

CIP: The New Acronym for Compliance

In the quest to thwart money laundering in the American banking industry, federal regulators have issued Section 326 of the USA PATRIOT Act. Understanding the finer points of Customer Identification Programs (CIPs) add to the layers of anti-money laundering compliance issues with which you must adhere.

by John Byrne

If you are involved in Bank Secrecy Act compliance you have already mastered the terms behind the acronyms SARs, CTRs, BSA, AML, EDD, and KYC. Now, add one more to the pantheon of money laundering terms: CIP or Customer Identification Program.

After what seemed an eternity — and certainly felt like it to those calling the ABA's compliance hotline — the Treasury and federal financial regulators issued the final rules to implement Section 326 of the USA PATRIOT Act.¹ Speculation is over and the industry appears to have succeeded in persuading regulators to make a number of adjustments to the original proposal. What is left now is the challenge of understanding what the rule is and what it is not.

This article will outline the major provisions of the rule and offer some insight as to your compliance responsibilities and some tips on available resources.

Congressional Direction

Section 326 of the USA PATRIOT Act² required the Secretary of the Treasury to promulgate regulations to set forth

minimum standards for financial institutions to follow in the identification and verification of customers during the account opening process.

The law requires that the regulations, at a minimum, require each covered financial institution 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 a person's identity, including name, address, and *other identifying information*; and
- consult lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency to determine whether a person seeking to open an account appears on any such list.

It is important to note that when the House Financial Services Committee passed the measure that eventually became Section 326, it made clear that the intent was for the regulations not to overburden the financial sector. Congress directed the Treasury to “make use of information currently obtained by most financial institutions in the



account opening process.”³ The committee went on to indicate that it is not the intent of the regulations to “require verification procedures that are prohibitively expensive or impractical.”

How have the agencies responded to this clear direction? Are the final rules “reasonable and practicable”? What questions remain? Let’s see.

Coverage Under Section 326

The financial institutions that will eventually be covered under Section 326 are extensive. Not all institutions, however, are obligated to comply with the rule at this time. For now, the rule covers only banks and trust companies, savings associations, credit unions, securities brokers and dealers, mutual funds, futures commission merchants, and futures-introducing brokers.

As you attempt to understand the scope of the final rule, it is important that you first address the definitions under this section. The following parts of the rule are key:

Account

One of the changes made to the rule in response to industry criticism was deletion of the term “business relationship” from the definition of “account.” This change was made to clarify that general business dealings are not part of account relationships for purposes of the rule.

The definition of “account” now covers formal banking relationships established to provide or engage in services, dealings, or other financial transactions such as:

- safety deposit boxes and other safe-keeping services;

Under Section 326, financial institutions are not required to verify the identity of individuals or other entities if there is no “account” relationship.

- deposit transactions;
- credit accounts of individuals and other extensions of credit; and
- cash management, custodian, and trust services.

The final rule also outlines that the definition of “account” does not include certain types of transactions or services, such as:

- products or services for which a formal banking relationship is not established, such as check cashing, the purchase or sale of a money order, or a wire transfer;
- accounts acquired through merger or acquisition; and
- accounts opened for the purpose of participating in employee benefit plans.

Under Section 326, financial institutions are not required to verify the identity of individuals or other entities if there is no “account” relationship. However, the final rule does remind the industry that, in some circumstances, it may be prudent to utilize the institution’s due diligence procedures to verify the identity of customers associated with transferred accounts.⁴

Customer

There were a number of major concerns with the proposed definition of “customer” under Section 326. For example, those commenting feared that a definition including those who were “seeking to open an account” would require 326 procedures on those who were simply asking for information about a product

or service. In addition, the proposed definition included any “signatory” to an account. The potential that banks would be required to verify hundreds of thousands of additional signers to corporate accounts was, in a word, mind-boggling. Concerns included the fact that many corporate accounts add signatories over time, with many signees never physically present in the bank when added.

The Treasury and the agencies acknowledged these concerns and, in the final rule, defined “customer” to mean any person who opens a “new” account. This includes each person named on a joint account unless otherwise specified. A customer is now also defined as an individual who opens a new account for a person lacking legal capacity (minor) or an entity that is not a legal person (civic club). (*Note:* See coverage of “signatories” later in this article.)

