WILMER, CUTLER & PICKERING

Financial Institutions Group Newsletter

AUGUST 9, 2002

TREASURY ISSUES PROPOSED "CUSTOMER IDENTIFICATION" RULES FOR PATRIOT ACT SECTION 326 AND AN INTERIM FINAL "SPECIAL DILIGENCE" RULE FOR PATRIOT ACT SECTION 312

Continuing its effort to issue the numerous regulations necessary to implement the USA PATRIOT Act ("Patriot Act"),[1] the Treasury Department published two rules in the *Federal Register* on July 23, 2002. The first rule — actually, a set of five separate but closely related proposed rules — would implement the customer identification requirements of section 326. The second rule implements, on an interim basis, the special and enhanced due diligence requirements of section 312. These rules, along with the rules implementing section 352's requirement that each financial institution implement a program to guard against money laundering, form the foundation for the post-Patriot Act anti-money laundering regulatory regime.

In previous Newsletters, we have discussed the anti-money laundering program requirements of section 352 and the proposed rule to implement section 312's special and enhanced due diligence requirements.[2] This Newsletter addresses the recently proposed section 326 customer identification regulations and the interim regulation that implements in part, and postpones in part, the special and enhanced due diligence obligations of section 312.

I. Proposed "Customer Identification" Rules Implementing Section 326

One theme that has emerged from Treasury's Patriot Act rulemaking is an effort to treat different components of the financial services industry differently while, at the same time, imposing generally consistent obligations on all. This is evident in the industry-specific rules Treasury has issued, and has promised to issue, to implement the anti-money laundering program requirements of section 352. It is also evident in the five separate proposed rules Treasury, along with the appropriate federal functional regulators, published on July 23 to implement the customer identification provisions of Section 326 of the Patriot Act. There is a proposed rule for (1) federally regulated banks, savings associations, and credit unions;[3] (2) banks, trust companies, and credit unions that lack a federal regulator;[4] (3) securities broker-dealers;[5] (4) mutual funds;[6] and (5) futures

[1] Pub. L. No. 107-56 (2001).

[2] *See* WCP Financial Institutions Group Newsletter, "Treasury Issues Regulations on Anti-Money Laundering Programs," May 22, 2002; WCP Financial Institutions Group Newsletter, "Treasury Issues Proposed 'Special Due Diligence' Rule for Correspondent and Private Banking Accounts," June 11, 2002.

[3] 67 Fed. Reg. 48,290 (July 23, 2002) (issued jointly by 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).

[4] 67 Fed. Reg. 48,299 (July 23, 2002) (issued by the Treasury Department's Financial Crimes Enforcement Network ("FinCEN")). The proposal calls for the same rules to apply to state-regulated banks as banks with a federal functional regulator.

[5] 67 Fed. Reg. 48,306 (July 23, 2002) (issued jointly by FinCEN and the Securities and Exchange Commission).

commission merchants and introducing brokers (collectively, "FCMs").[7] Treasury intends to issue additional rules applicable to other financial institutions, such as insurance companies and credit card system operators, that are not covered in these five rule proposals.

Each of these proposed rules requires similar customer identification efforts from the various financial institutions that are subject to the rules – in particular, each rule requires financial institutions to implement, as part of their overall anti-money laundering program,[8] a risk-based "Customer Identification Program" that enables the institution to form a reasonable belief that it knows the true identity of its customers. Nonetheless, because each proposed rule is tailored to the particular industry that it is designed to cover, there are some notable differences among the proposed rules that we highlight below. For purposes of analysis, it is useful to group the rules into two camps – the "bank rules" for depository institutions with a federal functional regulator and non-federally regulated institutions, and the "securities firm rules" for broker-dealers, FCMs, and mutual funds.

