WILMER, CUTLER & PICKERING

Financial Institutions Group Newsletter

MAY 23, 2003

The Treasury Department Issues Final Customer Identification Rules Under Section 326 of the USA Patriot Act

On May 9, 2003, the U.S. Treasury Department ("Treasury") joined with the federal functional regulators to publish in the *Federal Register* long-awaited final rules to implement the customer identification requirements of section 326 of the USA Patriot Act ("Patriot Act"). The rules call on a wide range of financial institutions—including banks, broker-dealers, mutual funds, and certain futures businesses—to establish Customer Identification Programs ("CIPs") to verify the identity of each customer who opens an account.

Financial institutions covered by the new rules will have until **October 1, 2003** to establish CIPs under which they will: collect certain minimum customer identification information from each customer who opens an account; utilize risk-based measures to verify the identity of each customer who opens an account; record customer identification information and the verification methods and results; provide notice to customers that the financial institution will seek identification information; and compare customer identification information with government-provided lists (not yet created) of suspected terrorists.

In considering compliance with these new rules, it is important to keep in mind that these rules only address identification of customers at the outset of the relationship. These rules are limited in scope and are *not* 'know your customer' rules. Accordingly, compliance with these rules does not substitute for proper due diligence and 'know your customer' efforts.

I. Background

Section 326 of the USA Patriot Act required Treasury to prescribe minimum standards for customer identification in connection with the opening of an account at a financial institution. Specifically, the statute directed Treasury to issue rules that call on financial institutions to implement "reasonable procedures": (a) to verify the identity of a person seeking to open an account, "to the extent reasonable and practicable"; (b) to maintain records of the information used to verify a person's identity; and (c) to consult lists of terrorists provided by the government to determine whether a person seeking to open an account appears on any such list. In issuing such rules, Treasury was required to take into consideration the various types of accounts maintained by the various types of financial institutions—that is, Treasury was instructed to avoid a "one-size-fits-all" approach.

Last July, Treasury—with the relevant federal functional regulators—issued a set of parallel proposed customer identification rules that applied to certain financial institutions—namely, depository institutions, broker-dealers, mutual funds, and certain futures related businesses. *See, e.g.*, 67 Fed. Reg. 48,290 (July 23, 2002). The proposed rules presented significant issues for the institutions covered by them, and the proposals elicited many comments from industry participants. Financial institutions complained that, among other things, the proposals (i) contained

onerous recordkeeping requirements, (ii) required identification steps not only with respect to accountholders but also those with signatory authority over accounts and those with the ability to conduct trades in accounts, and (iii) mandated needlessly detailed identification verification requirements. *See* WCP Financial Institutions Group Newsletter (Aug. 9, 2002).

II. The Final Rules' Requirements

a. Summary

The final rules encompass significant modifications from the proposed rules that resolve many (but not all) of the issues raised in the proposals. Among other noteworthy features, the final rules include the following:

- The requirements of the rules generally apply only to accountholders. In contrast to the proposals, there is generally no requirement in the final rules to look behind accountholders and obtain identification information on "signatories" on a bank account and others with authority over an account.
- The final rules also do not apply to financial institutions regulated by a federal regulator; state-regulated banks; federal, state, and local governmental entities; corporations whose shares are publicly traded on U.S. exchanges; and existing customers who open new accounts.
- Certain types of accounts—including ERISA accounts and accounts acquired by acquisition, merger, and purchase of assets or assumption of liabilities—are excluded from the rules.
- All of the identifying information received from a customer will not need to be verified (as the proposed rules required); instead, the final rules require that the customer's *identity* be verified.
- Instead of requiring institutions to keep copies of identity verification documents, as did the proposed rules, the final rules call on financial institutions to record information about the verification documents.
- The final rules shorten the recordkeeping requirements related to verification of customer identification; verification records need be kept for 5 years from the date that the record is created (and not, as in the proposal, 5 years after the account is closed).
- In response to industry requests, the final rules authorize financial institutions to rely in limited circumstances on the customer identification efforts of certain U.S. (but not foreign) financial institutions.

