rule. Treasury and the Agencies have determined that each bank must fully implement its CIP by October 1, 2003.

II. Section-by-Section Analysis of Final Rule Implementing Section 326

Section 103.121(a) Definitions

Section 103.121(a)(1) Account. The proposed rule defined ''account'' as each formal banking or business relationship established to provide ongoing services, dealings, or other financial transactions and stated that a deposit account, transaction or asset account, and a credit account or other extension of credit would each constitute an ''account.'' [6] The proposal also explained that the term ''account'' was limited to formal banking and business relationships established to provide ''ongoing'' services, dealings, or other financial transactions to make clear that this term is not intended to cover infrequent transactions such as the occasional purchase of a money order or a wire transfer.

Treasury and the Agencies received a large number of comments on this proposed definition. Some commenters agreed with the proposed definition though others thought the definition of ''account'' was either too broad or needed clarification. Some commenters suggested that the definition of ''account'' be narrowed to include only those relationships that are financial in nature. A number of commenters urged that the definition be limited to high-risk relationships that experts have identified as actually used by money launderers and terrorists. Some of these commenters suggested that particular types of accounts, especially those established as part of employee benefit plans, be excluded from the definition of ''account.''

Most commenters requested that the final rule provide additional examples of the relationships that would constitute an ''account.'' Many commenters requested that the rule clarify the meaning of ''ongoing services.'' These commenters asked whether a person who repeatedly and regularly purchased a money order, requested a wire transfer, or cashed a check on a weekly basis, without any other relationship with a bank, would be considered to have an ''account.'' Many other commenters asked that the exclusion for transfers of accounts between banks described in the preamble for the proposal—which commenters characterized as the ''transfer exception'' —be stated expressly in the regulation and expanded to cover all loans originated by a third party and purchased by a bank, such as mortgages purchased from non-bank lenders and vehicle loans purchased from car dealers.

The final rule contains a number of changes prompted by these comments. First, the reference to the term ''business relationship'' has been deleted from the definition of ''account.'' This change is made to clarify that the regulation applies to the bank's provision of financial products and services, as opposed to general ''business'' dealings, such as those in connection with the bank's own operations or premises. Second, the definition now contains additional, but non-exclusive, examples of products and services, such as safety deposit box and other safekeeping services, cash management, and custodian and trust services, that constitute an ''account.''

The definition of ''account'' also has been changed to include a list of products and services that will not be deemed an ''account.'' The preamble for the proposed rule had used the term ''ongoing services'' to define accounts covered by the final rule, and had referred to the exclusion of ''occasional'' transactions and ''infrequent'' purchases (which arguably would require a bank to monitor all transactions for repetitive contacts). By contrast, the final rule clarifies that ''account'' excludes products and services where a *formal banking relationship* is not established with a person, such as check cashing, wire transfer, or the sale of a check or money order.[7] Treasury and the

[5] 12 CFR 21.21 (OCC); 12 CFR 208.63, 211.5, and 211.24 (FRB); 12 CFR 326.8 (FDIC); 12 CFR 563.177 (OTS); and 12 CFR 748.2 (NCUA).

[6] The definition of ''account'' in the proposed rule was based on the statutory definition of ''account'' that is used in section 311 of the Act.

[7] This exclusion is consistent with legislative history indicating that by referencing the term ''customers,'' Congress intended ''that the regulations prescribed by Treasury take an approach similar to that of regulations promulgated under title V of the Gramm-Leach-Bliley Act of 1999, where the Federal functional regulators defined ''customers'' and ''customer relationship'' for purposes of the financial privacy rules.'' H.R. Rep. No. 107–250, pt. 1, at 62 (2001). The definitions of ''customer'' and ''customer

Agencies note that part 103 already requires verification of identity in connection with many of these products and services. *See, e.g.,* 31 CFR 103.29 (purchases of bank checks and drafts, cashier's checks, money orders, and traveler's checks for $3000 or more); 31 CFR 103.33 (funds transfers of $3000 or more).

In addition, the final rule codifies and clarifies the ''transfer exception.'' Under the final rule, the definition of ''account'' excludes accounts that a bank acquires through an acquisition, merger, purchase of assets, or assumption of liabilities from any third party.[8] Treasury and the Agencies note that the Act provides that the regulations shall require reasonable procedures for ''verifying the identity of *any person seeking to open an account.*'' Because these transfers are not initiated by customers, these accounts do not fall within the scope of section 326.[9]

Treasury and the Agencies generally agree with the view expressed by commenters who suggested that a bank's limited resources be focused on relationships that pose a higher risk of money laundering and terrorism. Accordingly, the Agencies have included an exception to the definition of ''account'' for accounts opened for the purpose of participating in an employee benefit plan established pursuant to the Employee Retirement Income Security Act of 1974. These accounts are less susceptible to use for the financing of terrorism and money laundering, because, among other reasons, they are funded through payroll deductions in connection with employment plans that must comply with Federal regulations which impose various requirements regarding the funding and withdrawal of funds from such accounts, including low contribution limits and strict distribution requirements.

Section 103.121(a)(2) Bank. The proposal jointly issued by Treasury and the Agencies applied to any financial institution defined as a ''bank'' in 31 CFR 103.11(c) and subject to regulation by one of the Agencies, including banks, savings associations, credit unions, Edge Act and Agreement corporations, and branches and agencies of foreign banks. The proposed definition also included ''any foreign branch of an insured bank'' to make clear that the procedures required by the rule would have to be implemented throughout the bank, no matter where its offices are located. The preamble for the proposal explained that the rule would apply to bank subsidiaries to the same extent as existing regulations requiring banks to have BSA compliance programs.[10] As described above, a second proposal issued simultaneously by Treasury applied to certain other financial institutions defined as a ''bank'' in 31 CFR 103.11(c), namely, those credit unions, private banks, and trust companies that do not have a Federal functional regulator.

Under the final rule, ''bank'' includes all financial institutions covered by both of the proposals described above, except that ''bank'' does not include any foreign branch of an insured U.S. bank. Several commenters explained that the proposal to cover foreign branches might conflict with local laws applicable to branches of insured banks operating outside of the United States and might place U.S. institutions at a competitive disadvantage. Consistent with the approach taken with respect to final regulations implementing other sections of the Act,[11] Treasury and the Agencies have determined that foreign branches of insured U.S. banks are not covered by the final rule. Nevertheless, Treasury and the Agencies encourage each bank to implement an effective CIP, as required by this final rule, throughout its organization, including in its foreign branches, except to the extent that the requirements of the rule would conflict with local law.

As noted in the preamble for the proposal, the CIP must be a part of a bank's BSA compliance program. Therefore, it will apply throughout such a bank's U.S. operations (including subsidiaries) in the same way as the BSA compliance program requirement. However, all subsidiaries that are in compliance with a separately applicable, industry-specific rule implementing section 326 of the Act will be deemed to be in compliance with this final rule.

Section 103.121(a)(3) Customer. The proposal defined ''customer'' to mean any person [12] seeking to open a new account. In addition, the proposal defined a ''customer'' to include any signatory on an account. The preamble for the proposal explained that the term ''customer'' included a person that applied to open an account, but not someone seeking information about an account, such as rates charged or interest paid on an account, if the person did not apply to open an account. The preamble also stated that any person seeking to open an account at a bank, on or after the effective date of the final rule, would be a ''customer,'' regardless of whether that person already had an account at the bank.

This proposed definition prompted a large number of comments. First, nearly all commenters recommended that the Agencies clarify in the text of the final rule that ''customer'' does not include a person who does not receive banking services, such as a person whose deposit or loan application is denied. Some of these commenters suggested that the rule for banks define ''customer'' to mean ''a person who opens a new account,'' as did the proposed rules for broker-dealers, mutual funds, futures commission merchants and introducing brokers.

relationship'' in the financial privacy rules apply only to a consumer who has a ''continuing relationship'' with a bank, for example, in the form of a deposit or investment account, or a loan. *See* .3(h) and (i) of 12 CFR part 40 (OCC); 12 CFR part 216 (Board); 12 CFR part 332 (FDIC); 12 CFR part 573 (OTS); and 12 CFR part 716 (NCUA).

[8] In many cases, these third parties are themselves ''financial institutions'' for purposes of the BSA. Treasury anticipates that these third parties ultimately will be subject to their own customer identification rules implementing section 326 of the Act in the event that they are not presently covered by such a rule.

[9] Nevertheless, there may be situations involving the transfer of accounts where it would be appropriate for a bank, as part of the customer due diligence procedures required under existing regulations requiring banks to have compliance programs implementing the BSA (BSA compliance programs), to verify the identity of customers associated with accounts that it acquires from another financial institution. Treasury and the Agencies expect financial institutions to implement reasonable procedures to detect money laundering in any account, however acquired.

[10] All insured depository institutions currently must have a BSA compliance program. *See* 12 CFR 21.21 (OCC); 12 CFR 208.63 (Board); 12 CFR 326.8 (FDIC); 12 CFR 563.177 (OTS); and 12 CFR 748.2 (NCUA). In addition, all financial institutions are required by section 352 of the Act, 31 U.S.C. 5318(h), to develop and implement an anti-money laundering program. Treasury issued a regulation implementing section 352 providing that a financial institution regulated by a Federal functional regulator is deemed to satisfy the requirements of section 5318(h)(1) if it implements and maintains an anti-money laundering program that complies with the regulation of its Federal functional regulator, *i.e.,* the requirement to implement a BSA compliance program. *See* 31 CFR 103.120(b); 67 FR 2113 (April 29, 2002). However, Treasury temporarily deferred subjecting certain non-Federally regulated banks to the anti-money laundering program requirements in section 352. *See* 67 FR 67547 (November 6, 2002) (corrected 67 FR 68935 (November 14, 2002)).

[11] *See, e.g.,* 67 FR 60562, 60565 (Sept. 26, 2002) (FinCEN's regulation titled ''Anti-Money Laundering Requirements ''Correspondent Accounts for Foreign Shell Banks: Recordkeeping and Termination of Correspondent Accounts for Foreign Banks' implementing sections 313 and 319(b) of the Act).

[12] The proposed rule defined ''person'' by reference to § 103.11(z). This definition includes individuals, corporations, partnerships, trusts, estates, joint stock companies, associations, syndicates, joint ventures, other unincorporated organizations or groups, certain Indian Tribes, and all entities cognizable as legal personalities. Treasury and the Agencies agree that it is not necessary to repeat this definition. Therefore, it is omitted from the final rule.

Treasury and the Agencies agree with the view expressed by some commenters that the statute should be construed to ensure that banks design procedures to determine the identity of only those persons who open accounts. Accordingly, the final rule defines a ''customer'' as ''a person that opens a new account.'' [13] For example, in the case of a trust account, the ''customer'' would be the trust. For purposes of this rule, a bank will not be required to look through trust, escrow, or similar accounts to verify the identities of beneficiaries and instead will only be required to verify the identity of the named accountholder.[14] In the case of brokered deposits, the ''customer'' will be the broker that opens the deposit account. A bank will not need to look through the deposit broker's account to determine the identity of each individual sub-account holder; it need only verify the identity of the named accountholder.

Many commenters requested that the final rule clarify whether ''customer'' includes a minor child or an informal group with a common interest, such as a club account, where there is no legal entity. The final rule addresses these comments by providing that ''customer'' means ''an individual who opens a new account for (1) an individual who lacks legal capacity, such as a minor; or (2) an entity that is not a legal person, such as a civic club.''

A few banks stated that defining ''customer'' to include a signatory was consistent with their current practice of verifying the identity of the named accountholder and any signatory on the account. However, most commenters strenuously objected to the inclusion of a signatory as a customer whose identity must be verified, and asserted that this proposed requirement would deviate significantly from their current business practices. These commenters stated that requiring banks to verify signatories on an account would be enormously burdensome to the financial institutions and signatories themselves—many of whom simply work as employees for firms with corporate accounts—and would outweigh any benefit.[15] One commenter asserted that inclusion of signatories as customers went beyond the scope of section 326 of the Act. Although some commenters advocated that any requirement regarding a signatory should be omitted altogether, these commenters generally advocated a risk-based approach that would give banks the discretion to determine when a signatory's identity should be verified.

Credit card banks, in particular, were critical of the signatory requirement because the proposed provision, as drafted, encompassed all authorized users of credit cards. These banks characterized the signatory requirement as unnecessary in the case of credit card companies, which, they explained, already use sophisticated fraud filters to detect fraud and abnormal use. These banks also noted that a person need not be a signatory to use another person's credit card, especially when purchasing products by telephone or over the Internet. Therefore, the signatory requirement would not necessarily ensure that banks would be able to verify the identity of those using a credit card account.

After revisiting the issue of whether a signatory should be a ''customer,'' Treasury and the Agencies have determined that requiring a bank to expend its limited resources on verifying the identity of all signatories on accounts could interfere with the bank's ability to focus on identifying customers and accounts that present a higher risk of not being properly identified. Accordingly, the proposed provision defining ''customer'' to include a signatory on an account is deleted. Instead, the final rule, at § 103.121(b)(2)(ii)(C), requires a bank's CIP to address situations when the bank will take additional steps to verify the identity of a customer that is not an individual by seeking information about individuals with authority or control over the account, including signatories, in order to verify the customer's identity.

In addition to defining who is a ''customer,'' the final rule contains a list of entities that will not be deemed ''customers.'' Many commenters questioned why a bank should be required to verify the identity of a government agency or instrumentality opening a new account, or of a publicly-traded company that is subject to SEC reporting requirements. Consistent with these and other comments urging that the final rule focus on requiring verification of the identity of customers that present a higher risk of not being properly identified, the final rule excludes from the definition of ''customer'' the following readily identifiable entities: a financial institution regulated by a Federal functional regulator; a bank regulated by a state bank regulator; and governmental agencies and instrumentalities, and companies that are publicly traded described in § 103.22(d)(2)(ii)–(iv).[16] Section 103.22(d)(2)(iv) exempts such companies only to the extent of their domestic operations. Accordingly, a bank's CIP will apply to any foreign offices, affiliates, or subsidiaries of such entities that open new accounts.

A great many commenters also objected to the requirement in § 103.121(b)(2)(ii) of the proposed rule that a bank verify the identity of an existing customer seeking to open a new account unless the bank previously verified the customer's identity in accordance with procedures consistent with the proposed rule and continues to have a reasonable belief that it knows the true identity of the customer. These commenters asserted that such a requirement would be burdensome for the bank and would upset existing customers. Some commenters recommended that the rule apply prospectively to new customers who previously had no account with the bank. Many commenters suggested that the final rule contain a risk-based approach where verification would not be required for an existing customer who opens a new account if the bank has a reasonable belief that it knows the identity of the customer, regardless of the procedures the bank followed to form this belief.

[13] Therefore, each person named on a joint account is a ''customer'' under this final rule unless otherwise provided.

[14] However, based on a bank's risk assessment of a new account opened by a customer that is not an individual, a bank may need to take additional steps to verify the identity of the customer by seeking information about individuals with ownership or control over the account in order to identify the customer, as described in § 103.121(b)(2)(ii)(C), or may need to look through the account in connection with the customer due diligence procedures required under other provisions of its BSA compliance program.

[15] Commenters contended that banks and individuals would confront numerous practical problems. Some commenters noted, for example, that the identification and verification of signatories could be burdensome for banks because business accounts might have many signatories and those signatories would change over time. Some commenters explained that collecting detailed information about an employee who is a signatory would raise privacy concerns for those employees who would be required to disclose personal information to their employer's financial institutions. Other commenters stated that a signatory rarely is present at the time of account opening and, consequently, a bank would encounter substantial obstacles when attempting to verify the signatory's identity using any of the most common methods described in the proposal, including by examining documents or by obtaining a credit report. (Under the Fair Credit Reporting Act (FCRA), a consumer reporting agency generally may furnish a consumer report in connection with transactions involving the consumer and no other. *See* 15 U.S.C. 1681b. Thus, for example, a bank would be prohibited from obtaining a credit report to verify the identity of an authorized user of a customer's credit card.)

[16] Treasury previously determined that banks should be exempted from having to file reports of transactions in currency in connection with these entities. *See* 31 CFR 103.22(d)(1).