A. The Statutory Requirement for Reasonable Customer Identification Procedures

Section 326 of the Patriot Act requires Treasury to implement final regulations by October 25, 2002 that set 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."[9] At a minimum, these regulations must require financial institutions to implement "reasonable procedures" to:

(1) verify the identity of any person seeking to open an account, "to the extent reasonable and practicable;"

(2) maintain records of the information used to verify the person's identity (including name, address, and other identifying information); and

(3) consult government lists of known or suspected terrorists to determine whether a person seeking to open an account appears on any such list.

Two features, in particular, stand out in this provision. First, Congress did not demand that Treasury issue regulations requiring financial institutions to "know" their customers. That is, section 326 does not require a revival of the proposed "Know Your Customer" regulation, which was withdrawn in 2000 in the face of intense criticism from industry and privacy advocates. Instead, Congress called only for regulations requiring financial institutions to "identify" their customers. The difference is critical. All section 326 says is that institutions should know with whom they are doing business; it does not require institutions to obtain information from every customer sufficient for the institution to be in a position to assess whether a specific transaction is normal and expected (or, conversely, abnormal or suspicious) for every customer. That sort of heightened due diligence is reserved for foreign correspondent and private banking accounts and addressed in section 312.

Second, Congress said repeatedly that financial institutions should be required to do only what is possible in identifying their customers. Section 326 provides that the regulations are to require "reasonable procedures" to obtain minimum identifying information. It then reinforces this point, stating that institutions are to be required to verify a customer's identity only "to the extent reasonable and practicable." This point is also reflected in the House Report on the Patriot Act, which indicates that Congress intended "the verification procedures prescribed [in the customer identification rules to] make use of information currently obtained by

---

6 67 Fed. Reg. 48,318 (July 23, 2002) (issued jointly by FinCEN and the Securities and Exchange Commission).

7 67 Fed. Reg. 48,328 (July 23, 2002) (issued jointly by FinCEN and the Commodity Futures Trading Commission).

8 Section 352 of the Patriot Act, 31 U.S.C. § 5318(h), requires financial institutions to develop anti-money laundering programs. *See* WCP Financial Institutions Group Newsletter, "Treasury Issues Regulations on Anti-Money Laundering Programs," May 22, 2002.

9 31 U.S.C. § 5318(*l*)(1).

most financial institutions in the account opening process."[10]

B. The Customer Identification Requirement of the Proposed Rules

As noted, the proposed rules require each covered financial institution to implement a written "Customer Identification Program" ("CIP"). The CIP must be part of the institution's anti-money laundering program and must be approved by the firm's most senior governing body (*e.g.*, the board of directors) or a person specifically authorized by that body to approve the CIP.

The basic substantive standard that the proposed rules would impose is this: Each financial institution's CIP must enable it to form a reasonable belief that it knows the true identity of its customers. Although, as we describe below, the proposed rules prescribe certain minimum requirements and standard procedures for all CIPs, the proposal also makes clear that each institution's CIP should be designed in light of (1) the type of customer identification information available to the institution and (2) an assessment of the risks posed by the particular business operations of the institution.[11] As in other rules promulgated to implement the Patriot Act, the regulators are not prescribing a one-size-fits-all approach to customer identification, but instead are calling for a risk-based approach to designing and implementing a CIP.

C. Specific Provisions Common to Each Proposed Rule

1. Key Definitions

Account: Each of the proposed rules defines "account" generally to be a "formal" business relationship between a customer and a financial institution. There is a significant difference, however, in how the scope of the term is described in the preambles to the bank rules, on the one hand, and the securities firm rules, on the other hand.

The proposed bank rules state that the definition of the term "account" is drawn from the definition of the term in section 311 – something that is not required by either section 311 or 326, but was done, according to the preambles, to promote consistency and "reduce confusion." Accordingly, in the bank rules "account" means "a *formal* banking or business relationship established to provide *ongoing* services, dealings or other financial transactions." The proposed rules make clear that "this term is not intended to cover infrequent transactions. . . ."