More detail on each of these requirements and other relevant aspects of these rules is provided below.

b. What Institutions Are Covered by the Final Rules?

The final customer identification rules—like the proposed rules—apply to (a) depository institutions, including banks, savings associations, and credit unions; (b) securities broker-dealers; (c) mutual funds; and (d) futures commission merchants ("FCMs") and introducing brokers ("IBs").

The rules apply to U.S. branches of foreign banks, but they do *not* apply to foreign branches of U.S. banks. This is consistent with other Patriot Act and Bank Secrecy Act obligations.[1] The rules also apply to bank subsidiaries and to non-federally regulated depository institutions, such as state-chartered private banks and trust companies. (It is interesting to note that the non-federally regulated banking entities are in a somewhat unique position—they have customer identification requirements under this set of rules, but they do not (yet) have Anti-Money Laundering Program ("AML Program") requirements under section 352 of the Patriot Act.)

These rules also do not apply to investment advisers or hedge funds, but Treasury has indicated elsewhere that these entities may in the future be subject to customer identification requirements.

c. Compliance Deadline

The final rules become effective on June 9, 2003, but, as noted above, the requirements of the rules will not apply to accounts opened before October 1, 2003.

---

[1] *See, e.g.*, 67 Fed. Reg. 60,562, 60,565-66 (Sept. 26, 2002) (defining a "covered financial institution" to include U.S. branches of foreign banks but not foreign branches of U.S. banks).

d. Scope and Key Definitions

The rules generally require financial institutions to establish CIPs to determine the identity of each ***customer*** who opens an ***account***. Those are the two key terms in the final rules; these terms drew plenty of attention in the proposed rules.

Customer. The final rules essentially define a "customer" as the **accountholder**. Accordingly, the person who or entity that opens a new account is the customer to which all of the customer identification steps apply. As a general matter, there is no need to look through trusts to get information on beneficiaries, to look behind omnibus accounts if an intermediary is the accountholder, or to look for information on signatories on accounts or persons who otherwise have authority over accounts of customers.

There is one relatively minor exception to the general rule, which exception covers an individual who opens an account for (i) an individual who lacks legal capacity (such as a minor child) or (ii) an entity that is not a legal person (such as a civic club). In these two situations, the individual who opens the account is the customer—and it is that person to whom all the identification requirements apply. There also is an important caveat to the general rule about not needing to look behind the accountholder: the rules state that CIPs adopted by financial institutions must describe and address—on a risk basis—those situations when they will look behind a business or entity to find out about underlying individuals or signatories.

The treatment of accountholders as customers is a significant change from the proposed rules. Those proposed rules had defined customer to include, in the case of the bank rules, signatories on an account and, in the case of the broker-dealer rules, those with authority over the account.

Another important element of the customer definition, and again a helpful departure from the proposed rules, is the exclusion of certain entities from the definition of customer. The excluded entities are: (i) "financial institutions" regulated by a federal regulator;[2] (ii) "banks" regulated by a state, which includes credit unions, private banks, and trust companies; (iii) federal, state, and local governmental entities; and (iv) corporations whose shares are publicly traded on U.S. exchanges.[3]

The final rules provide that a customer with an existing account will not be treated as a customer (who needs to be identified) as long as the financial institution has a reasonable belief that it knows the identity of the person or entity. Because a foreign branch of a U.S. bank is not covered by the rule, a customer of that foreign branch would not qualify for the existing customer exclusion. That customer, if it wanted to open a U.S. bank account, would need to be identified.

Another warning—there is no exception for a person who or entity that is not a customer of the financial institution but is known to bank personnel.

Account. The final rules generally define an "account" as a formal or contractual relationship with the financial institution to provide financial products and services. This includes, for banks, for example, safety deposit boxes and safekeeping and cash management services.