The final rule spelled out various situations in which there are no Section 326 customers. According to the final rule, a customer is *not*:

- a person with an existing account who opens a new account, provided the bank has a reasonable belief that it knows the customer’s true identity; or
- other financial institutions or government agencies or publicly traded companies to the extent of their domestic operations.

Even with the definition of customer under the final rule, some issues re-

main. Banks are reminded that even with the exception of publicly traded companies, a bank's customer identification program does apply to any foreign offices or affiliates, or subsidiaries of those entities when they open new accounts.

The exception for existing customers is a major concession by the agencies, and financial institutions must outline how they determine whether there is a reasonable belief that the existing account holder has been identified. For example, the fact that a customer received account statements, or other types of information from the institution, and there is no evidence the individual's information is not accurate should be sufficient to show reasonable belief.

Bank

The definition of "bank" means:

- banks subject to federal regulations and their subsidiaries;
- state-regulated credit unions, private banks, and trust companies; and
- U.S. offices of foreign banks but not foreign branches of U.S. banks.⁵

(Note: There are separate rules for broker/dealers and other covered financial institutions. The Treasury is considering rules to cover other financial institutions.)

The ABA urged the industry to oppose coverage of Section 326 to any individual simply "seeking" to open an account. The Association argued that the rule should not require recordkeeping for situations in which an individual does not actually receive bank services. The final rule follows that reasoning and those who merely seek to open accounts or try to open accounts but are denied are not covered.

ABA members, especially community banks, expressed concern about having to verify the identifying information about longtime customers simply because they wanted a new product. The final rule ensures that a bank that has a reasonable belief that the customer's identifying information is accurate will not have to ask for additional information under this section.

The Customer Identification Program (CIP)

At the center of the Section 326 rule is the creation of the customer identification program (CIP). There are three parts to the new CIP requirements:

- identification and verification of persons who open accounts;
- record keeping; and
- consulting the government lists of known or suspected terrorists.

Each institution will create its own customer identification program, which must be in writing and approved by the board of directors or a committee of the board. The rule actually requires that the board or committee approve the CIP in the AML procedures, which will be a "material" change requiring approval. In addition, the program should not be separate from the institution's anti-money laundering program.⁶

The preamble to the final rule points out that the board needs to have certain information to approve the CIP. Specifically, there needs to be sufficient detail to determine that:

- the bank's CIP contains the minimum requirements of the final rule; and
- the bank's identity verification pro-

cedures are designed to enable the bank to form a reasonable belief that it knows the true identity of the customer.⁷

Identification

The final rule following the majority of the comments received emphasizes that the CIP be "risk-based." Specifically, an institution must reasonably believe that it has identified the customer. Risk is based on elements such as the institution's size, location, and type of business or customer base.

The procedures for verifying the identity of the customer must describe the information that the institution needs to obtain from the customer at the time of opening the account and whether the institution will use documents, nondocumentary means, both, or additional methods to verify the identity of the customer.

The identifying information that must be obtained⁸ by the institution prior to opening the account for all customers is as follows:

- name;
- address (no P.O. Box except for members of the military);
- date of birth; and
- an identification number.

For a U.S. citizen, the institution must obtain a tax identification number. Identification numbers can be social security numbers, taxpayer identification numbers or employee identification numbers.

For a non-U.S. citizen, the institution will need one or more of the following:

- a taxpayer identification number;

- a passport number;
- an alien identification card; or
- other government-issued identification cards that show nationality or residence with a photograph or similar safeguard.

Unlike in the proposal, the bank is not required to obtain more than a single address for the customer. There is a stated exception for members of the military, and the agencies have opined that there may be other situations (i.e., seasonal addresses) that may make obtaining residential address information impractical.

Regarding the use of foreign identification documents, the final rule neither endorses nor prohibits a particular type

of identification document issued by foreign governments. This is a prime area for risk assessment. After the rule was released, the National Credit Union Administration (NCUA) announced its position that the “matricula card” was a 326-compliant document.⁹

Because the rule is “risk-based,” the institution does not have to verify each piece of identifying information. The institution will be held to a “reasonable belief” standard as to the customer’s identity. It should also be noted that banks are permitted to require customers to provide additional information to establish their identities.

In addition, the agencies do plan to

issue guidance but there is no direction yet on how an institution should react in the event that a customer’s identifying information does not match. For example, if the individual provides identifying information such as an address and there is no match, but all the other information is accurate, it remains the bank’s decision on how to proceed.