The securities firm rules, in contrast, neither link the definition of "account" to section 311, nor limit its scope to "ongoing" relationships. Rather, the proposed rules explain the term "account" "is intended to include *all types* of" accounts maintained by broker-dealers, FCMs, and mutual funds, *e.g.*, accounts to purchase, sell, lend, or otherwise hold securities or other assets, cash accounts, margin accounts, prime brokerage accounts, etc. This appears to be a much broader definition of the term account than in the bank customer identification rules; if so, it runs counter to Treasury's expressed intent that "the effect of the [customer identification] rules [will] be uniform throughout the financial services industry," and will create significant difficulties for securities firms in implementing the customer identification requirements of section 326.

Customer: Each of the proposed rules defines "customer" as any person (or entity) that opens a "new account," or is given signing or trading authority over an account, after the effective date of the final regulation.[12]

---

[10] *See* H.R. Rep. No. 107-250, pt. 1, at 63 (2001).

[11] The rules do not specify what type of "risk" is at issue – the specific risk that an institution will not be able to identify its customer or the more general risk that an institution will be used for money laundering and terrorist financing. Other rules, most notably the rules implementing the anti-money laundering program requirement of section 352, direct institutions to focus on the risk that an institution will be used for money laundering. Nonetheless, it seems more apt for the customer identification rule to have institutions assess the risk of misidentification. This point should be clarified in the final rule.

[12] Interestingly, the bank rules define a customer as any person "seeking to open a new account," while the securities firm rules define customer as any person "who opens a new account." This difference in regulatory language does not appear to suggest a substantive difference in the scope of the defined term.

On the one hand, this definition substantially reduces the potential burden of the CIP that financial institutions must implement, because pre-existing account holders are not "customers," nor are persons or entities with existing signing or trading authority over an existing account. A pre-existing account holder becomes a "customer" only if that person opens a new account at the financial institution; likewise, a person with signing or trading authority over an existing account becomes a "customer" only if that person is granted new authority over an existing account or authority over a new account.[13] Because the procedures in a CIP must be applied only with respect to "customers," the prospective focus of the definition of "customer" represents a substantial limitation on the proposed rules' burden.

On the other hand, because customer identification procedures must be undertaken each time an institutional account holder seeks to add a signatory to a bank account or an authorized person to a trading account, this provision would impose a very significant burden on financial institutions. For example, if a U.S. bank or brokerage opens a trading account for another financial institution, the U.S. bank or brokerage will need to identify each of the persons at the financial institution that has authority to direct trades through that account. That is, the U.S. bank or brokerage will be required to obtain personal identification information, as outlined below, from each of the other institution's employees who have the trading authority, and will have to undertake a full "customer" identification process each time the other institution grants trading authority to a new individual.[14]

The proposed rules do not appear to call for a risk-based application of this provision – the same customer identification information must be obtained for every person with signing or trading authority on an account, regardless of the identity of the principal account holder. Not only does this "across-the-board" requirement depart from Treasury's normal risk-based approach to anti-money laundering, it also conflicts with Congress' admonition that Treasury's rules require the implementation of "reasonable procedures" that "make use of information currently obtained by most financial institutions in the account opening process."

2. Minimum Requirements For All CIPs

Each financial institution subject to the customer identification rules must implement a CIP that satisfies the following minimum criteria:

Obtain Identifying Information: At a minimum, each financial institution's CIP must require that certain identifying information be obtained *before* opening a new account for a customer, adding a person as a signatory to a bank account, or adding an authorized person to a trading account. The proposed rules do not permit any exception to this requirement – although, as we note below, verification may occur within a reasonable time *after* an account is opened, the identifying information itself must be obtained before any account is opened.

The specific information that must be obtained differs depending on whether the customer is a U.S. person or a non-U.S. person,[15] and whether the customer is an individual or a non-individual, as follows:

- For U.S. persons, the institution must obtain an identification number, which can be a social security number, an individual taxpayer identification number, or an employee identification number. In addition,
  - for individuals, the institution must obtain the customer's name, address (both residence and, if different, mailing), and date of birth;
  - for non-individuals, the institution must obtain the customer's name and address

[13] A person seeking information about an account who does not then open a new account is not a customer, nor is a person whose account is transferred from one financial institution to another in a transaction not initiated by the customer (*e.g.*, in an acquisition or merger).