Treasury and the Agencies acknowledge that the proposed rule might have had unintended consequences for bank-customer relationships and that the risk-based approach suggested by commenters would avoid these consequences. Accordingly, the final rule excludes from the definition of ''customer'' 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.[17]

Section 103.121(a)(4) Federal functional regulator. The proposed rule defined ''Federal functional regulator'' by reference to § 103.120(a)(2), meaning each of the Agencies, the SEC, and the CFTC. There were no comments on this definition, and Treasury and the Agencies have adopted it as proposed.

Section 103.121(a)(5) Financial institution. The final rule includes a new definition for the term ''financial institution'' that cross-references the BSA, 31 U.S.C. 5312(a)(2) and (c)(1). This is a more expansive definition of ''financial institution'' than that in 31 CFR 103.11, and includes entities such as futures commission merchants and introducing brokers.

Section 103.121(a)(6) Taxpayer identification number. The proposed rule repeated the language from § 103.34(a)(4), which states that the provisions of section 6109 of the Internal Revenue Code and the regulations of the Internal Revenue Service thereunder determine what constitutes ''a taxpayer identification number.'' There were no comments on this approach, and Treasury and the Agencies have adopted it substantially as proposed, with minor technical modifications.

Section 103.121(a)(7) and (8) U.S. Person and non-U.S. person. The proposed rule provided that ''U.S. person'' is an individual who is a U.S. citizen, or an entity established or organized under the laws of a State or the United States. A ''non-U.S. person'' was defined as a person who did not satisfy either of these criteria.

As described in greater detail below, a bank is generally required to obtain a U.S. taxpayer identification number from a customer who opens a new account. However, if the customer is a non-U.S. person and does not have such a number, the bank may obtain an identification number from some other form of government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

Several commenters suggested that it would be less confusing to bankers if ''U.S. person'' meant both a U.S. citizen and a resident alien, consistent with the definition of this term used in the Internal Revenue Code (IRS definition).[18] A few commenters criticized the proposed definition because it would require banks to establish whether a customer is or is not a U.S. citizen.

Treasury and the Agencies believe that the proposed definition of ''U.S. person'' is a better standard for purposes of this final rule than the IRS definition. Adoption of the IRS definition of ''U.S. person'' would require bank staff to distinguish among various tax and immigration categories in connection with any type of account that is opened. Under the proposed definition, a bank will not necessarily need to establish whether a potential customer is a U.S. citizen. The bank will have to ask each customer for a U.S. taxpayer identification number (social security number, employer identification number, or individual taxpayer identification number). If a customer cannot provide one, the bank may then accept alternative forms of identification. For these reasons, the definition is adopted as proposed.

Section 103.121(b) Customer Identification Program: Minimum Requirements

Section 103.121(b)(1) General Rule. The proposed rule required each bank to implement a CIP that is appropriate given the bank's size, location, and type of business. The proposed rule required a bank's CIP to contain the statutorily prescribed procedures, described these procedures, and detailed certain minimum elements that each of the procedures must contain. In addition, the proposed rule required that the CIP be written and that it be approved by the bank's board of directors or a committee of the board.

The proposed rule also stated that the CIP must be incorporated into the bank's BSA[19] 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. It must include (1) internal policies, procedures, and controls to ensure ongoing compliance; (2) designation of a compliance officer; (3) an ongoing employee training program; and (4) an independent audit function to test programs. The preamble for the proposal explained that the CIP should be incorporated into each of these four elements of a bank's BSA program.

Most commenters agreed with the proposal's approach of allowing banks to develop risk-based programs tailored to their specific operation, though some of these commenters recommended that Treasury and the Agencies adopt an entirely risk-based approach without any minimum requirements while others recommended a more prescriptive approach. Many commenters suggested that Treasury and the Agencies clarify the extent to which a bank could rely on a third party, especially an affiliate, to perform some or all aspects of its CIP.

Other commenters focused on the requirement that a bank's board of directors approve the CIP. These commenters urged Treasury and the Agencies to adopt a regulation that states that the role of a bank's board of directors need only be to approve broad policy rather than the specific methods or actual procedures that will be a part of a bank's CIP. One commenter recommended that the governing body of a financial institution be permitted to delegate its responsibility to approve the CIP.

The final rule attempts to strike an appropriate balance between flexibility and detailed guidance by allowing a bank broad latitude to design and implement a CIP that is tailored to its particular business practices while providing a framework of minimum standards for identifying each customer, as the Act mandates. Following the description of the procedures and minimum requirements for each element of a bank's CIP (identity verification, recordkeeping, comparison with government lists, and customer notice), the final rule contains a new section describing the extent to which a bank may rely on a third party to perform these elements, described in detail below.

The final rule removes the requirement that the bank's board of directors or a committee of the board must approve the bank's CIP because this requirement is redundant. A bank's BSA compliance program must already be approved by the board. Treasury and the Agencies regard the addition of a CIP to the bank's BSA compliance program to be a material change in the BSA compliance program that will require board approval. The board of director's responsibility to oversee bank compliance with section 326 of the Act

[17] As a foreign branch of an insured U.S. bank is no longer a ''bank'' for purposes of this rule, a customer of a bank's foreign branch will no longer be ''a person who has an existing account with the bank.'' Therefore, the bank must verify the identity of a customer of its foreign branch in accordance with its CIP if such a customer opens a new account in the U.S.

[18] 26 U.S.C. 7701(a)(30)(A).

[19] *See* footnote 10, supra.

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

The final rule will apply to some non-Federally regulated banks that are not yet subject to an anti-money laundering compliance program requirement.[20] Therefore, the final rule only 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.[21]

Section 103.121(b)(2) Identity Verification Procedures. The proposed rule provided that each bank must have a CIP that includes procedures for verifying the identity of each customer, to the extent reasonable and practicable, based on the bank's assessment of certain risks. The proposed rule stated that these procedures must enable the bank to form a reasonable belief that it knows the true identity of the customer.

Some commenters recommended that the identity verification requirement be waived for new customers that are well known to a senior officer of the bank. Some of these commenters endorsed such a waiver provided that a bank employee could provide ''an affidavit of identity'' on behalf of the customer.

One commenter criticized the standard requiring a bank to have identity verification procedures ''that enable the bank to form a reasonable belief that it knows the true identity of the customer'' as too subjective. This commenter suggested that a better standard would be lack of affirmative notice of deficiency in the identity process. Another commenter suggested that the rule make clear that a bank is only required to verify a customer's identity, to the extent reasonable and practical, in order to establish that it has a reasonable basis for knowing the true identity of its customer.

The final rule provides that a bank's CIP must include risk-based procedures for verifying the identity of each customer[22] to the extent reasonable and practicable. The final rule also states that the procedures must enable the bank to form a reasonable belief that it knows the true identity of the customer. As section 326 of the Act states, a bank's affirmative obligation to verify the identity of its customer applies to ''any person'' rather than only to a person whose identity is suspect, as suggested by one commenter. Furthermore, Treasury and the Agencies have determined that the statutory obligation to ''*verify* the identity of any person'' requires the bank to implement and follow procedures that allow the bank to have a reasonable belief that it knows the true identity of the customer.

Given the flexibility built into the final rule, Treasury and the Agencies believe that it is not appropriate to provide special treatment for new customers known to bank personnel. In addition, permitting reliance on bank personnel to attest to the identity of a customer may be subject to manipulation. Accordingly, the final rule does not establish different rules for customers who are known to bank personnel.

The final rule requires the identity verification procedures to be based upon relevant risks, including those presented by the types of accounts maintained by the bank, the various methods of opening accounts provided by the bank, and the types of identifying information available. In addition to these risk factors, which are specifically identified in section 326, the final rule states that the procedures should take into account the bank's size, location, and type of business or customer base, additional factors mentioned in the Act's legislative history.[23]

Section 103.121(b)(2)(i) Customer Information Required. The proposed rule required that a bank's CIP must contain procedures that specify the identifying information the bank must obtain from a customer. It stated that, at a minimum, a bank must obtain from each customer the following information prior to opening an account: (1) Name; (2) address (a residential and mailing address for individuals, and principal place of business and mailing address for a person other than an individual); (3) date of birth for individuals; and (4) an identification number.

Treasury and the Agencies received a variety of comments criticizing the requirement that a bank obtain certain minimum identifying information prior to opening an account. Some commenters, including a trade association representing large financial institutions, recommended that a bank be permitted to open an account for a customer who lacks some of the minimum identifying information, provided that the bank has formed a reasonable belief that it knows the true identity of the customer. Credit card banks explained that the minimum information requirement would create problems for retailers that offer credit cards at the point of sale. These commenters stated that retailers were not likely to have the means to record identifying information other than what is currently collected. They suggested that when there are systems in place to identify customers and detect suspicious transactions, the rule should require only the collection of information that the credit card bank or card issuer deems necessary and appropriate to identify the customer.

Other commenters stated that the rule should not require a bank to obtain the minimum identifying information prior to account opening in every instance. Some of these commenters suggested that a bank be permitted to obtain the required information within a reasonable time after the account is opened. Some commenters suggested that the rule permit banks to obtain identifying information from a party other than the customer. This would arise, for example, when a bank offers a credit card based on information obtained from a credit reporting agency. Other commenters suggested that a bank also be required to obtain information about a customer's occupation, profession or business, as this information is needed by a bank that intends to file a report of transactions in currency or a suspicious activities report on the customer.

Consistent with the proposal, the final rule provides that a bank's CIP must contain procedures that specify the identifying information that the bank must obtain from each customer prior to opening an account. In addition, the rule specifies the four basic categories of information that a bank must obtain from the customer prior to opening an account. Treasury and the Agencies believe that requiring banks to gather these standard forms of information prior to opening an account is not overly burdensome because such identifying information is routinely

[20] *See* footnote 10, *supra.*

[21] The final rule therefore provides that until such time as credit unions, private banks, and trust companies without a Federal functional regulator are subject to such a program, their CIPs must be approved by their boards of directors.

[22] Other elements of the bank's CIP, such as procedures for recordkeeping or checking of government lists, are requirements that may not vary depending on risk factors.

[23] H.R. Rep. No. 107–250, pt. 1, at 62 and 63 (2001).

gathered by most banks in the account opening process and is required by other sections of 31 CFR part 103. Of course, based upon an assessment of the risks described above, a bank may require a customer to provide additional information to establish the customer's identity.

Treasury and the Agencies acknowledge that imposing this requirement on banks that offer credit card accounts is likely to alter the manner in which they do business by requiring them to gather additional information beyond that which they currently obtain directly from a customer who opens an account at the point of sale or by telephone. Treasury and the Agencies are mindful of the legislative history of section 326, which indicates that Congress expected the regulations implementing this section to be appropriately tailored for accounts opened in situations where the account holder is not physically present at the financial institution and that the regulations should not impose requirements that are burdensome, prohibitively expensive, or impractical.[24]

Therefore, Treasury and the Agencies have included an exception in the final rule 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. Treasury and the Agencies recognize that these practices have produced an efficient and effective means of extending credit with little risk that the lender does not know the identity of the borrower.

Treasury and the Agencies also received comments on the advisability of requiring banks to collect the specific identifying information (name, date of birth, address, and identification number), as would have been required under the proposed rule. With respect to obtaining the customer's name, one commenter recommended that based on Texas law and banks' experience, a bank should be required to obtain the name under which the customer is doing business and the customer's legal name. The final rule continues to require that the bank obtain the customer's name, meaning a legal name that can be verified. As noted above, this is a minimum requirement, and a bank may also need to obtain the name under which a person does business in order to establish a reasonable belief it knows the true identity of the customer.

One trade association suggested that banks be permitted to make a risk-based determination before requiring a customer to provide date of birth because many customers would prefer not to share this information. One commenter stated that date of birth is not an important identifying characteristic and should be deleted. Another commenter stated that credit card issuers do not request this information because it can raise fair lending issues. Finally, a few commenters noted that standardized mortgage applications require age rather than date of birth and would have to be altered.

The final rule provides that a bank must obtain the date of birth for a customer who is an individual. Treasury and the Agencies believe that date of birth is an important identifying characteristic and can be used to provide a bank or law enforcement with an additional means to distinguish between customers with identical names. However, the required collection and retention of information about a customer's date of birth does not relieve the bank from its obligations to comply with anti-discrimination laws or regulations, such as the prohibition in the Equal Credit Opportunity Act against discrimination in any aspect of a credit transaction on the basis of age or other prohibited classification. Banks collecting date of birth from individual customers should be able to take reasonable measures to convert this information into age for purposes of the forms used in the secondary mortgage market given the delayed compliance date for the final rule.

Many commenters criticized the requirement that a bank obtain both the customer's physical and mailing address, if different. Most commenters urged Treasury and the Agencies to eliminate the requirement that the customer provide a physical address. Some of these commenters stated that this requirement could interfere with the ability of certain segments of the population to obtain a bank account, such as members of the military, persons who reside in mobile homes with no fixed address, and truck drivers who do not have a physical address. Banks that offer credit card accounts and card issuers stated that the address requirement would be extremely burdensome because they would have to change the manner in which they do business, and in some cases, credit card banks currently do not have the capacity to collect both addresses. Some of these commenters stated that new credit card customers are reluctant to give more than one address and, therefore, it would be difficult to obtain this information from customers. A trade association representing credit card banks asserted that customers may have a legitimate reason for handling correspondence through post office boxes and should not have to provide a physical address. This commenter asserted that requiring the customer to provide a physical address will discourage the provision of financial services to the unbanked and will prevent a victim of identity theft from using an alternative to an unsecured home mailbox. Another commenter noted that the physical address of a customer's principal place of business may not be relevant if the bank is working with a customer's local office. This commenter recommended that the rule simply permit the bank to obtain the customer's street address. Credit card banks and issuers urged Treasury and the Agencies to make the requirement that a bank obtain the customer's physical address optional.

Section 326 of the Act requires Treasury and the Agencies to prescribe regulations that require financial institutions to implement ''reasonable procedures.'' Accordingly, under the final rule, a bank will not be required to obtain more than a single address for a customer. Nonetheless, Treasury and the Agencies believe that the identification, verification, and recordkeeping provisions of the Act, taken together, should provide appropriate resources for law enforcement agencies to investigate money laundering and terrorist financing. The final rule therefore provides that a bank generally must obtain a residential or business street address for a customer who is an individual because Treasury and the Agencies have determined that law enforcement agencies should be able to contact an individual customer at a physical location, rather than solely through a mailing address. Treasury and the Agencies recognize that this provision may be impracticable for members of the military who cannot readily provide a physical address, and other individuals who do not have a physical address but who reliably can be contacted. Accordingly, the final rule provides an exception under these circumstances that allows a bank to obtain an Army Post Office or Fleet Post Office box number, or the residential or business street address of next of kin or of another contact individual. For a customer other than an individual, such as a corporation, partnership, or trust, the bank may obtain the address of the principal place of business, local office,

[24] H.R. Rep. No. 107–250, pt. 1, at 63 (2001).

or other physical location of the customer. Of course, a bank is free to obtain additional addresses from the customer, such as the customer's mailing address, to meet its own or its customer's business needs.

The proposal required that banks obtain an identification number from customers. For U.S. persons, a bank would have been required to obtain a U.S. taxpayer identification number. For non-U.S. persons, a bank would have been required to obtain a number from various alternative forms of government-issued identification.

One commenter stated that this requirement would not be burdensome. Commenters representing certain consumer advocacy groups commended Treasury and the Agencies for providing banks with the discretion to accept alternative forms of identifying information from non-U.S. citizens. These commenters stated that this position would assist low-income immigrants in gaining financial stability. By contrast, some commenters stated that the final rule should not permit a bank to open an account for a customer using only a foreign identification number when the customer provides a U.S. address. Other commenters asked for guidance on whether a bank is permitted to accept a number from the identification document issued by a foreign government. A few commenters urged the government to require a national identification document for all individuals.

Other commenters, primarily credit card banks, stated that the requirement that a bank obtain a U.S. taxpayer identification number from U.S. persons would create considerable hardship. They stated that new credit card customers are reluctant to give out their social security numbers, especially over the telephone. They urged that banks be given the discretion to collect identifying information, other than social security numbers, when appropriate in light of consumer privacy and security concerns. In the alternative, they recommended that banks be permitted to obtain a U.S. taxpayer identification number for U.S. persons from a trusted third party source, such as a credit reporting agency.