This excludes, for banks, isolated and "one-off" relationships such as check cashing, sales of checks, or money orders. The final rules further clarify that business dealings in connection with a financial institution's own operations or premises (*e.g.*, a relationship with the financial institution's technology provider) do not constitute an account.

There are two exclusions to the definition of account. To begin with, the final rules exclude accounts acquired via acquisition, merger, purchase of assets, or assumption of liabilities. (The preamble to

---

[2] SEC-registered investment advisers do not appear to fall within this excluded category; investment advisers are not treated as "financial institutions" under the Bank Secrecy Act. Treasury has, however, proposed to designate registered investment advisers as financial institutions and to require them to implement AML programs. *See* 68 Fed. Reg. 23,646 (May 5, 2003). When this rulemaking is finalized, SEC-registered investment advisers presumably will be financial institutions (and not customers) for customer identification purposes.

[3] With respect to publicly listed companies, the preambles to the final rules make clear that foreign subsidiaries, offices, and affiliates must be treated as customers (and do not fall within the exclusion). It is unclear, however, how U.S. subsidiaries are to be treated; the preambles seem to assume that they are excluded from the definition of customer, but the regulatory language and cross-references to 31 CFR 103.22(d)(2) do not address U.S. subsidiaries of publicly listed companies.

the rules warn, however, that there may be particular situations in which a financial institution may need to conduct due diligence on customers acquired via this exception.) Also excluded are accounts opened for the purpose of participating in an employee benefit plan under ERISA.

e. Customer Identification Program—Minimum Requirements

As a general rule, each financial institution's CIP must be appropriate for the institution's size, location, and type of business. The final rules state that the CIP must be incorporated into the elements of each financial institution's AML Program, and the CIP must include written, risk-based procedures that enable the financial institution to determine with reasonable certainty the identity of each customer. The procedures must include certain minimum steps regarding the collection and verification of identification information.

Collection of Customer Identification Information. At a minimum, a financial institution must obtain **from each customer** the following four pieces of information **prior to** opening an account. There is a limited exception to this requirement for credit card banks, which are permitted to obtain the necessary information from a third-party source (*e.g.*, a credit report) prior to extending credit. The required minimum information is as follows: (i) name; (ii) date of birth (for an individual); (iii) street address; and (iv) identification number.

For an individual, the address obtained must be a residential or business street address. There is an exception for those in military service—they may provide an Army or Fleet P.O. Box or the address of a family member or next of kin. For a customer that is not an individual, the address must be the principal place of business, local office, or other physical location.[4]

The identification number required for U.S. persons is a taxpayer identification number (social security number or employer identification number). For a non-U.S. person, a financial institution must get one or more of (i) a taxpayer identification number, (ii) a passport number and country of issuance; (iii) an alien identification card number; or (iv) another government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.[5] The final rules state that if a foreign business does not have an "identification number," the financial institution must request government-issued documentation certifying the existence of the business. The rules do not state, however, what constitutes appropriate documentation, and presumably this will be based on the judgment of the financial institution.

A financial institution may open an account for an individual or entity that has applied for a U.S. tax identification number. The financial institution needs to confirm that the customer has applied for the tax identification number (before opening the account) and then get the identification number within a reasonable period.

Verification of Customer Identity. In contrast to the proposed rules, which required verification of *identification information*, the final rules require each financial institution to verify only the customer's *identity* such that the financial institution has reasonable confidence that it knows the true identity of the customer; this identity verification does not necessarily entail verifying each piece of identification information, as some read the proposed rules to require.

Verification of identity must be conducted through documents or other means, and each institution's CIP must describe the verification procedures to be used. In the final rules, Treasury makes clear that financial institutions need not verify the accuracy of each piece of identification information. (Commenters had objected to the proposed rules because they seemed to require such verification.) Verification must be completed within a 'reasonable time' after the account is opened.

---

[4] Credit card banks, in particular, had raised an objection to the requirement of a street address in their comments on the proposed rule. Credit card banks had sought permission to obtain only mailing addresses. Treasury stuck firm to the street-address requirement, arguing that street addresses are important to law enforcement.