The final rule, however, does require that the CIP contain procedures for responding to circumstances such as the one mentioned above. The rule mandates that the CIP address situations in which “the institution cannot form a reasonable belief as to the customer’s true identity.”

The Case for a Systemic CIP for Commercial

If the proposition of facing substantial fines, civil forfeiture of funds from illicit transactions and even federal prison terms is not enough incentive to develop an effective Customer Identification Program (CIP), then incalculable risk of damage to an institution’s valuable brand certainly should. Clearly these additional account opening measures represent an incremental cost of doing business for institutions that needs to be managed. Taking a systemic approach to your Customer Identification Program for commercial accounts, with the help of business information providers, affords the greatest protection and efficiency.

A systemic approach better ensures the CIP is executed consistently every time and is less subject to breakdown than manual procedures. Some available so-

lutions can help to identify and evaluate commercial account risk — helping you flag only those business accounts where enhanced due diligence is warranted, enabling you to staff your investigative team at the appropriate level.

Many banks find using a business information provider avoids reliance on applicant-only provided information and lifts the burden from the customer supplying all the necessary identification information. In addition, systematic solutions can be implemented “behind-the-scenes” to minimize the impact on existing account-opening workflow and maintain customer service levels.

Requirements for Non-Persons Accounts

The final rules require the collection of

basic information to verify the identity of non-person entities:

- the entity’s name;
- principle place of business or operation (i.e. headquarters location) or local branch address;
- government issued documents — examples cited include articles of incorporation, business license, partnership agreement, or a trust instrument; and
- nondocumentary methods — illustrations cited included contacting the customer, comparing application information to public records or third-party source database, references from other institutions, or obtaining a financial statement from the account applicant.

Experienced and capable business information providers will be able to provide most, if not all, of the information

The CIP must therefore cover:

- when the financial institution will not open an account;
- terms under which the customer may use the account while his or her identity is being verified (a major change that will greatly assist credit card issuers);
- when the financial institution will close the account; and
- when to file a Suspicious Activity Report (SAR).

Verification Methods

The final rule permits verification by documents or by nondocumentary methods (e.g., online verification tools such as public databases). The rule also

advises that the CIP address situations in which additional verification may be necessary.

The CIP must state the verification policy in the program description. For example, the institution must state that it will verify identity using documents such as a driver's license, passport, or matricula card if the individual is attempting to open the account while visiting the branch. On the other hand, if the institution provides electronic banking services, the CIP should state that where the account is being opened electronically, the institution would verify the customer's identity by using a software program, online system, or public database.¹⁰ The final rule allows an insti-

tution to utilize both methods of verification or to use either in all instances.

The Treasury and the agencies carefully avoided mandating a specific list of documents to be used for verification. Instead, the final rule continues to emphasize the need for institution risk assessment in determining what is considered acceptable documentation. The government does advise that institutions consider the need for redundancy and a variety of identification methods when the risk is high.¹¹

Signatories under Section 326

As pointed out earlier, the proposed coverage of Section 326 to all new signers on corporate accounts not held by indi-

Account Opening

and means cited in the final rules to verify identity. Quality providers maintain multi-sourced data to verify identity as part of their core offerings such as robust public record items, principal interviews, financial statements, corroboration through an account's existing trading partners, and other third-party sourced information.

If you are considering a provider, seek those that can demonstrate they have this breadth in entity coverage and depth of multi-sourced data to maximize the percentage of new accounts in which identity can be verified automatically. Select business information providers also offer cost effective investigative services to obtain corroborating evidence and verify businesses when identity cannot be confirmed automatically.

Verification of identity and obtaining some additional facts about your business customers at account opening is among the most powerful means of combating fraud loss. These additional facts can also allow you to refine your AML procedures through improved customer profiling and better detect when transaction behavior is really suspicious in nature. Again, this reduces unnecessary burden on the institution's investigative group.

Lastly, the CIP solution providers can enhance your overall Know Your Customer efforts, which can have ancillary business benefits as well. With improved intelligence, right at account opening, you are in a better position to understand that commercial customer's needs and offer services that are most appropriate to them.

Leveraging solutions from a third-party provider lets institutions outsource steps in their Customer Identification Program for new commercial accounts to vendors who specialize in business information gathering and maintenance — allowing them to focus resources back on the core business of serving the financial needs of customers.