Some commenters questioned what number to use for accounts opened in the name of a bowling league or class reunion, or to accept donations for a special cause. Other commenters questioned what number could be obtained from foreign businesses and enterprises that have no taxpayer identification number or other government-issued documentation.

The final rule provides that a bank must obtain an ''identification number'' from every customer. As discussed above, under the definition of ''customer,'' the final rule permits a bank to obtain the identification number of the individual who opens an account in the name of an individual who lacks legal capacity, such as a minor, or a civic group, such as a bowling league.

After reviewing the comments, Treasury and the Agencies have determined that requiring a bank to obtain a customer's identification number, such as a social security number, from the customer himself or herself, in every case, including over the telephone, would be unreasonable and impracticable because it would be contrary to banks' current practices and could alienate many potential customers. Accordingly, Treasury and the Agencies have adopted an exception for credit card accounts that will permit a bank offering such accounts to acquire information about the customer, including an identification number, from a trusted third party source prior to extending credit to the customer, rather than having to obtain this information directly from the customer prior to opening an account.

The final rule also provides that for a non-U.S. person, a bank must obtain one or more of the following: A taxpayer identification number (social security number, individual taxpayer identification number, or employer identification number); passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard. This standard provides a bank with some flexibility to choose among a variety of identification numbers that it may accept from a non-U.S. person.[25] However, the identifying information the bank accepts must permit the bank to establish a reasonable belief that it knows the true identity of the customer.

Treasury and the Agencies emphasize that the final rule neither endorses nor prohibits bank acceptance of information from particular types of identification documents issued by foreign governments. A bank must decide for itself, based upon appropriate risk factors, including those discussed above (the types of accounts maintained by the bank, the various methods of opening accounts provided by the bank, the other types of identifying information available, and the bank's size, location, and customer base), whether the information presented by a customer is reliable.

Treasury and the Agencies recognize that a foreign business or enterprise may not have a taxpayer identification number or any other number from a government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard. Therefore, the final rule notes that when opening an account for such a customer, the bank must request alternative government-issued documentation certifying the existence of the business or enterprise.

The proposal also contained a limited exception to the requirement that a bank obtain a taxpayer identification number from a customer opening a new account. The exception permitted a bank to open an account for a person other than an individual (such as a corporation, partnership, or trust) that has applied for, but has not received, an employer identification number (EIN), provided that the bank obtains a copy of the application before it opens the account and obtains the EIN within a reasonable period of time after the account is established. The preamble for the proposed rule explained that this exception was included for a new business that might need access to banking services, particularly a bank account or an extension of credit, before it has received an EIN from the Internal Revenue Service.

Some commenters questioned this limited exception for certain businesses. A few commenters suggested expanding the exception to include individuals who have applied for, but have not yet received a taxpayer identification number. Another commenter stated that the exception provided no added benefit and would add to a bank's recordkeeping and monitoring burden.

Treasury and the Agencies have determined that a bank should be afforded more flexibility in situations where a person, including an individual, has applied for, but has not yet received, a taxpayer identification number. Therefore, the final rule states that instead of obtaining a taxpayer identification number from a customer prior to opening an account, the CIP may include procedures for opening an account for a customer (including an individual) that has applied for, but has not received, a taxpayer identification

[25] The rule provides this flexibility because there is no uniform identification number that non-U.S. persons would be able to provide to a bank. *See* Treasury Department, ''A Report to Congress in Accordance with Section 326(b) of the USA PATRIOT Act,'' October 21, 2002.

number.[26] To lessen the recordkeeping burden for a bank that elects to use this exception, the final rule also provides that the bank's CIP need only include procedures requiring the bank 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. Thus, a bank will be able to exercise its discretion [27] to determine how to confirm that a customer has filed an application for a taxpayer identification number rather than having to keep a copy of the application on file.

Section 103.121(b)(2)(ii) Customer Verification. The proposed rule provided that the CIP must contain risk-based procedures for verifying the information that the bank obtains in accordance with § 103.121(b)(2)(i), within a reasonable period of time after the account is opened.[28] The proposed rule also described when a bank is required to verify the identity of existing customers.

Several commenters asked Treasury and the Agencies to underscore that these verification procedures may be risk-based by noting that a bank may verify less than all of the identifying information provided by the customer. Many commenters noted that there is currently no reliable, efficient, or effective means of verifying a customer's social security number. Some of these commenters asked the government to establish a method that would permit banks to establish the authenticity and accuracy of a customer's name and taxpayer identification number.

Treasury and the Agencies recognize that there currently is no method that would permit a bank to verify, for example, a taxpayer identification, passport or alien identification number through an official source. Accordingly, 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. Thus, 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.

Some commenters stated that they appreciated the flexibility of the proposal permitting an institution to determine how soon identity must be verified. Other commenters asked Treasury and the Agencies to clarify what is a ''reasonable period of time.'' As stated in the preamble for the proposal, Treasury and the Agencies believe that the amount of time it will take an institution to verify a customer's identity may depend upon various factors, such as the type of account opened, whether the customer is physically present when the account is opened, and the type of identifying information available. For the same reasons, the final rule provides banks with the flexibility necessary to accommodate a wide range of situations by stating that the bank must verify the identifying information within a reasonable time after the account is opened.[29]

As discussed above in the definition section, many commenters criticized the proposed approach regarding verification of existing customers that open new accounts. The final rule addresses these concerns by modifying the definition of ''customer'' to exclude a person who has an existing account with the bank if the bank has a reasonable belief that it knows the true identity of the person.

Many commenters urged that the final rule continue to allow, but not mandate, documentary verification. A few commenters requested that the final rule provide additional guidance on verification. Some commenters asked that the final rule clarify that a bank may choose to use only documentary methods and may refuse to open an account using other methods.

The final rule addresses these comments by stating that a bank's CIP's verification procedures must describe when the bank will use documents, non-documentary methods, or a combination of both methods to verify a customer's identity.

Section 103.121(b)(2)(ii)(A) Verification Through Documents. The proposed rule provided that the CIP must contain procedures describing when the bank will verify identity through documents and setting forth the documents that the bank will use for this purpose. It then gave examples of documents that could be used to verify the identity of individuals and other persons such as corporations, partnerships, and trusts.

Most commenters noted that banks do not have the means to authenticate or validate documents provided by their customers and urged Treasury and the Agencies to clarify that document authentication is not a CIP requirement. Treasury and the Agencies wish to confirm that once a bank has obtained and verified the identity of the customer through a document such as a driver's license or passport, the bank will not be required to take steps to determine whether the document has been validly issued. A bank generally may rely on government-issued identification as verification of a customer's identity; however, if a document shows obvious indications of fraud, the bank must consider that factor in determining whether it can form a reasonable belief that it knows the customer's true identity.

Some commenters also asked that Treasury and the Agencies provide more examples and discuss appropriate types of documentary identification in the final rule or in separate guidance that banks may easily access. Commenters asked whether a utility bill, or library card addressed to the same physical address and name of the person seeking the account, or a foreign identification card, such as a foreign voter registration card or driver's license, would be acceptable. Some commenters questioned whether copies of documents would suffice.

Given the recent increases in identity theft and the availability of fraudulent documents, Treasury and the Agencies agree with a commenter who suggested that the value of documentary verification is enhanced by redundancy. The rule gives examples of types of documents that are considered reliable. However, a bank is encouraged to obtain more than one type of documentary verification to ensure that it has a reasonable belief that it knows the customer's true identity. Moreover, banks are encouraged to use a variety of methods to verify the identity of a customer, especially when the bank does not have the ability to examine original documents.

The final rule attempts to strike the appropriate balance between the

[26] This position is analogous to that in regulations issued by the Internal Revenue Service (IRS) concerning ''awaiting-TIN [taxpayer identification number] certificates.'' The IRS permits a taxpayer to furnish an ''awaiting-TIN certificate'' in lieu of a taxpayer identification number to exempt the taxpayer from the withholding of taxes owed on reportable payments (*i.e.*, interest and dividends) on certain accounts. *See* 26 CFR 31.3406(g)–3.

[27] For example, the bank may wish to examine a copy of the application filed.

[28] The preamble for the proposed rule noted that, although an account may be opened, it is common practice among banks to place limits on the account, such as by restricting the number of transactions or the dollar value of transactions, until a customer's identity is verified. Therefore, the proposed regulation provided the bank with the flexibility to use a risk-based approach to determine how soon identity must be verified.

[29] It is possible that a bank would, however, violate other laws by permitting a customer to transact business prior to verifying the customer's identity. *See, e.g.*, 31 CFR part 500 (regulations of Treasury's Office of Foreign Asset Control (OFAC) prohibiting transactions involving designated foreign countries or their nationals).

benefits of requiring additional documentary verification and the burdens that may arise from such a requirement by providing that a bank's CIP must state the documents that a bank will use. This will require each bank to conduct its own risk-based analysis of the types of documents it believes will enable it to know the true identity of its customers.

The final rule continues to provide an illustrative list of identification documents. For an individual, these may include an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport. For a person other than an individual, these may include documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or a trust instrument.

Some commenters questioned whether the examples of identification documents given for persons other than individuals would be reliable. One commenter questioned whether trust documents alone would be sufficient verification of identity. Another commenter suggested allowing banks to rely on a certification by the trustee, or an appropriate legal opinion, rather than the trust instrument to verify the existence of a trust. Someone else suggested that banks should be allowed to rely on documentation consisting of evidence that a business is either publicly traded or is authorized to do business in a state or the United States.

The examples provided in the final rule were intended only to illustrate the documents a bank might use to verify the identity of a customer that is a corporation, partnership, or trust. A bank may use other documents, provided that they allow the bank to establish that it has a reasonable belief that it knows the true identity of its customer. Accordingly, the final rule makes no significant changes to the examples.

Section 103.121(b)(2)(ii)(B) Non-Documentary Verification. Recognizing that some accounts are opened by telephone, by mail, and over the Internet, the proposed rule provided 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). The preamble for the proposed rule also noted that even if the customer presents identification documents, it may be appropriate to use non-documentary methods as well.

The proposed rule gave examples of non-documentary verification methods that a bank may use, including 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 preamble for the proposed rule stated that a 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 proposal required that the procedures address situations where an individual, such as an elderly person, legitimately 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 account is not opened in a face-to-face transaction, for example over the phone, by mail, or through the Internet; and the type of account increases the risk that the bank will not be able to verify the true identity of the customer through documents.

Several commenters asked for additional guidance regarding when non-documentary verification methods should be used in addition to documentary verification methods and the circumstances in which only one or all of the non-documentary verification methods listed are necessary. Commenters also asked for guidance on audit methodology, and an explanation of the due diligence required for verification of accounts opened by telephone, mail, and through the Internet. A few commenters suggested that reference to verification, where a bank compares information provided by the customer with information from trusted third party sources, be expressly mentioned in the final rule.

As the large number of comments on this section illustrates, a rule that attempted to address every scenario and combination of risk-factors that a bank might confront would be extremely complex and invariably would fail to address many situations. Rather than adopt a lengthy and potentially unwieldy rule that still would not address every situation, Treasury and the Agencies have concluded that it would be more effective to adopt general principles that are fleshed out through 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.

The final rule *generally* retains the illustrative list of non-documentary methods contained in the proposal. Treasury and the Agencies have clarified that 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.

The final rule also retains the variety of situations that the procedures must address that were identified in the proposal, with the following two changes. First, because ''transaction'' is a defined term in 31 CFR part 103, instead of using the term ''face-to-face transaction,'' the final rule states that the procedures must address the situation where a customer opens an account without appearing in person at the bank. Second, the final clause of this provision provides that the CIP must include procedures to address situations 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. This clause acknowledges that there may be circumstances beyond those specifically described in this provision when a bank should use non-documentary verification procedures.

As stated in the preamble for the proposed rule, because identification documents may be obtained illegally and may be fraudulent, and in light of the recent increase in identity theft, Treasury and the Agencies encourage banks to use non-documentary methods even when the customer has provided identification documents.

Section 103.121(b)(2)(ii)(C) Additional Verification for Certain Customers. As described above, the proposed rule required the identification and verification of each signatory for an account. Most commenters objected to this requirement as overly burdensome, and, upon consideration of the points raised by the commenters, Treasury and the Agencies agree that it is appropriate

to delete it. For the reasons discussed below, however, the rule does require that a bank's CIP address the circumstances in which it will obtain information about such individuals in order to verify the customer's identity. Treasury and the Agencies believe that while the majority of customers may be verified adequately through the documentary or non-documentary verification methods described in paragraphs (b)(2)(ii)(A) and (B), there may be instances where this is not possible. The risk that the bank will not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership, or trust that is created or conducts substantial business in a jurisdiction that has been designated by the United States as a primary money laundering concern or has been designated as non-cooperative by an international body.

Obtaining sufficient information to verify a customer's identity can reduce the risk that a bank will be used as a conduit for money laundering and terrorist financing. Treasury and the Agencies believe that a bank must identify customers that pose a heightened risk of not being properly identified, and a bank's CIP must prescribe additional measures that may be used to obtain information about the identity of the individuals associated with the entity in whose name such an account is opened when standard documentary and non-documentary methods prove to be insufficient.

For these reasons, the requirement to verify the identity of signatories has been replaced by a new provision in the final rule that requires that a bank's CIP 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 also will obtain information about individuals with authority or control over such account, including signatories, in order to verify the customer's identity. This additional verification method will only apply when the bank cannot adequately verify the customer's identity using the documentary and non-documentary verification methods described in (b)(2)(ii)(A) and (B). Moreover, a bank need not undertake any additional verification if it chooses not to open an account when it cannot verify the customer's identity using standard documentary and non-documentary verification methods.

Section 103.121(b)(2)(iii) Lack of Verification. The proposed rule stated that a bank's 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. The preamble for the proposed rule listed what these procedures should include. In addition, the proposal stated that a bank should only maintain an account for a customer when it can form a reasonable belief that it knows the customer's true identity.[30]

The final rule retains the general requirement that a bank's CIP include procedures for responding to circumstances in which the bank cannot form a reasonable belief that it knows the true identity of the customer. However, the rule text itself now 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.

One commenter stated that requiring a bank to close an account if it cannot verify a customer's identity would conflict with state laws and would subject the bank to legal liability. The commenter urged that if this provision is retained, the final rule also should shield banks from state regulatory and borrower liability in these circumstances. Other commenters asked that Treasury and the Agencies clarify that further investigation that results in failure to open an account will not trigger adverse action requirements under the FCRA, 15 U.S.C. 1681 *et seq.* or the Equal Credit Opportunity Act (ECOA), 15 U.S.C. 1691 *et seq.*

The final 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. Treasury and the Agencies have determined that 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. Treasury and the Agencies also note that a bank must 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.[31]

Section 103.121(b)(3) Recordkeeping

Section 103.121(b)(3)(i) Required Records. The proposed rule set forth recordkeeping procedures that must be included in a bank's CIP. Under the proposal, a bank would have been required to maintain a record of the identifying information provided by the customer. Where a bank relies upon a document to verify identity, the proposal would have required the bank to maintain a copy of the document that the bank relied on that clearly evidences the type of document and any identifying information it may contain. The bank also would have been required to record the methods and result of any additional measures undertaken to verify the identity of the customer. Last, the bank would have been required to record the resolution of any discrepancy in the identifying information obtained.

This section of the proposed rule prompted the most comment. Though one commenter felt that the recordkeeping requirements in the proposed rule were weak, almost all other commenters identified the proposed documentation and record retention requirements as overly burdensome. Commenters urged Treasury and the Agencies to permit a bank to record the information from the documents obtained rather than requiring banks to maintain copies of these documents for the life of the account. Commenters generally argued that it would be difficult and very burdensome to store and retrieve copies of documents used to verify the identity of the customer. In addition, some commenters noted that many kinds of identification documents, particularly some new driver's licenses, have security features that prevent them from being copied legibly. Other commenters stated that copies of documents would be difficult to safeguard and could facilitate identity theft.

Commenters stated that requiring banks to keep copies of documents would substantially deviate from current banking practice and would violate certain states' laws. Banks offering credit card accounts through retailers, who require the customer to

[30] The preamble also explained that 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.