[14] If the other institution is foreign, this requirement may conflict with the privacy expectations of the foreign institution's employees.

[15] "U.S. person" means: (i) a U.S. citizen; or (ii) a corporation, partnership, trust or person (other than an individual) that is established or organized under the laws of a state or the United States.

(both principal place of business and, if different, mailing).[16]

- For non-U.S. persons, the institution must obtain an identification number. This number can be a taxpayer identification number, a passport number, an alien identification card number, or the number and country of issuance of any other government-issued document evidencing nationality or residence *and* bearing a photograph or "similar safeguard."[17] In addition,

  - for individuals, the institution must obtain the customer's name, address (both residence and, if different, mailing), and date of birth;

  - for non-individuals, the institution must obtain the customer's name and address (both principal place of business and, if different, mailing).[18]

Verify Identifying Information to the Extent Reasonable and Practicable: After obtaining the required minimum identifying information, the proposed rules require that each institution's CIPs describe how the institution will verify, to the extent reasonable and practicable, the accuracy of a customer's identifying information.

The procedures must detail when an institution will use documents to verify customer identification information and when it will use "non-documentary" verification methods either in addition to, or lieu of, documents alone.

The documents that may be used for an individual include an unexpired government-issued identification showing nationality or residence with a photograph or similar safeguard. For a non-individual, relevant documents include documents showing the existence of the entity, such as the entity's registered articles of incorporation, partnership agreement, or government-issued business license.

An institution is required to use non-documentary verification methods – such as checking fraud databases, credit agencies, or references – when an individual does not or cannot present adequate verifying documents, as when an account is opened over the internet or by mail. Non-documentary means must also be used if circumstances indicate an increased risk that a customer's "true identity" cannot be established through documents alone.

Regardless of the method used, verification must occur within a reasonable period of time before or after the account is opened so the customer identification information is neither stale nor are opportunities created for money laundering.[19] If verification is not possible within a reasonable time after opening an account, the CIP must (1) specify the actions an institution will take (including when an account should not be opened); (2) address the terms under which a customer may conduct transactions while his/her identification is being verified; and (3) specify at what point, after attempts to verify identity have failed, an institution will close an account and/or file a Suspicious Activity Report.

Check Government Lists of Terrorists: For years, financial institutions, chafing at the amorphous requirement to identify and report suspicious transactions, have requested regulators to list persons who are

---

[16] An institution may open an account for a new business that has applied for a taxpayer identification number and has not yet received one, but the CIP must require the institution to (i) obtain a copy of the application before it opens the account, and (ii) obtain the identification number within a reasonable period of time after establishing the account.

[17] The preambles explain that the proposed rules use the term "similar safeguard" to permit the use of "any biometric identifiers" other than a photograph, *e.g.*, fingerprint, DNA sample, etc.

[18] The proposed bank and broker-dealer rules assert that the existing customer identification requirements codified at 31 C.F.R. §§ 103.34(a) & 103.35(a), which generally permit a bank or broker-dealer to maintain an account even if complete identifying information is not obtained, "are inconsistent with the intent and purpose of section 326." Treasury proposes to repeal those provisions.

[19] An institution need not verify identifying information of an existing customer seeking to open a new account if the institution (i) previously verified the customer's identity and (ii) continues to have a reasonable belief that it knows the customer's identity.

known to the government to be involved in money laundering or, more recently, terrorist financing. Institutions have said that if provided with such lists, they would stop and report transactions by identified persons and entities.

The proposed rules implementing section 326's requirement that financial institutions consult government lists of known or suspected terrorists before opening an account make this request a reality. Each proposed rule requires the CIP to contain reasonable procedures, as part of the customer identification process, (1) to check lists of known or suspected terrorists *provided to the institution* by any federal government agency; (2) to ensure that the institution follows all agency directives issued in connection with such lists; and (3) to respond when a customer appears on such a list.