Dan DuBois, Leader, Identity and Compliance Services at D&B Corporation, can be reached by phone at (610) 882-6751; or by e-mail at duboisd@dnb.com

viduals was a major concern for the industry. It was argued that there are instances where signatories to an account will number in the hundreds. Verification of the identity of each of those signatories would be extremely costly, impractical, and not useful for law enforcement purposes. The ABA stressed the need for a “risk-based” response to the issue of signatories, and the final rule reflects that position.

A financial institution may also have to seek additional information on individuals such as signatories, who have authority or control over accounts, to form a reasonable belief that it knows the customers’ true identities if the institution’s risk assessment makes it necessary. The CIP must clearly state the policy on signatories.

Recordkeeping under Section 326

One of the most controversial sections of the Section 326 proposal was the mandate that institutions retain photocopies of documents, such as driver’s licenses, used to verify customers’ identities. While the proposal did point out that retention of copies of driver’s licenses would not violate Regulation B (Equal Credit Opportunity Act), the industry opposed the proposal because of customer concerns surrounding identity theft and the cost of copying such information, as well as ensuring that systems be developed to allow for centralizing the copying of licenses.¹²

Verification of the identity of each of those signatories would be extremely costly, impractical, and not useful for law enforcement purposes. The ABA stressed the need for a “risk-based” response to the issue of signatories, and the final rule reflects that position.

ABA members were generally opposed to the copying and retention of driver’s licenses or other government-issued documents. The final rule eliminates the requirement that licenses or other government-issued identification be copied and/or retained.¹³ However, the records required to be maintained are still quite extensive.

The final rule requires that the Customer Identification Program maintain records such as:

- the identifying information (name, address, DOB, and SSN);
- a description of the document relied on for verification (e.g. driver’s license, passport, etc.);
- a description of the methods and result of nondocumentary means of verification; and
- a description of the resolution of any substantive discrepancies.

For example, if an institution uses an online verification tool such as InstantID, it would have to record the result of the search of the customer’s identifying information. If the institution reviewed a document, it would note the type of document, place and date of issuance, and expiration date.

In most cases, per Section 1, records must be kept for five years after an account has closed. Sections 2-4 must be kept for five years after the date the information was obtained. For credit card

accounts, the retention period is five years after the card has been dormant.

Consulting Government Lists

The final rule also requires procedures for determining whether the customer appears on any federal government terrorist lists within a reasonable period of time after account opening, or earlier if required by federal law. At this time, the final rule does not describe any lists as government lists for 326 purposes. The CIP should, however, generally describe the procedures for consulting the lists.

Notices under Section 326

The final rule requires each institution to provide notices to its customers on the scope of Section 326. The rule refers to “adequate” notice and does not mandate a certain method, though it does offer a sample notice. An institution can generally describe the Section 326 requirements on a lobby poster, train employees to describe the requirements at account opening, or place the information on the account application. According to the agencies, the following would be considered adequate:

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.

Another sample:

Our bank complies with Section 326 of the USA PATRIOT Act. This law mandates that we verify certain information about you while processing your account application.

Reliance on Third Parties

In response to many comments, the final rule also allows a bank to create procedures in its CIP that outline when the institution will rely on other financial institutions, including affiliates, to perform some or all of the elements of the CIP. The reliance must be reasonable and the other institution must be

In response to many comments, the final rule also allows a bank to create procedures in its CIP that outline when the institution will rely on other financial institutions, including affiliates, to perform some or all of the elements of the CIP.

subject to AML program requirements and be regulated by a federal functional regulator. The other institution must at-test annually that it has implemented and will follow the bank's CIP.¹⁴ Financial institutions may also contract with third party service providers or agents (i.e., auto dealers) to perform the CIP functions, but the institution will be ultimately responsible for noncompliance.

Compliance Date and Next Steps

The CIP requirements must be fully implemented by October 1, 2003. To date,

we have heard from the Office of Thrift Supervision (OTS) that it will not examine institutions for CIP compliance until after that date. The agencies are also preparing FAQs to further assist with compliance questions.