[31] *See* 12 CFR 202.9(b) (Federal Reserve Regulation B that prescribes the form of ECOA notice and statement of specific reasons); 15 U.S.C. 1681m (FCRA provision that provides for duties of users taking adverse actions on the basis of information contained in consumer reports from other third parties or affiliates).

provide identifying documents at the point of sale, strenuously opposed this requirement if it were interpreted to cover documents presented to the merchant. These commenters stated that copy machines are not usually available at the point of sale, and that the rule as proposed would require merchants to purchase large numbers of additional copy machines. The commenters also anticipated that consumers would be greatly inconvenienced by this requirement and might have to endure lengthy waits during any busy shopping season. These commenters questioned whether the risks of money-laundering and the financing of terrorism through retail store credit cards, which generally have relatively low credit limits, restrictions on pre-payment, and other features to detect fraud, warrant the imposition of these additional costs.

Other commenters stated that requiring banks to keep copies of documents that have pictures, such as driver's licenses, could expose the bank to allegations of unlawful discrimination, even if the retention of this information were not prohibited under ECOA. Some banks objected to this requirement on the grounds that it directly conflicted with the position that the Agencies have traditionally taken on this issue, including the criticism of banks that have retained such information in their files when extending credit.

Other commenters asked that a bank be permitted to record the processes and procedures generally used for verification rather than being required to keep records of the methods used and the resolution for each and every account, especially where the bank uses standardized procedures for all customers and could demonstrate that these procedures were applied. Some commenters suggested that the final rule permit banks to use a risk-based approach for recordkeeping.

In light of the comments received, Treasury and the Agencies have reconsidered and modified the recordkeeping requirements of the proposed rule. The final rule provides that a bank's CIP must include procedures for making and maintaining a record of all information obtained under the procedures implementing the requirement that a bank develop and implement a CIP. However, the final rule affords banks significantly more flexibility than did the recordkeeping provisions contained in the proposal. Under the final rule, a bank's records are to include ''a description,'' rather than a copy, of any document upon which the bank relied in order to verify the identity of the customer, noting the type of document, any identification number contained in the document, the place of issuance, and, if any, the date of issuance and expiration date. The final rule also clarifies that the record must include ''a description'' of the methods and results of any measures undertaken to verify the identity of the customer, and of the resolution of any ''substantive'' discrepancy discovered when verifying the identifying information obtained, rather than any documents generated in connection with these measures.

As Treasury and the Agencies indicated in the preamble for the proposal, 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 CFR 103.38(d).

Section 103.121(b)(3)(ii) Retention of Records

The proposal required a bank to retain all of the records specified in the recordkeeping provision for five years after the date the account is closed.

This requirement prompted strenuous objections. Assuming that copies of the documents used to verify the identity of the customer would have to be retained, commenters asserted that retaining records until five years after the account is closed would be very burdensome. Some commenters noted that imaging is not a routine practice for community banks and could be costly. Banks offering credit card accounts stated that the record retention requirement would require a change in forms, processes, and systems, while also increasing storage costs. As credit cards do not have a specific term, commenters noted that banks would be required to keep these records forever, unless they are culled manually. Some commenters suggested that the retention period be shortened, with suggestions ranging from one to three years after the account is closed, while other commenters suggested that the period be shortened to five years from when the account is opened. Many commenters stated that two years from when the information is obtained would be consistent with other regulatory requirements, such as the record retention requirements for an application for an extension of credit subject to ECOA (12 CFR 202.12(b)).

By eliminating the requirement that a bank retain copies of the documents used to verify the identity of the customer, Treasury and the Agencies believe that the final rule largely addresses the main concern of these commenters. However, Treasury and the Agencies also have determined that, while the identifying information provided by the customer should be retained, there is little value in requiring banks to retain the remaining records for five years after an account is closed because this information is likely to have become stale. Therefore, the final rule now prescribes a bifurcated record retention schedule that is consistent with the general five-year retention requirement in 31 CFR 103.38. First, the bank must retain the information referenced in paragraph (b)(3)(i)(A) (that is, information obtained about a customer), 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. Second, the bank need only retain the records that it must make and maintain under the remaining parts of the recordkeeping provision, paragraphs (b)(3)(i)(B), (C), and (D) (that is, information that verifies a customer's identity) for five years after the record is made.

Section 103.121(b)(4) Comparison with Government Lists. The proposed rule required a bank to have procedures for determining whether the customer appears on any list of known or suspected terrorists or terrorist organizations provided to the bank by any Federal government agency. In addition, the proposal stated that the procedures must ensure that the bank follows all Federal directives issued in connection with such lists.

Most commenters were concerned about how a bank would be able to determine what lists should be checked for purposes of this provision and how these lists would be made available. Some commenters asked that the final rule confirm that a bank will not have an affirmative duty to *seek out* all lists compiled by the Federal government and would only be required to check lists *provided* to it by the Federal government. Some commenters noted that lists published by OFAC are published but are not provided to financial institutions.[32] Many commenters urged that all lists within the meaning of section 326 of the Act,

[32] Nevertheless, the legislative history for this provision indicates that the lists Congress intended financial institutions to consult ''are those already supplied to financial institutions by the Office of Foreign Asset Control (OFAC), and occasionally by law enforcement and regulatory authorities, as in the days immediately following the September 11, 2001, attacks on the World Trade Center and the Pentagon.'' H.R. Rep. No. 107–250, pt. 1, at 63 (2001).

be centralized, issued by a single designated government agency, and provided to financial institutions in a commonly used electronic format. Some of these commenters suggested that instead of providing multiple lists, the government set up a single Web site that would permit a bank to search for a name alphabetically, similar to the OFAC list. Other commenters asked Treasury and the Agencies to clarify what action a bank should take when a customer appears on a list.

Commenters also asked for guidance regarding the timing of when the comparison must be performed and asked whether the lists could be checked after an account is opened. Some commenters stated that there is no practical way for a financial institution to check lists prior to opening an account.

The final rule states that a bank's 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. Because Treasury and the Federal functional regulators have not yet designated any such lists, the final rule cannot be more specific with respect to the lists banks must check in order to comply with this provision. However, banks will not have an affirmative duty under this regulation to seek out all lists of known or suspected terrorists or terrorist organizations compiled by the Federal government. Instead, banks will receive notification by way of separate guidance regarding the lists that must be consulted for purposes of this provision.

Treasury and the Agencies have modified this provision to give guidance as to *when* a bank must consult a list of known or suspected terrorists or terrorist organizations. The final rule states that the CIP's procedures must require the bank to make a determination regarding whether a customer appears on a list ''within a reasonable period of time'' after the account is opened, or earlier if required by another Federal law or regulation or by a Federal directive issued in connection with the applicable list.

The final rule provides that a bank's CIP must contain procedures requiring the bank to follow all Federal directives issued in connection with such lists. Again, because there are no lists that have been designated under this provision as yet, the final rule cannot provide more guidance in this area.

Section 103.121(b)(5) Customer Notice. The proposed rule would have required a bank's CIP to include procedures for providing bank customers with adequate notice that the bank is requesting information to verify their identity. The preamble for the proposal stated that a bank could satisfy that notice requirement by generally notifying its customers about the procedures the bank must comply with to verify their identities. It stated that the bank could post a notice in its lobby or on its Internet website, or provide customers with any other form of written or oral notice.

Treasury and the Agencies received a large number of comments on this provision. Some commenters did not agree that section 326 of the Act requires notice to bank customers. Some of these commenters suggested that a bank's request for identifying information should be considered adequate notice. Other commenters did not question this requirement and stated that they appreciated the flexibility of this provision. However, a great many commenters asked for additional guidance on the content and timing of the notice and specifically requested that the final rule provide model language so that all institutions represent the requirements of section 326 in the same manner and the adequacy of notice is not left to the interpretation of individual examiners.

Section 326 provides that the regulations issued ''shall, at a minimum, require financial institutions to implement, and customers (after being given adequate notice) to comply with reasonable procedures'' that satisfy the statute. Based upon this statutory requirement, the final rule requires a bank's CIP to include procedures for providing bank customers with adequate notice that the bank is requesting information to verify their identities. However, the final rule provides additional guidance regarding what constitutes adequate notice and the timing of the notice requirement.

The final rule states that notice is adequate if the bank generally describes the identification requirements of the final rule and provides notice in a manner reasonably designed to ensure that a customer views the notice, or is otherwise given notice, before opening an account. The final rule also states that depending upon the manner in which an account is opened, a bank may post a notice in the lobby or on its website, include the notice on its account applications, or use any other form of oral or written notice. In addition, the final rule includes sample language that, if appropriate, will be deemed adequate notice to a bank's customers when provided in accordance with the requirements of this final rule.

Section 103.121(b)(6) Reliance on Another Financial Institution. Many commenters urged that the final rule permit a bank to rely on a third party to perform elements of the bank's CIP. For example, some commenters asked that the final rule clarify that a bank may use a third party service provider to perform tasks and keep records. Other commenters recommended that the rule should permit a third party to verify the identity of the bank's customer in indirect lending arrangements, for example, where a car dealer acting as agent of the bank extends a loan to a customer or where a mortgage broker acts on a bank's behalf. Some commenters urged that the final rule be modified to more broadly permit financial institutions to share customer identification and verification duties with other financial institutions so as to avoid each institution having to undertake duplicative customer identification efforts. Some of these commenters suggested that a bank be permitted to allocate its responsibility to verify the customer's identity by contract with another financial institution as permitted in the proposed rule for broker-dealers.

Other commenters requested that the final rule permit the CIP obligations to be performed initially by only one financial institution if a customer has different accounts with different affiliates. These commenters noted that it is common for a customer to maintain several different accounts with a financial institution and its affiliates. The same customer, for example, may have a credit card account with one affiliate, a home mortgage with another affiliate, and a brokerage account with a broker-dealer affiliate. The commenters urged that a bank be permitted to rely on customer identification and verification performed by an affiliate because it would be superfluous and unnecessarily burdensome to subject the same customer to substantially similar customer identification and verification procedures on multiple occasions. Furthermore, those commenters urged Treasury and the Agencies to allow a bank to rely on an affiliate in order to reduce the substantial costs of maintaining duplicative records regarding identity verification under the recordkeeping provisions of the rule.

Treasury and the Agencies recognize that there may be circumstances where a bank should be able to rely on the performance by another financial institution of some or all of the elements of the bank's CIP. Therefore, the final rule provides that a bank's CIP may

include procedures specifying when the bank will rely on the performance by another financial institution (including an affiliate) of any procedures of the bank's CIP and thereby satisfy the bank's obligations under the rule. Reliance is permitted if a customer of the bank is opening, or has opened, an account or has established a similar banking or business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions.

In order for a bank to rely on the other financial institution, such reliance must be reasonable under the circumstances, and the other financial institution must be subject to a rule implementing the anti-money laundering compliance program requirements of 31 U.S.C. 5318(h) and be regulated by a Federal functional regulator. The other financial institution also must enter 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. The contract and certification will provide a standard means for a bank to demonstrate the extent to which it is relying on another institution to perform its CIP, and that the institution has in fact agreed to perform those functions. If it is not clear from these documents, a bank must be able to otherwise demonstrate when it is relying on another institution to perform its CIP with respect to a particular customer.

The bank will not be held responsible for the failure of the other financial institution to adequately fulfill the bank's CIP responsibilities, provided the bank can establish that its reliance was reasonable and that it has obtained the requisite contracts and certifications. Treasury and the Agencies emphasize that the bank and the other financial institution upon which it relies must satisfy all of these conditions set forth in the rule. If they do not, then the bank remains solely responsible for applying its own CIP to each customer in accordance with this regulation.

All of the Federal functional regulators are adopting comparable provisions in their respective regulations to permit such reliance. Furthermore, the Federal functional regulators expect to share information and to cooperate with each other to determine whether the institutions subject to their jurisdiction are in compliance with the conditions of the reliance provision of this final rule.

The final rule issued here does not affect a bank's authority to contract for services to be performed by a third party either on or off the bank's premises. Thus, for example, a bank may contract with a third party service provider to keep its records even when the bank does not act under the reliance provision set forth in the regulation. However, Treasury and the Agencies note that the performance of these services for Federally regulated banks [33] will be subject to regulation and examination by the Agencies under other applicable laws and regulations. *See, e.g.,* 12 U.S.C. 1867.

The final rule also does not alter a bank's authority to use an agent to perform services on its behalf. Therefore, a bank is permitted 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. However, as with any other responsibility performed by an agent, and in contrast to the reliance provision in the rule, the bank ultimately is responsible for that agent's compliance with the requirements of this final rule.

Section 103.121(c) Exemptions. The proposed rule provided that the appropriate Federal functional regulator, with the concurrence of Treasury, may by order or regulation exempt any bank or type of account from the requirements of this section. The proposal stated that, in issuing such exemptions, the Federal functional regulator and Treasury shall consider whether the exemption is consistent with the purposes of the BSA, consistent with safe and sound banking, and in the public interest. The proposal stated that the Federal functional regulator and Treasury also may consider other necessary and appropriate factors.

There were a number of comments suggesting that various types of accounts be exempted from the final rule. For example, several commenters suggested that accounts of Federal, state, and local governmental entities, public companies, and correspondent banks be exempted from the final rule. One commenter suggested that student loan programs be exempted from the rule because current safeguards are sufficient to verify the identity of student loan borrowers. Another commenter suggested that small trust companies and limited purpose banks that provide trust services be exempted from the rule, because such entities are more local in operation, would be burdened by the rule, and have fewer employees to ensure compliance. Yet another commenter suggested that the NCUA exempt credit unions from the CIP requirements.

Any suggested exemptions that Treasury and the Agencies have determined to be appropriate are incorporated into the definitions of ''account'' and ''customer'' for the reasons described above. The exemption provision of the final rule is essentially adopted as proposed with respect to banks that have a Federal functional regulator. Because the final rule will also apply to certain banks that do not have a Federal functional regulator, a new provision has been added to make clear that Treasury alone will make all determinations regarding exemptions for these institutions.

Section 103.121(d) Other Information Requirements Unaffected. The proposal provided that nothing in § 103.121 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 103. 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 § 103.121, as well as with the provisions of § 103.22, which require that certain information concerning the transaction be reported by filing a Currency Transaction Report (CTR). There were no comments on this provision. Therefore, Treasury and the Agencies have adopted this provision generally as proposed, except that it has been clarified to provide that nothing in § 103.121 should be construed to relieve a bank of any of its obligations, including its obligations to obtain, verify, or maintain information in connection with an account or transaction that is required by another provision in part 103.

III. Conforming Amendments to 31 CFR 103.34

Section 103.34(a) sets forth customer identification requirements when certain types of deposit accounts are opened. Together with the proposed rule implementing section 326, Treasury, on its own authority, proposed deleting 31 CFR 103.34(a) for the following reasons.

First, the preamble for the proposal explained that Treasury regards the requirements of §§ 103.34(a)(1) and (2) as inconsistent with the intent and purpose of section 326 of the Act and incompatible with proposed section 103.121. Generally §§ 103.34(a)(1) and (2) require a bank, within 30 days after

[33] Because it lacks the specific statutory authority to regulate and examine service providers, NCUA, as a matter of safety and soundness, will require credit unions to document that their service providers fully comply with this regulation and with the credit union's customer identification program.

certain deposit accounts are opened, to secure and maintain a record of the taxpayer identification number of the customer involved. If the bank is unable to obtain the taxpayer identification number within 30 days (or a longer time if the person has applied for a taxpayer identification number), it need take no further action under § 103.34 concerning the account if it maintains a list of the names, addresses, and account numbers of the persons for which it was unable to secure taxpayer identification numbers, and provides that information to Treasury upon request. In the case of a non-resident alien, the bank is required to record the person's passport number or a description of some other government document used to determine identification. These requirements conflicted with those in proposed § 103.121 which required a bank to obtain the name, address, date of birth and an identification number from any person seeking to open a new account.

Second, § 103.34(a)(3) currently provides that a bank need not obtain a taxpayer identification number with respect to specified categories of persons [34] opening certain deposit accounts. Proposed § 103.121 did not exempt any persons from the CIP requirements. Treasury requested comment on whether any of the exemptions in § 103.34(a)(3) should apply in light of the intent and purpose of section 326 of the Act and the requirements of proposed § 103.121.

