Anti-Money Laundering Committee

Suggested Practices For Customer Identification Programs

Securities Industry Association

TABLE OF CONTENTS

Suggested Practices For Customer Identification Programs*

Preamble

The Securities Industry Association ("SIA") and its members have long supported efforts to deter and prevent money laundering. To this end, on February 13, 2002, the SIA issued its *Preliminary Guidance for Deterring Money Laundering Activity* (the "*Preliminary Guidance*") to assist member firms in establishing anti-money laundering programs ("AML Programs")[1] and implementing newly enacted provisions of the USA PATRIOT Act of 2001 (the "PATRIOT Act"). Since that time, many new implementing regulations proposed by the U.S. Department of the Treasury's Financial Crimes Enforcement Network) ("FinCEN") and the Securities and Exchange Commission ("SEC") have become effective. In addition, the NYSE and the NASD have issued their own AML rules and related guidance for compliance with the PATRIOT Act.[2]

Of particular significance is the joint FinCEN/SEC rule implementing section 326 of the PATRIOT Act ("CIP Rule"), which requires broker-dealers to implement a customer identification program ("CIP").[3] Although the CIP Rule became effective on June 9, 2003, the final compliance date to implement a CIP was October 1, 2003.

To supplement its *Preliminary Guidance*, the SIA's Anti-Money Laundering Committee ("AML Committee") is issuing these *Suggested Practices for Customer Identification Programs* ("*CIP Suggested Practices* "). The *CIP Suggested Practices*, which should be read in conjunction with the *Preliminary Guidance*, [4] discusses the minimum identification information and verification procedures required by the CIP Rule and sets forth what the AML Committee believes are certain practices firms

---

* **Prepared by the SIA's Anti-Money Laundering Committee with the assistance of Betty Santangelo of Schulte Roth & Zabel LLP. Dorothy Kozakiewicz, a former associate, also provided substantial assistance.**

1 *See* the SIA's website www.sia.com/moneyLaundering/pdf/AMLguidance.pdf. As the Preliminary Guidance was issued in advance of the final implementation of the CIP rules, firms must take that fact into account in incorporating these practices into their AML programs. The Preliminary Guidance is in the process of being updated to reflect later developments under the PATRIOT Act.

2 *See* NYSE Rule 445 and NASD Rule 3011, which require broker-dealer firms to have AML compliance programs. *See also* NYSE Information Memo 02-21 (May 6, 2002) and NASD's Notice to Members 02-21 (April 2002), NASD Notice to Members 03-34 (June 2003) and NASD's Updated Small Firm Template discussing the CIP Rule (updated Sept. 2003).

3 Joint Final Rule, *Customer Identification Programs for Broker-Dealers*, 68 Fed. Reg. 25,113 (May 9, 2003), codified at 31 C.F.R. § 101.122.

4 SIA's *Preliminary Guidance* has been referred to in both the FinCEN/SEC Joint Final Rule (68 Fed Reg. at 25,126) and the NASD's *Updated Small Firm Template*. *See supra* notes 2 and 3.

may wish to consider in developing and implementing an effective CIP.[5] The AML Committee recognizes that, due to their differences in size, customer base, business model, and location, securities firms face varying challenges in protecting against potential money laundering. While the AML Committee hopes that the *CIP Suggested Practices* will assist all firms in developing and implementing their CIPs, each firm must conduct an assessment of its own risks and implement a CIP that best reflects an account opening process designed to address its own vulnerabilities to money laundering and terrorist financing. Accordingly, where not inconsistent with the CIP Rule, firms may find it appropriate to adjust these practices to their own business models.