Importantly, the preambles to each of the proposed rules specifies that a financial institution is required to consult only those lists circulated by the federal government and made available to the financial institution. A financial institution need not search out government lists of known or suspected terrorists to comply with this rule. Rather, for this provision to function, the government must make available lists to financial institutions.

Keep All Records: The proposed rules provide that an institution's CIP must include reasonable procedures for maintaining records of information used to verify name, address and other identifying information, including information provided by the customer and other information sought and/or relied upon in the verification process. All these records must be retained for *five years* after the date the account is closed, and may be retained electronically.

Provide Customer Notice: The financial institution's program must include procedures for providing customers with adequate notice that the institution is requesting information to verify their identity. This may be accomplished by posting a sign in the lobby, or by providing oral, written or electronic notice.

3. Risk Focus

Along with the prescriptive minimum customer identification and verification requirements for each CIP, the proposed customer identification rules also repeatedly make clear that each financial institution's CIP must take account of the specific risks encountered by the specific business operations of each institution implementing the program.

The bank customer identification rules elaborate on this concept briefly, saying that the CIP must be "appropriate given the bank's size, location and type of business," and that "identity verification procedures . . . are to be risk-based."

The proposed customer identification rules for securities firms go even further and set out illustrative lists of "relevant risk factors" that each firm must consider in crafting its CIP. The proposed customer identification rule for broker-dealers, for example, sets out seven pertinent factors to consider:

(1) The firm's size;

(2) The firm's location;

(3) The method by which customers open accounts at the firm (*i.e.*, in person or remotely);

(4) The types of accounts the firm maintains;

(5) The types of transactions the firm executes for customers;

(6) The firm's customer base (*i.e.*, individuals or legal entities; foreign or domestic, and if foreign, from which countries); and

(7) Whether a firm relies on another firm to undertake any of the customer identification steps for "shared accounts."[20]

The seventh risk factor is particularly significant. Each of the proposed securities firm customer identification rules acknowledges that customer identification efforts may be allocated by contract among firms that, for other purposes, work together in servicing an account. The broker-dealer rule explains that an introducing and clearing broker-dealer may allocate customer identification responsibility in a carrying or clearing agreement governed by NASD Rule 3230 and/or NYSE Rule 382. Likewise, the proposed rules for FCMs permits allocation of responsibility between an introducing broker and the FCM or between an FCM and a clearing broker. And the mutual fund rule notes that

[20] The proposed rules for mutual funds and FCMs contain a similar list of factors.

some elements of the customer identification process "will be best performed by personnel of . . . separate entities," such as a transfer agent.

Note, however, that each rule conditions the ability to allocate customer identification responsibility in three significant ways. First, the allocation of responsibility must be done by contract – informal understandings of which firm is handling which aspect of the customer identification process are not sufficient.

Second, the firm allocating customer identification responsibilities must "continually assess" the quality of the other firm's performance and cease reliance on the other firm if it "is no longer reasonable" to do so.

Finally, regardless of whether responsibility is allocated, each firm remains responsible for ensuring that all aspects of the customer identification rule are met for every customer. This limitation will, most likely, reduce the extent to which firms avail themselves of this option and, as a result, significantly undercut the "efficiencies" that Treasury says allocation is designed to foster.

D. Request for Comments

The regulators have requested comment on a number of topics including, among other things:

- Whether the proposed definition of "account" is appropriate;
- How the proposed regulation should apply to various types of accounts designed to allow customers to conduct business immediately;
- Whether the definition of "bank" should (1) exclude foreign branches or (2) clarify that a foreign branch must comply only to the extent the program does not contravene applicable local law;
- Whether foreign entities will be able to provide the identifying information required;
- Whether the proposal would subject firms to conflicting state laws;
- The extent to which proposed verification procedures would make use of information currently used in the account opening process.

Comments are due by September 6, 2002.