Third, § 103.34(a)(4) also provides that IRS rules shall determine whose number shall be obtained in the case of multiple account holders. In the preamble that accompanied its proposal, Treasury stated that this provision is inconsistent with section 326 of the Act, which requires that banks verify the identity of ''any'' person seeking to open an account.

In addition, Treasury proposed deleting § 103.34(b)(1) which requires a bank to keep ''any notations, if such are normally made, of specific identifying information verifying the identity of the signer [who has signature authority over an account] (such as a driver's license number or credit card number).'' Treasury stated that the quoted language in § 103.34(b)(1) is inconsistent with the proposed requirements of § 103.121. For this reason, Treasury, under its own authority, proposed to delete the quoted language.

Few comments were received regarding the proposed deletion of these provisions. Some commenters agreed that § 103.34(a) should be deleted if proposed § 103.121 were adopted. One commenter suggested that § 103.34(a) should be revised to achieve the objectives of the section 326 of the Act. One commenter representing a military bank requested continuance of the exemption for agencies and instrumentalities of the Federal government that will permit exemption of commissaries, exchanges and various military organizations. Another commenter requested maintenance of the exemption for government entities, court funds, unincorporated units of tax-exempt organizations, and school thrift programs.

Treasury has determined that given the more comprehensive requirements of the final version of § 103.121, there is no longer a need for § 103.34 (a). A number of the exemptions formerly in § 103.34(a) have now been added to § 103.121. Other exemptions conflict with the language and intent of section 326 of the Act and thus were not adopted in the final rule. While § 103.34(a) will no longer be needed once the final rule is fully effective, withdrawing the provision before October 1, 2003, would create a gap period during which banks would not be subject to a rule under the BSA requiring a customer to be identified when opening an account. Because Treasury and the Agencies do not believe such a gap period would be appropriate, the final rule—rather than withdrawing § 103.34(a)—amends the section to cut off its applicability on October 1, 2003, when § 103.121 becomes fully effective.[35]

By contrast, Treasury no longer believes that it is necessary to delete the quoted language in § 103.34(b), which requires a bank to keep ''any notations, if such are normally made, of specific identifying information verifying the identity of [a person with signature authority over an account] (such as a driver's license number or credit card number).'' The definition of ''customer'' in the final version of § 103.121 no longer includes a signatory on an account. Therefore, § 103.121 and § 103.34(b)(1) are not inconsistent and the records required to be kept in accordance with § 103.34(b)(1) will still have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, and to protect against international terrorism. Therefore, the proposal to delete the quoted language in § 103.34(b)(1) is not adopted as proposed.

IV. Technical Amendment to 31 CFR 103.11(j)

Section 103.11(j), which defines the term ''deposit account,'' contains an obsolete reference to the definition of ''transaction account,'' which is defined in § 103.11(hh). Under its own authority, Treasury proposed to correct this reference. There were no comments on this proposed technical correction. Therefore, it is adopted as proposed.

V. Regulatory Analysis

A. Regulatory Flexibility Act

Under the Regulatory Flexibility Act (RFA), an agency must either prepare a Final Regulatory Flexibility Analysis (FRFA) for a final rule or certify that the final rule will not have a significant economic impact on a substantial number of small entities.[36] *See* 5 U.S.C. 604 and 605(b).

Treasury and the Agencies have reviewed the impact of this final rule on small banks. Treasury and the Agencies certify that the final rule will not have a significant economic impact on a substantial number of small entities.

First, Treasury and the Agencies believe that banks already have implemented prudential business practices and anti-money laundering

[34] The exemption applies to (i) agencies and instrumentalities of Federal, State, local, or foreign governments; (ii) judges, public officials, or clerks of courts of record as custodians of funds in controversy or under the control of the court; (iii) aliens who are ambassadors; ministers; career diplomatic or consular officers; naval, military, or other attaches of foreign embassies and legations; and members of their immediate families; (iv) aliens who are accredited representatives of certain international organizations, and their immediate families; (v) aliens temporarily residing in the United States for a period not to exceed 180 days; (vi) aliens not engaged in a trade or business in the United States who are attending a recognized college or university, or any training program supervised or conducted by an agency of the Federal Government; (vii) unincorporated subordinate units of a tax exempt central organization that are covered by a group exemption letter; (viii) a person under 18 years of age, with respect to an account opened as part of a school thrift savings program, provided the annual interest is less than $10; (ix) a person opening a Christmas club, vacation club, or similar installment savings program, provided the annual interest is less than $10; and (x) non-resident aliens who are not engaged in a trade or business in the United States.

[35] Appropriate conforming amendments are made to §§ 103.34(b)(11) and (12) to add a cross-reference to the Internal Revenue Code regarding the rules for determining what constitutes a taxpayer identification number.

[36] The RFA defines the term ''small entity'' in 5 U.S.C. 601 by reference to the definitions published by the Small Business Administration (SBA). The SBA has defined a ''small entity'' for banking purposes as a bank or savings institution with less than $150 million in assets. *See* 13 CFR 121.201. The NCUA defines ''small credit union'' as those under $1 million in assets. Interpretive Ruling and Policy Statement No. 87–2, Developing and Reviewing Government Regulations (52 FR 35231, September 18, 1987).

programs that include most of the procedures that a CIP must contain under this final rule. Banks generally undertake extensive measures to verify the identity of their customers as a matter of good business practice. In addition, Federally regulated banks already must have anti-money laundering programs that include procedures for identification, verification, and documentation of customer information.[37]

Second, although the final rule contains several requirements that will be new to banks we anticipate that the costs of implementing these requirements will not be economically significant. For example, the recordkeeping requirements in the final rule may impose some costs on banks to the extent that the information that must be maintained is not already collected and retained.[38] Treasury and the Agencies believe that the compliance burden is minimized for banks, including small banks, because the final rule vests a bank with the discretion to design and implement appropriate recordkeeping procedures, including allowing banks to maintain electronic records in lieu of (or in combination with) paper records.

The section of the final rule that requires banks to check lists of known and suspected terrorists and terrorist organizations and to follow Federal agency directives in connection with the lists is also a new requirement that will impose nominal burden, once Treasury and the Agencies publish lists that banks must consult. However, no such lists have been issued to date. Moreover, banks already must have procedures to satisfy other similar requirements. For instance, banks already have to ensure that they do not engage in transactions involving designated foreign countries, foreign nationals, and other entities prohibited under OFAC rules. *See* 31 CFR part 500. We also understand that many banks, including small banks, use electronic search tools to check lists [39] and already use identity verification software, both as part of their customer due diligence obligations under existing BSA compliance program requirements and to detect fraud.

The notice provisions of the rule also are new. However, they are very flexible and, as written, should impose only minimal costs. The final rule permits a bank to satisfy the notice requirement by choosing from a variety of low-cost measures, such as posting a sign in the lobby or on its website, by adding it to an account statement, or using any other form of written or oral notice. In addition, the amount of time that a bank will need to develop its notices will be minimal as the final rule now contains a sample notice.

Treasury and the Agencies believe that the flexibility incorporated into the final rule will permit each bank to tailor its CIP to fit its own size and needs. In this regard, Treasury and the Agencies believe that expenditures associated with establishing and implementing a CIP will be commensurate with the size of a bank. If a bank is small, the burden to comply with the proposed rule should be *de minimis*.

Most commenters on the proposed rule stated that Treasury and the Agencies had underestimated the burden imposed by the proposed rule. They highlighted aspects of the proposal that they maintained would have imposed excessive burdens and would have required banks to alter their current practices. Most comments focused on the proposed provisions requiring banks to verify the identity of signatories on accounts, to keep copies of documents used to verify a customer's identity, and to retain identity verification records for five years after an account is closed.

In drafting the final rule, Treasury and the Agencies have either eliminated or minimized the most significant burdens identified by commenters. In response to commenters, for example, the final rule eliminates signatories from the definition of ''customer,'' no longer requires a bank to keep copies of documents used to verify a customer's identity, and reduces the universe of records that must be kept for five years after an account is closed. Treasury and the Agencies have taken other steps that significantly reduce the scope of the rule and burdens of the rule. Many of these burden-reducing actions are described in the Paperwork Reduction Act discussion below.[40] As a result of these changes, the final rule is far more flexible and less burdensome than the proposed rule while still fulfilling the statutory mandates enumerated in section 326 of the Act.

Finally, Treasury and the Agencies did consider whether it would be appropriate to exempt small banks from the requirements of the rule. We do not believe that an exemption for small banks is appropriate, given the flexibility built into the rule to account for, among other things, the differing sizes and resources of banks, as well as the importance of the statutory goals and mandate of section 326. Money laundering can occur in small banks as well as large banks.

B. Paperwork Reduction Act

Certain provisions of the final rule contain ''collection of information'' requirements within the meaning of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*). An agency may not conduct or sponsor, and a respondent is not required to respond to, an information collection unless it displays a currently valid Office of Management and Budget (OMB) control number. Treasury submitted the final rule to the OMB for review in accordance with 44 U.S.C. 3507(d). The OMB has approved the collection of information requirements in today's rule under control number 1506–0026.

[37] *See* footnote 10.

[38] *See, e.g.*, identification and verification of customers in connection with each share or deposit account opened (31 CFR 103.34).

[39] We believe that most banks will use technology rather than manual methods to check lists. OFAC lists are generally incorporated into bank software and, in response to bank inquiries, Treasury and the Agencies have made clear that banks are permitted to share the lists they receive pursuant to section 314 of the Act with their service providers. We expect that any lists provided under section 326 of the Act will also be provided under the same conditions.

[40] In addition to the burden-reducing measures discussed in the Paperwork Reduction Act discussion, other changes include:

- A clarification that a bank must verify the customer's *identity* using the identifying information obtained. The proposed rule would have required the bank to verify all identifying information. The elimination of the requirement that a bank must obtain a physical and a mailing address from a customer opening an account. Under the final rule, the bank is only required to obtain a physical address.
- A new provision that permits a bank to rely on another financial institution to perform its CIP under certain conditions. This provision allows financial institutions that share a customer to share customer identification and verification obligations and to reduce the cost of maintaining duplicative records required by the recordkeeping provisions of the final rule.
- A revised provision that extends to customers who are individuals the exception that permits a bank to open an account for a customer that has applied for, but has not received, a taxpayer identification number.
- A new exemption for credit card accounts from the requirement that a bank obtain identifying information from the customer prior to opening an account. In connection with credit card accounts, a bank is permitted to obtain identifying information from a third party source prior to extending credit.
- A clarification stating that the government will provide lists of known or suspected terrorists and terrorist organizations to banks. Banks will not be required to seek out this information. In addition, the rule now states that the bank may determine whether a customer appears on the list within a reasonable time after the account is opened, unless it is required to do so earlier by another Federal law, regulation, or directive.
- A transition period that permits banks a period of several months to comply with the final rule.

Collection of Information Under the Proposed Rule

The proposed rule applied only to a financial institution that is a ''bank'' as defined in 31 CFR 103.11(c),[41] and any foreign branch of an insured bank. The proposed rule required each bank to establish a written CIP that must include recordkeeping procedures (proposed § 103.121(b)(3)) and procedures for providing customers with notice that the bank is requesting information to verify their identity (proposed § 103.121(b)(5)).

The proposed rule required a bank to maintain a record of (1) the identifying information provided by the customer, the type of identification document(s) reviewed, if any, the identification number of the document(s), and a copy of the identification document(s); (2) the means and results of any additional measures undertaken to verify the identity of the customer; and (3) the resolution of any discrepancy in the identifying information obtained. It also required these records to be maintained at the bank for five years after the date the account is closed (proposed § 103.121(b)(3)).

The proposed rule also required a bank to give its customers ''adequate notice'' of the identity verification procedures (proposed § 103.121(b)(5)). The proposed rule stated that a bank could satisfy the notice requirement by posting a sign in the lobby or providing customers with any other form of written or oral notice.

Collection of Information Under the Final Rule

The final rule, like the proposed rule, requires banks to implement reasonable procedures to (1) maintain records of the information used to verify a customer's identity, and (2) provide notice of these procedures to customers. These recordkeeping and disclosure requirements are required under section 326 of the Act. However, the final rule greatly reduces the paperwork burden attributable to these requirements, as described below.

The final rule also contains a new recordkeeping provision permitting a bank to rely on another financial institution to perform some or all its CIP, under certain circumstances. Among other things, the other financial institution must provide the bank with 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.

Response to Comments Received

We received approximately 500 comments on the proposed rule. Most of the commenters specifically mentioned the recordkeeping burden associated with the proposed rule. Some commenters also asked Treasury and the Agencies to clarify the meaning of ''adequate notice'' and requested that a sample notice be provided in the final rule.

Only a few commenters provided burden estimates of additional burden hours that would result from the proposed rule. However, these burden estimates did not necessarily focus on the recordkeeping and disclosure requirements in the proposal and ranged from 200 extra hours per year to 9,000 additional hours. Treasury and the Agencies believe that the final rule substantially addresses the concerns of the commenters. Specific concerns about paperwork burden have been addressed as follows:

First, the recordkeeping and disclosure burden are minimized in the final rule because Treasury and the Agencies reduced the entire scope of the final rule, by:

• Narrowing and clarifying the scope of ''account.'' The final rule specifically excludes accounts that (1) a bank acquires through an acquisition, merger, purchase of assets, or assumption of liabilities from a third party, and (2) accounts opened for the purpose of participating in an employee benefit plan established pursuant to the Employee Retirement Income Security Act of 1974. It also specifically excludes wire transfers, check cashing, and the sale of travelers checks, and any other product or service that does not lead to a ''formal banking relationship'' from the scope of the rule;

• Narrowing the definition of ''bank'' covered by the rule to exclude a bank's foreign branches; and

• Limiting and clarifying who is a ''customer'' for purposes of the final rule. The final rule now defines ''customer'' as ''a person that opens a new account'' making clear that a person who does not receive banking services, such as a person whose deposit or loan application is denied, is not a customer. The definition of customer also excludes signatories from the definition of ''customer.'' Moreover, the final rule excludes from the definition of ''customer'' the following readily-identifiable entities: A financial institution regulated by a Federal functional regulator; a bank regulated by a state bank regulator; and governmental agencies and instrumentalities and companies that are publicly traded (*i.e.*, entities described in § 103.22(d)(2)(ii)–(iv)). The final rule also excludes existing customers of the bank, provided that the bank has a reasonable belief that it knows the true identity of the person.[42]

Second, recordkeeping burden was further reduced by:

• Eliminating the requirement that a bank keep copies of any document that it relied upon in order to verify the identity of the customer and substituting a requirement that a bank's records need only include ''a description'' of any document that it relied upon in order to verify the identity of the customer. The final rule also clarifies that the records need only include ''a description'' of the methods and results of any measure undertaken to verify the identity of the customer, and of the resolution of any substantive discrepancy discovered when verifying the identifying information obtained, rather than any documents generated in connection with these measures; and

• Reducing the length of time that records must be kept. The final rule requires that identifying information be kept for five years after the date the account is closed (or for credit card accounts, five years after the account is closed or becomes dormant). All other records may be kept for five years after the account is opened.

Third, disclosure burden was reduced by providing sample language that, if appropriate and properly provided, will be deemed adequate notice to a bank's customer. Disclosure burden also was reduced by clarifying the term ''adequate notice.''

Treasury and the Agencies believe that little additional burden is imposed as a result of the recordkeeping requirements outlined in section 103.121(b)(3), because the type of recordkeeping required by the final rule is a usual and customary business practice. In addition, banks already must keep similar records to comply with existing regulations in 31 CFR part 103 (*see, e.g.*, 31 CFR 103.34, requiring certain records for each deposit or share account opened).

Treasury and the Agencies believe that nominal burden is associated with the disclosure requirement outlined in § 103.121(b)(5). This section contains a sample notice that if appropriate and

[41] This definition includes banks, thrifts, and credit unions.

[42] The proposed rule stated that the identity of an existing customer would not need to be verified if the bank (1) had previously verified the customer's identity in accordance with procedures consistent with the proposed rule, and (2) continues to have a reasonable belief that it knows the true identity of the customer.

provided in accordance with the final rule, will be deemed adequate notice. In addition, it continues to permit banks to choose among a variety of low-cost methods of providing adequate notice and to select the least burdensome method, given the circumstances under which customers seek to open new accounts.