The ABA will continue to provide resources to assist in crafting your institution's Customer Identification Program (CIP). The updated *ABA Industry Resource Guide on Identification and Verification of Accountholders* will be available shortly. The guide contains suggestions

| FRAUD PREVENTION



NOTHING BURNS UP YOUR PROFITS FASTER THAN FRAUD.

THINK OF US AS A FLAME-RESISTANT COATING.

From training to software,
we can help you protect your profits.



1.800.552.9410 www.bankerssystems.com

241484

on program procedures, available resources such as useful web sites and examples of CIP provisions.

For more information, please visit www.aba.com. ❖

Have a question or comment?

Use the postage-paid reply card provided in this issue or leave a message at (202) 663-5075.

1. 68 FR 25090 (May 9, 2003).

2. Pub. L. 107-56.

3. H. Rept 107-250, p. 63. The committee also reiterated the fact that banks have account opening procedures in place when it added that "[c]urrent regulatory guidance instructs depository institutions to make reasonable efforts to determine the true identity of all customers requesting an institution's services."

4. See footnote 8 from the 326 final rule 68FR 25093.

5. The last point was added to the final rule after the receipt of comments concerned with conflict of laws in certain foreign jurisdictions. The agencies and Treasury, however, have stated that they encourage banks to add the CIP throughout the entire organization unless there is a conflict.

6. A reminder that a bank's BSA or AML program must include: internal policies, procedures, and controls; designation of a compliance officer; an ongoing employee training program; and an independent audit function to test programs.

7. 68 FR 25096.

8. Credit card accounts allow a bank to obtain some of the identifying information from a third party source such as a credit reporting agency prior to extending credit.

9. In a letter to Rep. Ruben Hinojosa (D-TX), the NCUA pointed out that "the regulatory language permits the use of these cards as a means of establishing a customer's identity."

10. The agencies and Treasury do encourage institutions to use nondocumentary verification due to the increase in crimes such as identity theft. See FR at 25100.

11. The ABA is offering a verification product through an agreement with Lexis-Nexis. Information about the product, InstantID, is available on www.aba.com.

12. Credit card banks made the point that there would be a need to procure a large number of photocopy machines for remote locations such as sports arenas.

13. In response to pressure from the House Judiciary Committee, the Treasury has since published a notice asking the public to comment on, among other things, whether banks should be mandated to retain photocopies of drivers licenses. ABA is spearheading a grass-roots effort to oppose any changes such as these to the final rule.

14. The agencies have been asked whether it is sufficient that the institution being relied upon simply has a valid CIP. We believe that the answer will be yes.

about the author

John Byrne is Senior Counsel and Compliance Manager in the Regulatory and Trust Affairs Section of ABA's Government Relations Division. He is responsible for ABA's lobbying, regulatory and educational efforts on money laundering, asset forfeiture, computer security, privacy and other general electronic banking and compliance issues. In this position, he has represented the ABA before Congress, various regulatory agencies and in the media.

Mr. Byrne has been a member of the Treasury Department's Bank Secrecy Act Advisory Board since its inception and co-chairs the American Bar Association/American Bankers Association Annual Money Laundering Enforcement Seminar (now in its 15th year). John also co-chairs the "SAR Activity Review" project, advises the Association of Anti-Money Laundering Specialists (ACAMS), staffs ABA's Fraud Prevention Oversight Council, Payment Systems Committee as well as the Compliance Executive Committee. He has written extensively on money laundering and privacy issues and is a frequent contributor and advisor to *Money Laundering Alert*, *Bankers Hotline*, *ABA Bank Compliance*, and other banking publications. John has been a faculty member of the ABA's Graduate Compliance School, the Association's Bank Security School, speaks at dozens of conferences each year and has done several overseas money laundering deterrence programs for the US Customs Service and the State Department.

Mr. Byrne also was the first private sector recipient of the "Director's Medal for Exceptional Service" from the Treasury Department's Financial Crimes Enforcement Network (FinCEN). John is also the editor of ABA's *Money Laundering and Terrorism Issues Update*, a weekly e-mail newsletter.

Prior to this position, Mr. Byrne was an Assistant General Counsel in ABA's Office of the General Counsel. He received his undergraduate degree from Marquette University in Milwaukee, Wisconsin and his J.D. from George Mason University in Arlington, Virginia. He is a member of the District of Columbia and Pennsylvania Bars. He can be reached by phone at (202) 663-5029; or by e-mail at jbyrne@aba.com.