II. Special Due Diligence for Correspondent and Private Banking Accounts

On May 30, 2002, the Treasury Department issued a proposed rule implementing the special and enhanced due diligence provisions of section 312 of the Patriot Act.[21] Under this provision, financial institutions must apply special due diligence procedures to all correspondent accounts for foreign financial institutions and all private banking accounts for non-U.S. persons; financial institutions must apply enhanced due diligence for correspondent accounts for offshore banks, banks in blacklisted jurisdictions, and private bank accounts for senior foreign political figures. As we discussed in a previous Newsletter, Treasury's proposed rule envisioned a very broad-gauged compliance obligation for the entire financial services industry.[22]

In an expression of unusual unity, eleven major associations representing a broad spectrum of financial institutions filed a lengthy joint comment letter on the proposed rule that raised concerns regarding a number of the provisions in the proposed rule. Facing a July 23 statutory effective date for section 312, and confronted with "substantial and important concerns about the scope of the [proposed] regulation as well as the major definitions," the Treasury Department issued an interim final rule on July 23.[23] This interim rule postpones implementation of any specific regulatory requirement until Treasury issues a final rule, thereby permitting Treasury more time to consider the shape and content of its 312 regulation. Treasury stated that it anticipates issuing a final rule by October 25, 2002.

The interim final rule does not, however, relieve all financial institutions of compliance with section 312. Instead, it directs that certain financial institutions

[21] 67 Fed. Reg. 37,736 (May 30, 2002).

[22] *See* WCP Financial Institutions Group Newsletter, "Treasury Issues Proposed 'Special Due Diligence' Rule for Correspondent and Private Banking Accounts," June 11, 2002.

[23] 67 Fed. Reg. 48,348 (July 23, 2002).

comply with the statutory obligations set out in section 312, and it provides "guidance" on what a 312-compliant due diligence program would entail.

Banks Only–Correspondent Accounts: Banks must comply with both the correspondent account and private banking provisions of section 312. The interim rule provides that a due diligence program for correspondent accounts will be reasonable if it focuses compliance efforts on correspondent accounts that pose a high risk of money laundering. Banks should give priority to conducting due diligence on (1) high-risk foreign banks for which the U.S. bank maintains "correspondent deposit accounts or their equivalents;" (2) correspondent accounts used to provide services to third parties (*i.e.*, payable-through accounts); and (3) high-risk foreign financial institutions such as money transmitters. In addition, U.S. banks must give priority to accounts opened on or after July 23, 2002.

In addition to these "baseline" requirements, a bank's enhanced due diligence program will be reasonable if it focuses on foreign banks that operate in non-cooperative countries or have offshore licenses. It also should comport with industry best practices, *e.g.*, the New York Clearing House Association's "Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking" (March 2002) and the Basel Committee on Banking Supervision's paper on "Customer Due Diligence for Banks" (October 2001). Again, priority must be given to accounts opened on or after July 23, 2002.

Banks, Broker-Dealers, and FCMs–Private Banking Accounts: The interim rule requires banks, along with broker-dealers and FCMs, to comply with the private banking provisions of section 312. The interim rule provides that a private banking due diligence program will be reasonable if it focuses on private banking accounts that present a "high risk" of money laundering and applies enhanced scrutiny to accounts maintained by senior foreign political figures, their close associates and immediate family members. The interim rule suggests that institutions look to three prior issuances for guidance on what such a due diligence program should contain – the Federal Reserve's "Private Banking Activities" paper, (SR 97-19 (SUP)), the Treasury Department's "Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Official Corruption" (January 2001), and the Wolfsberg AML Principles (May 2002).

* * * *

For further information regarding these rules or other aspects of the Patriot Act, please contact any one of the following:

Todd Stern	(202) 663-6940 tstern@wilmer.com
Satish Kini	(202) 663-6482 skini@wilmer.com
David S. Cohen	(202) 663-6925 dcohen@wilmer.com
Stephen Heifetz	(202) 663-6558 sheifetz@wilmer.com