Treasury and the Agencies also believe that nominal burden is associated with the new recordkeeping requirement in § 103.121(b)(6). This section permits a bank to rely on another financial institution to perform some or all its CIP under certain conditions, including the condition that the financial institution enter into a contract with the bank providing that it will certify annually to the bank that it (1) has implemented its anti-money laundering program and (2) will perform (or its agent will perform) the specified requirements of the bank's CIP. Not all banks will choose to rely on a third party. For those that do, the minimal burden of retaining the certification described above should allow them to reduce net burden under the rule by such reliance.

Burden Estimates

Treasury and the Agencies have reconsidered the burden estimates published in the proposed rule, given the comments stating that the burdens associated with the paperwork collections were underestimated. Having done so, and considering the reduction in burden taken in this final rule, Treasury and the Agencies have adjusted their estimates of the paperwork burden of this rule. The burden estimates that follow are estimates of the incremental burden imposed upon banks by this final rule, recognizing that some of the requirements in this rule are a usual and customary practice in the banking industry, or duplicate other regulatory requirements.

The potential respondents are national banks and Federal branches and agencies (OCC financial institutions); state member banks and branches and agencies of foreign banks (Board financial institutions); insured state nonmember banks (FDIC financial institutions); savings associations (OTS financial institutions); Federally insured credit unions (NCUA financial institutions); and certain non-Federally regulated credit unions, private banks, and trust companies (FinCEN institutions).

Estimated number of respondents:
OCC: 2207.
Board: 1240.
FDIC: 5,500.
OTS: 962.
NCUA: 9,688.
FinCEN: 2,460.

Estimated average annual recordkeeping burden per respondent: 10 hours.

Estimated average annual disclosure burden per respondent: 1 hour.

Estimated total annual recordkeeping and disclosure burden: 242,627 hours.

Treasury and the Agencies invite comment on the accuracy of the burden estimates and invite suggestions on how to further reduce these burdens. Comments should be sent (preferably by fax (202–395–6974)) to Desk Officer for the Department of the Treasury, Office of Information and Regulatory Affairs, Office of Management and Budget, Paperwork Reduction Project (1506–0026), Washington, DC 20503 (or by the Internet to *jlackeyj@omb.eop.gov*), with a copy to FinCEN by mail or the Internet at the addresses previously specified.

Executive Order 12866

Treasury, the OCC, and OTS have determined that the final rule is not a ''significant regulatory action'' under Executive Order 12866 for the following reasons.

The rule follows closely the requirements of section 326 of the Act. Moreover, Treasury, the OCC, and OTS believe that national banks and savings associations already have procedures in place that fulfill most of the requirements of the final rule because the procedures are a matter of good business practice. In addition, national banks and savings associations already are required to have BSA compliance programs that address many of the requirements detailed in this final rule.

At the proposed rule stage, Treasury, the OCC, and OTS invited national banks, the thrift industry, and the public to provide any cost estimates and related data that they think would be useful in evaluating the overall costs of the rule. Most of the cost estimates provided by commenters related to the requirements in the proposed rule that banks verify the identity of signatories on accounts, keep copies of documents used to verify a customer's identity, and retain identity verification records for five years after an account is closed. As described in the preamble, the final rule eliminates signatories from the definition of ''customer,'' and no longer requires a bank to keep copies of documents used to verify a customer's identity. The final rule also reduces the universe of records that must be kept for five years after an account is closed. Treasury, the OCC and the OTS have taken other steps that significantly reduce the scope of the rule and the burden of the rule. These burden-reducing measures are described in the Paperwork Reduction Act discussion and Regulatory Flexibility Act discussion, above.[43]

List of Subjects

12 CFR Part 21

Crime, Currency, National banks, Reporting and recordkeeping requirements, Security measures.

12 CFR Part 208

Accounting, Agriculture, Banks, banking, Confidential business information, Crime, Currency, Investments, Mortgages, Reporting and recordkeeping requirements, Securities.

12 CFR Part 211

Exports, Foreign banking, Holding companies, Investments, Reporting and recordkeeping requirements.

12 CFR Part 326

Banks, banking, Currency, Insured nonmember banks, Reporting and recordkeeping requirements, Security measures.

12 CFR Part 563

Accounting, Advertising, Crime, Currency, Investments, Reporting and Recordkeeping requirements, Savings associations, Securities, Surety bonds.

12 CFR Part 748

Credit unions, Crime, and Security measures.

31 CFR Part 103

Administrative practice and procedure, Authority delegations (Government agencies), Banks, banking, Brokers, Currency, Foreign banking, Foreign currencies, Gambling, Investigations, Law enforcement, Penalties, Reporting and recordkeeping requirements, Securities.

Department of the Treasury

31 CFR Chapter I

Authority and Issuance

■ For the reasons set forth in the preamble, part 103 of title 31 of the Code of Federal Regulations is amended as follows:

[43] For these same reasons, and consistent with section 201 of the Unfunded Mandates Reform Act of 1995 (Pub. L. 104–4), Treasury, the OTS and the OCC have also determined that this final rule will not result in expenditures by State, local, and tribal governments in the aggregate, or by the private sector of $100 million or more in any one year, and therefore the rule is not subject to the requirements of section 202 of that Act.

PART 103—FINANCIAL RECORDKEEPING AND REPORTING OF CURRENCY AND FOREIGN TRANSACTIONS

■ 1. The authority citation for part 103 is revised to read as follows:

Authority: 12 U.S.C. 1829b and 1951–1959; 31 U.S.C. 5311–5314 and 5316–5332; title III, secs. 312, 313, 314, 319, 326, 352, Pub L. 107–56, 115 Stat. 307.

§ 103.11 [Amended]

■ 2. Section 103.11(j) is amended by removing ''paragraph (q)'' and adding ''paragraph (hh)'' in its place.

§ 103.34 [Amended]

■ 3. Section 103.34 is amended as follows:

■ a. By amending the first sentence of paragraph (a)(1) to add the words ''and before October 1, 2003'' after the words ''May 31, 1978'' and after the words ''June 30, 1972'';

■ b. By amending paragraph (b)(11) to add the words ''as determined under section 6109 of the Internal Revenue Code of 1986'' after the words ''taxpayer identification number;'' and

■ c. By amending paragraph (b)(12) to add the words ''as determined under section 6109 of the Internal Revenue Code of 1986'' after the words ''taxpayer identification number.''

■ 2. Subpart I of part 103 is amended by adding new § 103.121 to read as follows:

§ 103.121 Customer Identification Programs for banks, savings associations, credit unions, and certain non-Federally regulated banks.

(a) *Definitions.* For purposes of this section:

(1)(i) *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.

(ii) *Account* does not include:

(A) 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;

(B) An account that the bank acquires through an acquisition, merger, purchase of assets, or assumption of liabilities; or

(C) An account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974.

(2) *Bank* means:

(i) A bank, as that term is defined in § 103.11(c), that is subject to regulation by a Federal functional regulator; and

(ii) A credit union, private bank, and trust company, as set forth in § 103.11(c), that does not have a Federal functional regulator.

(3)(i) *Customer* means:

(A) A person that opens a new account; and

(B) An individual who opens a new account for:

(*1*) An individual who lacks legal capacity, such as a minor; or

(*2*) An entity that is not a legal person, such as a civic club.

(ii) *Customer* does not include:

(A) A financial institution regulated by a Federal functional regulator or a bank regulated by a state bank regulator;

(B) A person described in § 103.22(d)(2)(ii) through (iv); or

(C) 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.

(4) *Federal functional regulator* is defined at § 103.120(a)(2).

(5) *Financial institution* is defined at 31 U.S.C. 5312(a)(2) and (c)(1).

(6) *Taxpayer identification number* 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).

(7) *U.S. person* means:

(i) A United States citizen; or

(ii) A person other than an individual (such as a corporation, partnership, or trust), that is established or organized under the laws of a State or the United States.

(8) *Non-U.S. person* means a person that is not a *U.S. person.*

(b) *Customer Identification Program: minimum requirements.*

(1) *In general.* 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 (b)(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. Until such time as credit unions, private banks, and trust companies without a Federal functional regulator are subject to such a program, their CIPs must be approved by their boards of directors.

(2) *Identity verification procedures.* The CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. 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 (b)(2).

(i) *Customer information required.* (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 (b)(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:

(*i*) For an individual, a residential or business street address;

(*ii*) 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

(*iii*) 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:

(*i*) For a U.S. person, a taxpayer identification number; or

(*ii*) For a non-U.S. person, one or more of the following: a taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

Note to paragraph (b)(2)(i)(A)(*4*)(*ii*): 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 (b)(2)(i)(A) by acquiring it from a third-party source prior to extending credit to the customer.

(ii) *Customer verification.* The CIP must contain procedures for verifying the identity of the customer, using information obtained in accordance with paragraph (b)(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 (b)(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.

(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 (b)(2)(ii)(A) and (B) of this section.

(iii) *Lack of verification.* 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.

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

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

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

(B) A description of any document that was relied on under paragraph (b)(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 (b)(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.

(ii) *Retention of records.* The bank must retain the information in paragraph (b)(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 (b)(3)(i)(B), (C), and (D) of this section for five years after the record is made.

(4) *Comparison with government lists.* The CIP must include procedures for determining whether the customer appears on any list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators. 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.

(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 website, 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.

(6) *Reliance on another financial institution.* 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:

(i) Such reliance is reasonable under the circumstances;

(ii) 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

(iii) 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.

(c) *Exemptions.* 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.

(d) *Other requirements unaffected.* 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.

Dated: April 28, 2003.

James F. Sloan,

Director, Financial Crimes Enforcement Network.

Dated: April 17, 2003.

In concurrence:

John D. Hawke, Jr.,

Comptroller of the Currency.

In concurrence:

By order of the Board of Governors of the Federal Reserve System, April 21, 2003.

Jennifer J. Johnson,

Secretary of the Board.

In concurrence:

By order of the Board of Directors of the Federal Deposit Insurance Corporation this 16th day of April, 2003.

Valerie J. Best,

Assistant Executive Secretary.

In concurrence:

Dated: April 9, 2003.

James E. Gilleran,

Director, Office of Thrift Supervision.

In concurrence:

Dated: April 7, 2003.

Becky Baker,

Secretary of the Board, National Credit Union Administration.

Office of the Comptroller of the Currency

12 CFR Chapter I

Authority and Issuance

■ For the reasons set out in the preamble, the OCC amends chapter I of title 12 of the Code of Federal Regulations as set forth below:

PART 21—MINIMUM SECURITY DEVICES AND PROCEDURES, REPORTS OF SUSPICIOUS ACTIVITIES, AND BANK SECRECY ACT COMPLIANCE PROGRAM

Subpart C—Procedures for Monitoring Bank Secrecy Act Compliance

■ 1. The authority citation for part 21, subpart C, continues to read as follows:

Authority: 12 U.S.C. 93a, 1818, 1881–1884 and 3401–3422; 31 U.S.C. 5318.

■ 2. In § 21.21:

■ A. Revise the section heading; and

■ B. Revise § 21.21(b) to read as follows:

§ 21.21 Procedures for monitoring Bank Secrecy Act (BSA) compliance.

* * * * *

(b) *Establishment of a BSA compliance program.* (1) *Program requirement.* Each bank shall develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with the recordkeeping and reporting requirements set forth in subchapter II of chapter 53 of title 31, United States Code and the implementing regulations issued by the Department of the Treasury at 31 CFR part 103. The compliance program must be written, approved by the bank's board of directors, and reflected in the minutes of the bank.

(2) *Customer identification program.* Each bank is subject to the requirements of 31 U.S.C. 5318(l) and the implementing regulation jointly promulgated by the OCC and the Department of the Treasury at 31 CFR 103.121, which require a customer identification program to be implemented as part of the BSA compliance program required under this section.

* * * * *

Dated: April 17, 2003.

John D. Hawke, Jr.,

Comptroller of the Currency.

Federal Reserve System

12 CFR Chapter II

Authority and Issuance

■ For the reasons set out in the preamble, the Board of Governors of the Federal Reserve System amends 12 CFR Chapter II as follows:

PART 208—MEMBERSHIP OF STATE BANKING INSTITUTIONS IN THE FEDERAL RESERVE SYSTEM (REGULATION H)

■ 1. The authority citation for part 208 continues to read as follows:

Authority: 12 U.S.C. 24, 24a, 36, 92a, 93a, 248(a), 248(c), 321–338a, 371d, 461, 481–486, 601, 611, 1814, 1816, 1818, 1820(d)(9), 1823(j), 1828(o), 1831, 1831o, 1831p–1, 1831r–1, 1831w, 1831x, 1835a, 1843(l), 1882, 2901–2907, 3105, 3310, 3331–3351, and 3906–3909; 15 U.S.C. 78b, 78l(b), 78l(g), 78l(i), 78o–4(c)(5), 78q, 78q–1, and 78w; 31 U.S.C. 5318; 42 U.S.C. 4012a, 4104a, 4104b, 4106, and 4128.

■ 2. Revise § 208.63(b) to read as follows:

§ 208.63 Procedures for monitoring Bank Secrecy Act compliance.

* * * * *

(b) *Establishment of BSA compliance program.* (1) *Program requirement.* Each bank shall develop and provide for the continued administration of a program reasonably designed to ensure and monitor compliance with the recordkeeping and reporting requirements set forth in subchapter II of chapter 53 of title 31, United States Code, the Bank Secrecy Act, and the implementing regulations promulgated thereunder by the Department of the Treasury at 31 CFR part 103. The compliance program shall be reduced to writing, approved by the board of directors, and noted in the minutes.

(2) *Customer identification program.* Each bank is subject to the requirements of 31 U.S.C. 5318(l) and the implementing regulation jointly promulgated by the Board and the Department of the Treasury at 31 CFR 103.121, which require a customer identification program to be

implemented as part of the BSA compliance program required under this section.

* * * * *

PART 211—INTERNATIONAL BANKING OPERATIONS (REGULATION K)

■ 1. The authority citation for part 211 is revised to read as follows:

Authority: 12 U.S.C. 221 *et seq.,* 1818, 1835a, 1841 *et seq.,* 3101 *et seq.,* and 3901 *et seq.;* 15 U.S.C. 6801 and 6805; 31 U.S.C. 5318.

■ 2. In § 211.5, add new paragraph (m) to read as follows:

§ 211.5 Edge and agreement corporations.

* * * * *

(m) *Procedures for monitoring Bank Secrecy Act compliance.*

(1) [Reserved]

(2) *Customer identification program.* Each Edge or agreement corporation is subject to the requirements of 31 U.S.C. 5318(l) and the implementing regulation jointly promulgated by the Board and the Department of the Treasury at 31 CFR 103.121, which require a customer identification program.

■ 3. In § 211.24, add new paragraph (j) to read as follows:

§ 211.24 Approval of offices of foreign banks; procedures for applications; standards for approval; representative office activities and standards for approval; preservation of existing authority.

* * * * *

(j) *Procedures for monitoring Bank Secrecy Act compliance.*

(1) [Reserved]

(2) *Customer identification program.* Except for a federal branch or a federal agency or a state branch that is insured by the FDIC, a branch, agency, or representative office of a foreign bank operating in the United States is subject to the requirements of 31 U.S.C. 5318(l) and the implementing regulation jointly promulgated by the Board and the Department of the Treasury at 31 CFR 103.121, which require a customer identification program.

By order of the Board of Governors of the Federal Reserve System, April 21, 2003.

Jennifer J. Johnson,

Secretary of the Board.

Federal Deposit Insurance Corporation

12 CFR Chapter III

Authority and Issuance

■ For the reasons set out in the preamble, the FDIC amends title 12, chapter III of the Code of Federal Regulations, as set forth below:

PART 326—Minimum Security Devices and Procedures and Bank Secrecy Act Compliance

■ 1. The authority citation for part 326 is revised to read as follows:

Authority: 12 U.S.C. 1813, 1815, 1817, 1818, 1819 (Tenth), 1881–1883; 31 U.S.C. 5311–5314 and 5316–5332.2.

■ 2. Revise § 326.8(b) to read as follows:

§ 326.8 Bank Secrecy Act compliance.

* * * * *

(b) *Compliance procedures.* (1) *Program requirement.* Each bank shall develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with recordkeeping and reporting requirements set forth in subchapter II of chapter 53 of title 31, United States Code and the implementing regulations issued by the Department of the Treasury at 31 CFR part 103. The compliance program shall be written, approved by the bank's board of directors, and noted in the minutes.