[5] The final rules do not state what is acceptable government-issued documentation, and financial institutions will need to make risk-based determinations as to what identification they will accept.

Verification may be accomplished either through **documentary** or **non-documentary** means. To begin with, a CIP must contain procedures describing when a financial institution will verify its client's identity through documents and setting forth the documents that will be used for this purpose.[6] There is no express requirement in the rules to obtain more than one piece of identification or to take other steps if a person provides a piece of acceptable identification (such as a driver's license), but in the preamble to the final rules, Treasury "encourages" financial institutions to get more than one piece of documentary identification to make sure of a customer's true identity.

The rules give two sets of examples of documents that may be used. In the case of an individual, documentary verification may be conducted by reviewing a valid government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard (*e.g.*, a driver's license or passport). In the case of a person other than an individual, documentary verification may be conducted by reviewing documents showing the existence of the entity, such as certified articles of incorporation or a partnership agreement, or a government-issued business license.

CIPs also must contain procedures describing what non-documentary means of identification will be used and when they will be used—either in lieu of or in addition to documentary identification. The non-documentary procedures should address a number of situations: (i) when an individual is unable to provide valid government-issued identification; (ii) when the financial institution is not familiar with the identification presented; (iii) when the customer opens an account without appearing in person; and (iv) when there are risk factors that indicate that the bank is unable to verify the true identity of the customer through documents.

The final rules state that verification without documents may be accomplished using one or (preferably) more of the following methods: contacting a customer; cross-checking information provided by the customer with information obtained from a database; checking references; and/or reviewing a customer's financial statements.

Information Regarding Signatories and Others. The proposed rules included all "signatories" within the meaning of the term "customer" and, therefore, would have required financial institutions to obtain and verify identification information regarding each account signatory. The final rules contain no such requirement. Instead, the final rules state that when a new account is opened by a customer who is not an individual and the customer's identity cannot be sufficiently verified using documentary or non-documentary means, the CIP must require other verification efforts; in particular, the CIP must require the institution to obtain information regarding individuals with authority or control over the account, such as account signatories.

The final rules state that a financial institution is required to obtain information about persons other than a customer only when the financial institution cannot obtain documentary or non-documentary verification of the customer's identification and that customer is not an individual.

Lack of Verification. CIPs must address situations in which the financial institution cannot form a reasonable belief that it knows a customer. The procedures need to describe: when the financial institution should not open an account; when the financial institution may conditionally allow a customer to open and use an account while verification is in progress; when the financial institution should close an account; and when the financial institution should file a Suspicious Activity Report.[7]

f. Recordkeeping

The recordkeeping provisions were some of the most controversial provisions of the proposed rules. The proposed rules would have required (1) keeping copies of all documentation, and (2) keeping all records for five years after an account is closed. The final rules modify both requirements, to the benefit of industry.

What Records Must Be Kept? The final rules provide that each financial institution must record: all customer identification **information** (name, date of birth if applicable, address, and identifi-

---

[6] Each firm will need to conduct its own risk-based analysis of the documents on which it will rely.

[7] Commenters on the proposed rules requested a safe harbor to protect a financial institution if it determines that an account may not be opened or must be closed due to insufficient verification of a customer's identity. The preambles to the final rules, however, explain that there is no statutory basis for a safe harbor. Financial institutions accordingly must remain vigilant about their obligations under laws such as the Equal Credit Opportunity Act and the Fair Credit Reporting Act.

cation number); a **description** of any document used for verification purposes, including (if available) any identification number on the document, the place of issuance, the date of issuance and the expiration date; a **description** of the methods and results of any non-documentary verification efforts; and a **description** of the resolution of any substantive discrepancies uncovered during the verification process. Thus, under the final rules, the underlying documents from which this information is drawn need not be kept.