(2) *Customer identification program.* Each bank is subject to the requirements of 31 U.S.C. 5318(l) and the implementing regulation jointly promulgated by the FDIC and the Department of the Treasury at 31 CFR 103.121, which require a customer identification program to be implemented as part of the Bank Secrecy Act compliance program required under this section.

* * * * *

By order of the Board of Directors of the Federal Deposit Insurance Corporation this 16th day of April, 2003.

Valerie J. Best,

Assistant Executive Secretary.

Office of Thrift Supervision

12 CFR Chapter V

Authority and Issuance

■ For the reasons set out in the preamble, OTS amends title 12, chapter V of the Code of Federal Regulations, as set forth below:

PART 563—SAVINGS ASSOCIATIONS—OPERATIONS

■ 1. The authority citation for part 563 is revised to read as follows:

Authority: 12 U.S.C. 375b, 1462, 1462a, 1463, 1464, 1467a, 1468, 1817, 1820, 1828, 1831o, 3806; 31 U.S.C. 5318; 42 U.S.C. 4106.

■ 2. In § 563.177:

■ A. Revise the section heading; and

■ B. Revise paragraph (b) to read as follows:

§ 563.177 Procedures for monitoring Bank Secrecy Act (BSA) compliance.

* * * * *

(b) *Establishment of a BSA compliance program.* (1) *Program requirement.* Each savings association shall develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with the recordkeeping and reporting requirements set forth in subchapter II of chapter 53 of title 31, United States Code and the implementing regulations issued by the Department of the Treasury at 31 CFR part 103. The compliance program must be written, approved by the savings association's board of directors, and reflected in the minutes of the savings association.

(2) *Customer identification program.* Each savings association is subject to the requirements of 31 U.S.C. 5318(l) and the implementing regulation jointly promulgated by the OTS and the Department of the Treasury at 31 CFR 103.121, which require a customer identification program to be implemented as part of the BSA compliance program required under this section.

* * * * *

Dated: April 9, 2003.

James E. Gilleran,

Director, Office of Thrift Supervision.

National Credit Union Administration

12 CFR Chapter VII

Authority and Issuance

■ For the reasons set out in the preamble, NCUA amends title 12, chapter VII of the Code of Federal Regulations, as set forth below:

PART 748—SECURITY PROGRAM, REPORT OF CRIME AND CATASTROPHIC ACT AND BANK SECRECY ACT COMPLIANCE

■ 1. The authority citation for part 748 is revised to read as follows:

Authority: 12 U.S.C. 1766(a), 1786(q); 15 U.S.C. 6801 and 6805(b); 31 U.S.C. 5311 and 5318.

■ 2. In § 748.2:

■ A. Revise the section heading; and

■ B. Revise paragraph (b) to read as follows:

§ 748.2 Procedures for monitoring Bank Secrecy Act (BSA) compliance.

* * * * *

(b) *Establishment of a BSA compliance program.* (1) *Program requirement.* Each federally-insured credit union shall develop and provide for the continued administration of a

program reasonably designed to assure and monitor compliance with the recordkeeping and recording requirements set forth in subchapter II of chapter 53 of title 31, United States Code and the implementing regulations issued by the Department of the Treasury at 31 CFR part 103. The compliance program must be written, approved by the credit union's board of directors, and reflected in the minutes of the credit union.

(2) *Customer identification program.* Each federally-insured credit union is subject to the requirements of 31 U.S.C. 5318(l) and the implementing regulation jointly promulgated by the NCUA and the Department of the Treasury at 31 CFR 103.121, which require a customer identification program to be implemented as part of the BSA compliance program required under this section.

* * * * *

Dated: April 7, 2003.

Becky Baker,

Secretary of the Board, National Credit Union Administration.

[FR Doc. 03–11019 Filed 5–8–03; 8:45 am]

BILLING CODE 4810–02–P; 6720–01–P; 6210–01–P; 7537–01–P; 4810–33–P; 6714–01–P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34–47752, File No. S7–25–02]

DEPARTMENT OF THE TREASURY

31 CFR Part 103

RIN 1506–AA32

Customer Identification Programs for Broker-Dealers

AGENCIES: Financial Crimes Enforcement Network, Treasury; Securities and Exchange Commission.

ACTION: Joint final rule.

SUMMARY: The Department of the Treasury, through the Financial Crimes Enforcement Network (FinCEN), and the Securities and Exchange Commission are jointly adopting a final rule to implement section 326 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. Section 326 requires the Secretary of the Treasury to jointly prescribe with the Securities and Exchange Commission a regulation that, at a minimum, requires brokers or dealers to implement reasonable procedures to verify the identity of any person seeking to open an account, to the extent reasonable and practicable; to maintain records of the information used to verify the person's identity; and to determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to brokers or dealers by any government agency. This final regulation applies to brokers or dealers in securities except for brokers or dealers that register with the Securities and Exchange Commission solely because they effect transactions in securities futures products.

DATES: *Effective Date:* This rule is effective June 9, 2003.

Compliance Date: Brokers or dealers subject to this final regulation must comply with it by October 1, 2003.

FOR FURTHER INFORMATION CONTACT: *Securities and Exchange Commission:* Division of Market Regulation, (202) 942–0177 or *marketreg@sec.gov.*

Treasury: Office of the Chief Counsel (FinCEN), (703) 905–3590; Office of the General Counsel (Treasury), (202) 622–1927; or the Office of the Assistant General Counsel for Banking & Finance (Treasury), (202) 622–0480.

SUPPLEMENTARY INFORMATION:

I. Background

A. Section 326 of the USA PATRIOT Act

On October 26, 2001, President Bush signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act or Act).[1] Title III of the Act, captioned ''International Money Laundering Abatement and Anti-terrorist Financing Act of 2001,'' adds several new provisions to the Bank Secrecy Act (BSA).[2] These provisions are intended to facilitate the prevention, detection, and prosecution of international money laundering and the financing of terrorism. Section 326 of the Act adds a new subsection (l) to 31 U.S.C. 5318 of the BSA that requires the Secretary of the Treasury (Secretary or Treasury) to prescribe regulations ''setting forth the minimum standards for financial institutions and their customers regarding the identity of the customer that shall apply in connection with the opening of an account at a financial institution.''

Section 326 applies to all ''financial institutions.'' This term is defined broadly in the BSA to encompass a variety of entities, including commercial banks, agencies and branches of foreign banks in the United States, thrifts, credit unions, private banks, trust companies, brokers and dealers in securities, investment companies, futures commission merchants, insurance companies, travel agents, pawnbrokers, dealers in precious metals, check-cashers, casinos, and telegraph companies, among many others.[3]

The regulations implementing section 326 must require, at a minimum, financial institutions to implement reasonable customer identification procedures for (1) verifying the identity of any person seeking to open an account, to the extent reasonable and practicable; (2) maintaining records of the information used to verify the person's identity, including name, address, and other identifying information; and (3) determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency. In prescribing these regulations, the Secretary is directed to take into consideration the types of accounts maintained by different types of financial institutions, the various methods of opening accounts, and the types of identifying information that are available.

B. Overview of Comments Received

On July 23, 2002, Treasury and the SEC jointly proposed a rule to implement section 326 with respect to brokers or dealers in securities (broker-dealers).[4] We received 20 comments in

[1] Pub. L. 107–56.

[2] 31 U.S.C. 5311 *et seq.*

[3] *See* 31 U.S.C. 5312(a)(2), 5312(c)(1)(A). For any financial institution engaged in financial activities described in section 4(k) of the Bank Holding Company Act of 1956, the Secretary is required to prescribe the regulations issued under section 326 jointly 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 ''banking agencies''), the Securities and Exchange Commission (Commission or SEC), and the Commodity Futures Trading Commission (CFTC).

[4] Customer Identification Programs for Broker-Dealers, Securities Exchange Act of 1934 Release No. 46192 (July 12, 2002), 67 FR 48306 (July 23, 2002) (Notice of Proposed Rulemaking or NPRM). Treasury simultaneously published (1) jointly with the banking agencies, a proposed rule applicable to banks (as defined in 31 CFR 103.11(c)) and foreign branches of insured banks; (2) a proposed rule applicable to credit unions, private banks and trust companies that do not have a federal functional regulator; (3) jointly with the SEC, a proposed rule applicable to mutual funds; and (4) jointly with the CFTC, a proposed rule applicable to futures commission merchants and introducing brokers. Customer Identification Programs for Banks, Savings Associations, and Credit Unions, 67 FR 48290 (July 23, 2002); Customer Identification Programs for Certain Banks (Credit Unions, Private Banks and Trust Companies) That Do Not Have a Federal Functional Regulator, 67 FR 48299 (July 23, 2002); Customer Identification Programs for Mutual Funds, IC–25657 (July 12, 2002), 67 FR 48318 (July 23, 2002); Customer Identification Programs for

Continued

Office of Thrift Supervision
Department of the Treasury

1700 G Street, N.W., Washington, DC 20552 • (202) 906-6000

Customer Identification Programs

A Staff Summary and Answers to Questions

This staff summary addresses the rules implementing Section 326 of the USA PATRIOT Act (USAPA), which require every thrift and all other financial institutions to adopt a Customer Identification Program (CIP). The memorandum includes a general summary of the regulation and extensive answers to certain important questions.

I. Congressional Mandate

Congress instructed the Secretary of the Treasury, after consultation with the financial institution functional regulators, to issue regulations implementing the requirements of Section 326 (CIP Regulation). In the CIP Regulation, thrifts are required to:

- Implement a written CIP appropriate for its size and type of business.
- Incorporate the CIP into its anti-money laundering program, which must be approved by the thrift's board of directors.
- Include in the CIP, risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. In general, thrifts must, at a minimum, obtain a name, address, date of birth, and an identification number for each customer and must verify the identity of the customer using this information. The CIP must include procedures for making and maintaining a record of information obtained pursuant to this section.
- Have procedures in the CIP for determining whether a 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 OTS and the other federal functional regulators.
- Implement procedures for providing thrift customers with adequate notice that the thrift is requesting information to verify their identities. The CIP Regulation includes a sample notice, which thrifts may use.
- Comply by the effective date. Thrifts must fully implement their CIP by October 1, 2003.

II. Summary of Final Regulation, 31 CFR 103.121

Like other sections of the USAPA, Treasury has codified the CIP Regulation in the general requirements of the Bank Secrecy Act under Part 103 of Title 31 of the Code of Federal Regulations, 31 CFR Part 103.121. By regulation, all thrifts must comply with the Bank Secrecy Act requirements found at 31 CFR Part 103, including all relevant USAPA provisions. 12 CFR § 563.177.

The CIP Regulation will impact every institution that we examine. The regulation mandates that thrifts establish account opening procedures, which include collecting certain information before opening an account, verifying the collected information within a reasonable time, and having a Customer Identification Program that addresses all aspects of a thrift's customer due diligence program.

The mandatory account opening procedures relate only to new accounts. If a thrift does not have a reasonable belief that it knows the true identity of an existing customer, thrifts must also verify identification for new accounts opened by existing customers. Accounts generated through the Internet or telephone solicitation are all covered by the final regulation. Institutions that generate accounts through these methods should adopt procedures that ensure an adequate level of customer identity verification due diligence.

The rule pertains only to customers and not to customers of the customer. Therefore, brokered deposits are excluded provided the thrift has performed adequate due diligence on the deposit broker. Also excluded are signatories of accounts. Instead, the CIP must address situations where, based on the thrift's risk assessment of a new account, the thrift will take additional steps to verify the identity of a customer that is not an individual by seeking information about individuals with authority or control over the account, including signatories, in order to verify the customer's identity.

The OTS will expect institutions to review their business operations and to incorporate a CIP that addresses the identified risks. The CIP must be incorporated into a thrift's anti-money laundering program, which must be approved by the thrift's board of directors. The CIP should encompass all activities of the thrift and its subsidiaries to the same extent as existing BSA compliance program requirements. Thrifts should incorporate their CIP into an overall BSA program, which must include (1) internal policies, procedures, and controls to ensure ongoing compliance; (2) designation of a BSA compliance officer; (3) an ongoing employee training program; and (4) an independent audit process to test programs. 12 CFR § 563.177.

III. Answers to Important Questions with Regard to the CIP Regulation

A. What accounts are covered by the rule?

Account means each 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 any 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. As a further illustration, account does not include the provision of a product or service where a formal banking relationship is not established such as check cashing, a wire transfer, or the sale of a check or money order. Also, an account does not include subaccounts held by a deposit broker, an account that the thrift acquires through an acquisition, purchase or merger, or an account opened for the purposes of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974.

B. Who is a customer for purposes of the rule?

A customer covered by the rule includes all persons that open an account. Customer also includes an individual that opens a new account for another individual who lacks legal capacity, such as a minor, or for an entity that is not a legal person, such as a civic club. In addition to individuals, a customer includes corporations, trusts, partnerships, associations, or similar organizations. Thus, the definition of customer may include a civic club, bowling league or other such organization despite its lack of legal status as a "person."

Customer does not include: a person who has an existing account with the thrift provided the thrift reasonably believes that it knows the person's true identity. Customer also does not include a financial institution regulated by a Federal functional regulator; a bank or thrift regulated by a state bank regulator; a municipality or other local, state, or federal government entity; or any entity whose stock or analogous equity interest are listed on the New York Stock Exchange or the American Stock Exchange or is designated as a NASDAQ National Market Security listed on the NASDAQ Stock Market.

C. The Customer Identification Program: What Does the Rule Require?

Thrifts must implement a written CIP tailored to their size and business type. Thrifts must incorporate the CIP into their overall anti-money laundering program, which must be approved by the thrift's board of directors. The Regulation acts as an addition to already existing anti-money laundering and BSA regulations. 12 CFR § 563.177, 12 CFR § 563.180; 31 CFR Part 103. Also, the enumerated requirements represent a floor for customer identification, not a ceiling. Thrifts must incorporate additional procedures if they maintain accounts that represent a greater risk of not knowing the true identity of a customer (*e.g.*, an attorney-in-fact account). At minimum, the CIP must include:

1. Identity Verification Procedures: What Customer Identification Information Must a Thrift Collect and Verify?

   The CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. The procedure must enable the thrift to form a reasonable belief that it knows the true identity of the customer. The procedures must be based on the thrift's assessment of the relevant risks, including those presented by

the types of accounts it maintains, the methods for opening accounts it provides, the types of identifying information available, and the thrift's size, location, and customer base.

The CIP must include procedures for collecting the following minimum information prior to opening the account (or in the case of a credit card account, before extending credit to a person that opens the account):

- Name.
- Address. For individuals, this should include actual residential or business street address. For an individual who does not have such an address, the address may include an Army Post Office or Fleet Post Office box number, or the residential or business address of next of kin or another contact person. For a person other than an individual (e.g., a business), this should include the address of the principal place of business, a local office, or some other physical location. Thrifts must get the actual street address and not just a P.O. Box. Examiners should pay particular attention to this requirement to insure that thrifts collect actual street addresses.
- Date of birth (for an individual).
- A government issued identification number. The CIP Regulation prescribes different requirements for customers who are U.S. persons and those that are non-U.S. persons. U.S. persons are United States citizens and businesses, and other entities that are organized under the laws of a State or of the United States. U.S. persons must provide a U.S. taxpayer identification number such as a social security number or employer identification number. Non-U.S. persons can use one or more of the following: a U.S. taxpayer identification, a passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard. A thrift's CIP may include procedures for opening an account for a person (including an individual) that has applied for, but has not received, a taxpayer identification number.

In addition to collecting the required information, thrifts must verify the identity of the customer using the collected information. The required verification should occur a reasonable time after the account is opened. Thrifts must develop procedures describing when it will use documents, nondocumentary methods, or a combination of both documentary and nondocumentary methods for verification.

a. Verification through Documents

The drafters of the CIP Regulation believed that most financial institutions would use documents to verify the required identification information for traditional, face-to-face account opening situations. The CIP must contain procedures that set forth

the documents that the thrift will use for this purpose. The documents could include:

- For individuals, valid (not expired) government-issued identification that evidences nationality or residence and bears a photograph or similar safeguard, such as a driver's license or passport. The preamble to the rule notes that a thrift generally may rely on government-issued identification as verification of a customer's identity, unless the document shows evident signs of fraud. The preamble also emphasizes that the value of documentary verification is enhanced by redundancy. Thrifts are encouraged to obtain more than one type documentary verification to ensure that they have a reasonable belief that they know the customer's true identity. Thrifts are also encouraged to use a variety of methods to verify the identity of a customer, especially when they do not have the ability to examine original documents.
- For corporations, partnerships, trusts, and other persons that are not individuals, documents that show the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or trust instrument.

b. Nondocumentary verification methods

The CIP must contain procedures that describe the nondocumentary methods the thrift will use to verify identity. These procedures are particularly important for those thrifts that use nontraditional methods of account opening or extending credit (e.g., Internet, telephone or mail solicitation). These positive, negative and logical verification 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 another source.
- Checking references with other financial institutions.
- Obtaining a financial statement.

Also, the CIP must address situations where an individual is unable to present a valid government issued identification that bears a photograph or similar safeguard; the thrift is unfamiliar with or questions the validity of the documents presented; the account is opened without obtaining documents; the customer opens the account without appearing in person at the thrift; or the thrift is otherwise presented with circumstances that increase the risk that the thrift will not be able to verify the true identity of the customer through documents (*e.g.*, attorney in fact accounts).

c. Additional verification for nonindividuals

The CIP must address situations where, based on risk assessment for a new account that is opened by a corporation, business, trust or other similar entity, the thrift will obtain additional information about individuals with authority or control over the account, including signatories. This verification method applies only when the thrift cannot verify the customer's true identity using the documentary and nondocumentary methods described above. For example, if a start up business engaged in foreign commercial transactions using few or no other local based businesses with principals of non-U.S. citizenship and unknown to the thrift wanted to open an account, the thrift may want to verify the identification information about individuals with authority or control over the account, including signatories. While there is no blanket requirement to verify the identity of signatories on an account, thrifts should include procedures in their CIP to address instances where they would want to identify and verify all signatories on an account.

d. Lack of verification

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

- When the thrift should not open the account.
- The terms under which a customer may use an account while the thrift verifies the customer's identity.
- When the thrift should close an account, after attempts to verify a customer's identity have failed.
- How the thrift will incorporate their SAR filing obligations into this process.

2. Recordkeeping: What records documenting the verification efforts must a thrift maintain?

The CIP must include procedures for making and maintaining a record of the information collected under the CIP Regulation. Specifically, the record must include:

- All identifying information about a customer (i.e., name, address, date of birth, and identification number).
- A description of any document relied on to verify identification, including the type of document, any identification number contained in the document, the place of issuance and the date of issuance (if any) and the expiration date. Importantly, the thrift need not maintain a copy of the document, just a description.

- A description of the methods and results undertaken to verify the identity of the customer when the thrift utilizes nondocumentary or additional methods for verification.
- A description of the resolution of any substantive discrepancy discovered when verifying the information provided by the customer. For example, a notation that the thrift closed an account that it had opened when they could not verify the address and identification number provided by a customer that opened an account over the Internet.

Thrifts must maintain the information described in the first bullet for five years after the account is closed or, in the case of credit card accounts, five years after the account becomes dormant or is closed. Thrifts must maintain the descriptions of the documents relied upon, the methods of verification of identity, and the resolution of discrepancies for five years after the thrift makes the record.

3. Government Lists: What lists of known or suspected terrorists or money launderers must the thrift consult?

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. Treasury will consult the OTS and the other federal banking agencies prior to designating a mandatory list. Ultimately, thrifts only need to check those lists designated by Treasury. Going forward, Compliance Policy will keep examiners informed of any lists that thrifts are required to consult under this section.

4. Customer Notice: Are thrifts required to provide customers with notice that they are collecting and verifying the requested information?

Yes. The CIP must contain procedures for providing thrift customer with adequate notice that the thrift is requesting information in order to verify their identity. The rule text includes the following model notice:

"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."

5. Reliance on Others. May a thrift rely on others to perform procedures under its CIP?

The CIP may include procedures specifying when a thrift will rely on another financial institution (including an affiliate) to perform any procedure in the thrift's CIP with respect to certain customers. These customers include any customer that is opening an account, has opened an account, or has established a similar formal banking or business arrangement with the other financial institution. The reliance must be reasonable under the circumstances.

The other financial institution must be subject to a rule implementing section 326 of USAPA and must be regulated by a Federal functional regulator. The other financial institution must enter into a contract requiring it to certify annually to the thrift that it has implemented an anti-money laundering program, and that it will perform the specified requirements of the thrift's CIP.

6. Are any thrifts exempt from the requirements to enact a CIP?

No. The OTS, with the concurrence of Treasury, may exempt any thrift or type of account from the CIP Regulation. We do not anticipate exempting any OTS regulated thrifts from compliance with the regulation.

D. When does the regulation take effect, when will we start examining for compliance and how does compliance with the CIP Regulation fit into the melded exam process?

Thrifts must fully implement their CIP by October 1, 2003. We will examine for compliance after October 1. For exams that commence prior to that date, examiners should remind thrifts of their upcoming obligations.

We will examine for compliance with the CIP Regulation, as well as the other applicable USAPA regulations, through our BSA program in the melded exam. We are revising this program and it will be in place prior to October 1, 2003. When the procedures are finalized, we will announce their availability on the OTS website. For all exams, regardless of their start date, the CIP Regulation adds to and does not replace any already existing anti-money laundering and BSA requirements. All institutions must incorporate the CIP into their anti-money laundering program under 12 CFR 563.177.

IV. Conclusion

The CIP Regulation under the USAPA affects every OTS regulated institution. As part of their board-approved BSA program, all thrifts are required to create and implement a comprehensive, CIP, which addresses all lines of business engaged in by the institution and its subsidiaries to the same extent as existing BSA compliance program requirements. The requirements listed in the regulation and discussed in detail above represent minimum standards. Thrifts that maintain accounts or lines of business, which include a higher risk of not knowing the true identity of the

account holder, should adopt additional customer due diligence procedures. We will examine for compliance with the CIP Regulation through the BSA program in the melded exam. The regulation becomes fully effective on October 1, 2003.

Office of Thrift Supervision
Department of the Treasury

1700 G Street, N.W., Washington, DC 20552 • (202) 906-6000

USA PATRIOT ACT PREPAREDNESS CHECK-UP

A Framework for Achieving Compliance with New USA PATRIOT Act Regulations

In issuing final regulatory requirements for Customer Identification Programs (CIP), Treasury and the banking agencies have established a compliance deadline of October 1, 2003. This affords thrifts the opportunity to evaluate their current practices and make necessary changes to assure compliance by the deadline. To assist you, we created this preparedness check-up to guide your efforts to achieve timely compliance. This framework should be useful in updating your current Bank Secrecy Act – Anti-Money Laundering (BSA/AML) program for other USA PATRIOT Act (USAPA) requirements in addition to the CIP rule, such as requirements related to responding to law enforcement information requests and to managing private banking accounts of non-U.S. persons.

We encourage all institutions to ADApT their current BSA/AML program to the new USAPA requirements: **Analyze** their current program; **Develop** a comprehensive BSA/AML program, which includes a customer identification program that addresses all of the thrift's business lines; **Apply** your revised program throughout the affected day-to-day operations; and **Test** the new program through internal audits and testing to ensure that the program functions as intended.

ANALYZE: Review your current BSA/AML program and compare it to your business strategy, operational risks, and available resources. Ask the following questions:

- *How does the way we conduct our business expose us to risk from money laundering or terrorist financing activities?*
  - — What are our current business lines and how do we generate our customers?
  - — Do we offer private banking services? If so, do we maintain private banking accounts for non-U.S. citizens and do those accounts exceed $ 1 million?
  - — Do we maintain correspondent accounts for foreign financial institutions? If yes, what country of origin are the banks that maintain the account?
- *What are the practices we currently follow to assure the identity of our customers?*
  - — What are our current policies for obtaining identifying information from our customers?
  - — Do we currently verify the identification information that we obtain from our customers, and if so, how? When do we make exceptions to identity verification and why?

- — Do we keep a record of the information we obtain and verify?
- — What is our practice for sharing information with law enforcement or others about persons whose identity or conduct we suspect?

- *What means do we use to keep our procedures, our people and our service providers up to date with respect to BSA/AML compliance obligations?*
  - — What types of BSA training do we provide to bank personnel and how has it kept pace with changes since September 11, 2001?
  - — What systems do we rely on to comply with current BSA requirements? Have we purchased additional software/system support to comply with USAPA regulations?
  - — In what ways do third party providers currently play a role in our BSA/AML program? Have the third party providers we use adjusted their systems to meet USAPA obligations?
  - — When was the last time our board reviewed and approved our BSA/AML program?
  - — What does our last internal audit tell us about our record of BSA/AML compliance and our ability to self-identify and self-correct program deficiencies before bank examiners find them?
  - — Have we designated an individual to be in charge of overall BSA/AML compliance and afforded that person adequate authority and resources to do the job? Is our current staffing in the BSA area adequate given the responsibilities imposed by USAPA?
  - — How well did we handle responding to the "Control List?" (CEO Memo 151.) What does that or other more recent experience tell us about our ability to receive and respond in a timely fashion to information requests generated by FinCEN pursuant to Section 314(a) or other government designated lists?

DEVELOP: After analyzing your current policies, procedures, and risks, you will probably need to add to your already existing BSA/AML program in order to fully comply with the new USAPA regulations and other general regulatory requirements. Ask the following questions:

- *Have we addressed each of the regulatory requirements in devising our Customer Identification Program?*
  - — Have we approached the development of our new program with industry "best practices" in mind?
  - — Do the customer identification elements of our BSA/AML program adequately address all of our business lines and methods for generating accounts?
  - — Does our CIP address how we will collect at least the minimum information required by the rule for persons opening accounts including name, appropriate address, date of birth (for individuals), and government issued identification number (such as a social security number)?

- — Do we have products, services, or market segments that warrant collecting more than the minimum amount of information to enable us to adequately identify our customers, and if so, have we described those accounts or occasions that trigger additional information collection and the elements to be gathered?
- — Does our CIP address how we will verify identification information to attain a reasonable belief regarding the true identity of our new customers or existing customers opening new accounts?
- — Have we covered situations where accounts are opened without face-to-face contact?
- — Does our CIP provide appropriate risk-based standards for assessing new accounts opened by a customer that is not an individual? Do those standards provide that in such cases the thrift will obtain information about other individuals with authority or control over an account, such as signatories, in order to verify the customer's identity?
- — Does our CIP specify situations where we will not offer banking services, will permit a customer to have limited use of an account while verifying the customer's identity, or will actually close an account?
- — Have we devised a prompt process to determine whether the customer appears on government designated lists of known or suspected terrorists?
- — Have we drafted the required notice to customers advising them that we will verify their identity in accordance with our legal obligation and policies?
- — Have we determined how customers will be notified about identity verification requirements?

- *Have we revised our BSA/AML program to address any business operations that require enhanced scrutiny?*
  - — Have we developed standards for enhanced due diligence for our private banking accounts involving non-U.S. persons? Have we determined whether or under what circumstances this level of diligence should apply to similar accounts of U.S. persons? Is it clear from our revised program that enhanced due diligence applies to existing, and not just new, private banking accounts?
  - — Have we developed standards for enhanced due diligence for our correspondent accounts with foreign banks that take into account the particular foreign institutions involved and the risk of improper activity attendant to the circumstances presented?
- *Have we devised a system for promptly responding to law enforcement inquiries and securely sharing customer information with other institutions?*
  - — Does our program designate someone who is responsible for receiving and acting on law enforcement requests distributed pursuant to Section 314(a) of USAPA?
  - — Is there a process to follow to promptly respond to law enforcement inquiries about persons suspected of money-laundering or terrorist financing?

— Have we decided whether and under what conditions to share information with other institutions about customers engaged in suspicious activities? Do those plans meet our legal obligations under the Right to Financial Privacy Act, GLBA and USAPA?

- *Have we charted a course to attain compliance in a timely fashion?*

  — Do responsibilities for OFAC compliance continue to be adequately covered after revisions to our BSA/AML program?

  — Will our updated BSA/AML program that includes the CIP be presented to, reviewed by and approved by the Board of Directors as part of the BSA compliance program in advance of the October 1, 2003 compliance deadline? Will the Board be sufficiently versed in USAPA issues and institution operations to take informed action on the updated program?

  — Are agreements with service providers being modified to include any changes necessary to assure they perform in accordance with our program and our regulatory obligations?

  — Are training modules being developed or acquired and employees being scheduled for training in accordance with their responsibilities?

  — Have we alerted internal audit or compliance review functions to the need to modify their oversight standards to cover the CIP and other changes in our BSA/AML program and regulatory obligations?

APPLY: After analyzing your current program and developing the necessary enhancements, thrifts must implement necessary changes in BSA policies and procedures. Ask the following questions:

- *Is staff informed of new requirements?*

  — What communications are being made to assure that all employees with a role in the CIP or BSA/AML are aware of their new program responsibilities or any changes in past responsibilities?

  — Have new approved policies and procedures been distributed to managers and staff?

  — Is staff training going according to plan?

  — Is the person coordinating implementation providing timely and accurate responses to staff questions and requests for guidance?

  — Is there a process for informing staff of further regulatory developments?

- *Are changes in customer identification information collection and verification practices occurring?*

  — Do we observe new customers receiving notices and providing requested identification?

  — Are any new forms being filled in completely and accurately?

- How are employees dealing with the reaction of existing customers opening new accounts?
- Are those responsible for verification of customer identities and comparison of names against designated government lists doing those tasks in the time frames called for by our CIP and regulatory standards?
- Does it appear that enough resources have been provided to sufficiently fulfill any increased compliance burden?
- Are the requisite records being maintained?

- *Are private banking accounts with non-U.S. persons and any foreign bank correspondent accounts being handled appropriately?*
  - Did we conduct a thorough review of our private banking and correspondent accounts to identify those that are subject to our program's enhanced due diligence?
  - Do the findings resulting from our account review warrant taking action to close an account, suspend account activity or file a suspicious activity report?

TEST: You should test your new program to ensure that it functions as intended. Ask the following questions:

- *Does internal audit or compliance review identify program shortcomings?*
  - Have we updated our internal audit procedures to incorporate reviews for compliance with USAPA requirements?
  - Does staff recordkeeping appear to provide an adequate compliance paper trail for our CIP and law enforcement response obligations?
  - Does an audit of sampled transactions identify CIP or other BSA/AML program deficiencies or regulatory violations?
  - Is our audit program sufficiently detailed to evaluate BSA/AML compliance including USAPA requirements? Is the frequency of audit reviews appropriate to our institution's money-laundering and terrorist financing risk profile? Does internal oversight have sufficient management independence and Board access to be effective?
  - Does the internal audit program or other reliable review sufficiently oversee the record of service providers upon whom we rely for complying with BSA/AML program or CIP obligations?
  - Have we responded to law enforcement information requests in as efficient and compliant a fashion as possible given our institution's resources?

- *Is staff and service provider implementation of regulatory requirements keeping pace with our operational needs?*
  - — Are there performance gaps in the rollout of the program among staff that require an adjustment to, or rethinking of, resource allocation?
  - — Are service providers faithfully executing their responsibilities under our new program and their own policies without a fall-off in operational productivity?
  - — Do we need to shift responsibility for certain areas of compliance to other employees given the increased responsibility of our designated BSA officer?
  - — Do we need to outsource some of our BSA compliance functions?
  - — Does it appear that we need unanticipated enhanced technological capabilities in order to fulfill our program and regulatory obligations?
- *Is our updated BSA/AML program with CIP providing us with reliable assurances of regulatory compliance?*
  - — Are there lessons learned from our initial experience or internal reviews that recommend improvements to our revised program?
  - — What does customer reaction tell us about the operating success of our CIP or private banking procedures?
  - — Is the staff conducting the program properly accountable to the Board? Are performance reports and audit reports reaching responsible senior officials?
  - — Can we respond promptly to correct any deficiencies in our BSA/AML compliance program? Are corrective action recommendations tracked to assure completion?

The OTS believes that applying the ADApT process will assist you in achieving timely compliance with the new USAPA requirements and establishing a comprehensive BSA/AML program.