How Long to Keep The Records. The final rules take a bifurcated approach, distinguishing between identification information and verification information. A financial institution must retain the records of identification information (name, date of birth if applicable, address, and identification number) for five years after the account is closed.[8] This is no different than the proposed rules. But, a financial institution must retain the records of verification for **five years after the records are made**. This is different than the proposed rules, which required the maintenance of all records for five years after account closure.

g. Reliance on Other Financial Institutions

Many commenters on the proposed rules asked to be allowed to rely on other financial institutions' customer identification efforts. The idea was that if one financial institution had identified a customer, a second should not have to go through all the same steps.

The final rules incorporate a limited reliance concept. One financial institution may rely on another for any of the elements of the customer identification program if: (i) reliance is reasonable under the circumstances; (ii) the other financial institution is subject to a requirement to implement an anti-money laundering program (which means that for now, and until Treasury's proposed anti-money laundering rule for investment advisers becomes effective, other financial institutions will not be able to rely on investment advisers, which are not subject to anti-money laundering program requirements); (iii) the other financial institution is regulated by a federal functional regulator (this excludes reliance on state-chartered banks and trust companies, as well as insurance companies); (iv) the other financial institution contractually agrees to perform the identification function; and (v) the other financial institution certifies annually that it has implemented its anti-money laundering program and will perform the specified requirements of the customer identification program.

These steps apply equally to affiliates and non-affiliates. Significantly, because foreign financial institutions are not required by U.S. regulations to implement anti-money laundering programs, a U.S. financial institution may not rely on the customer identification efforts of a foreign financial institution.

If a financial institution takes the requisite steps so that it may rely on another financial institution, it is not responsible for another financial institution's failure to fulfill the CIP responsibilities. A financial institution that does not take the requisite steps, however, still may contract with agents to perform services on behalf of the financial institution. Thus, for example, a mutual fund can use a transfer agent to perform CIP services. But, in these situations, the financial institution retains ultimate responsibility for the agent's compliance and, in the fund example, the fund must monitor its transfer agent's performance.

h. Notice to Customers

The final rules state that a financial institution must provide customers with notice that the institution will seek identification information. The notice must be "reasonably designed" to ensure that a customer is able to view the notice before opening an account. Depending on the manner in which the financial institution opens accounts for its clients, the institution may be able to post the notice on its website or in its lobby, or include the notice in its account applications.

The final rules include sample notice language:

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

[8] In the case of a credit card account, the identification information must be retained for five years after the account is closed *or* becomes dormant.

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.

i. Comparison with Government Lists

The final rules state that each institution's CIP must include procedures for determining, within a reasonable period of time, whether a customer appears on any government-provided list of suspected terrorists. The final rules also clarify, however, that financial institutions are not required to seek out any lists but will only be required to check lists specifically provided by the government. As yet, no such lists have been created. Note: this requirement does not supplant or obviate the need to comply with OFAC requirements.

III. Compliance Steps

Although the compliance deadline is not until October 1, financial institutions will need promptly to begin planning how they will comply with the new rules. Because the rules afford considerable compliance flexibility, they also will require thoughtful application to particular situations and circumstances. Financial institutions will need to make a number of risk-based determinations about how they will treat various types of accounts and customers, based on their size, location, and potential money laundering risk: For instance, when will the institution verify the identity of beneficial owners, signatories, and others? When will the institution use documentary versus non-documentary means of verification? What documents will the institution accept?

Financial institutions also will want to consider modifying new account documentation and disclosures. They also will need to verify that their recordkeeping systems have the capacity to record and then retain the necessary information for the prescribed period of time. Financial institutions further will need to consider whether they want to rely on another financial institution's customer identification efforts and, if so, set in place the necessary contracts.

* * *

If you have questions or would like further information about the final rules or other aspects of the Patriot Act, please contact:

Todd Stern +1 (202) 663-6940
todd.stern@wilmer.com
Satish Kini +1 (202) 663-6482
satish.kini@wilmer.com
David Cohen +1 (202) 663-6925
david.cohen@wilmer.com
Stephen Heifetz +1 (202) 663-6558
stephen.heifetz@wilmer.com