Firms also should be aware that the CIP is only a part of the Firm's obligations and that the Firm will need to take additional steps to comply with its broader AML Program obligations, including, if necessary, appropriate additional due diligence procedures. The *CIP Suggested Practices* does not address such obligations.[6] It also does not address the requirements under any other section of the PATRIOT Act, including sections 311 and 312. In addition, firms also have separate obligations under the SEC, the NYSE, and the NASD rules and regulations, (*e.g.*, SEC Rules 17a-3 and 17a-4 under the Securities Exchange Act, NYSE Rule 405 and NASD Rule 2310), as well as the programs administered by the Office of Foreign Assets Control ("OFAC").[7] The *CIP Suggested Practices* does not attempt to address these issues, except where specifically required by the CIP Rule. While such obligations are important to a firm's overall AML compliance program and should be addressed by each firm, the *CIP Suggested Practices* is limited to a discussion of a firm's obligations under the CIP Rule.

1.0 General Discussion of the CIP Rule

The CIP Rule requires all persons registered, or required to be registered, with the SEC as a broker-dealer to establish, document and maintain a written CIP that must be part of its overall AML Program. Among other things, the CIP must include risk-based procedures for verifying, to the extent reasonable and practicable,

---

[5] The regulatory analysis and recommendations contained in this document reflect the views of the SIA Anti-Money Laundering Committee and have not been endorsed by FinCEN, the SEC or any self-regulatory organizations.

[6] For further guidance on the way in which the CIP Program fits into the AML Program, see the *Preliminary Guidance* issued in February 2002, available on the SIA website (*see* n. 1).

[7] OFAC administers a series of laws that impose economic and trade sanctions against: (a) certain foreign governments and their agents, (b) agencies and organizations that sponsor terrorism, and (c) international narcotics traffickers and individuals and organizations engaging in activities related to the proliferation of weapons of mass destruction. All U.S. persons are prohibited from conducting transactions with any individual, entity or jurisdiction included on the OFAC program lists. In addition, firms should have procedures for comparing customers to the OFAC lists (*see also* Section 4.0 Timing of Verification and n.47, below).

the identity of each "customer" who opens a new "account." In establishing its CIP, each firm must identify and consider relevant risk factors associated with its business, including its size, location and customer base, the types of accounts it maintains, the methods by which accounts can be opened, and the types of identifying information available. The overriding requirement of the CIP Rule is that a firm's CIP must be designed to allow it to form "a reasonable belief that it knows the true identity of each customer."

At a minimum, a firm's CIP must include:

1. a description of the types of identifying information the firm will obtain from customers opening new accounts;
2. procedures for verifying the identity of such customers, to the extent reasonable and practicable, within a reasonable period of time before or after account opening;
3. procedures for making and maintaining records related to the CIP;
4. procedures for determining whether customers opening new accounts appear on any government list of known or suspected terrorists or terrorist organizations specifically designated by FinCEN and the SEC as a section 326 list;[8]
5. procedures for providing notice to customers prior to account opening that information may be requested to verify their identity;
6. procedures specifying the action the firm will take when it cannot adequately verify the identity of a customer opening a new account.

As stated, the CIP Rule applies to all registered broker-dealers, including those that are subsidiaries of banks or bank holding companies. Banks themselves are subject to their own CIP Rule, which is substantially similar to the broker-dealer CIP Rule. To avoid duplicative regulation, FinCEN has indicated that broker-dealer subsidiaries that comply with the broker-dealer CIP Rule will be viewed by bank supervisory agencies as being in compliance with applicable bank CIP regulations.[9]

---

[8] FinCEN and the SEC have not yet designated a list for purposes of the CIP Rule. However, firms should not confuse the list requirement in the CIP Rule with the obligations and prohibitions that arise under OFAC. OFAC imposes separate requirements that all firms must comply with on a continuous basis.

[9] *See Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain non-Federally Regulated Banks*, 68 Fed. Reg. 25,090, 25,093 (May 9, 2003).

Because various types of financial institutions are subject to comparable CIP Rules,[10] in a multi-service firm, different parts of a firm's business may be subject to their own CIP requirements. In such circumstances, a firm may wish to consider whether to adopt a consolidated CIP for the different parts of its businesses or whether separate CIPs would work best for its business model. For example, where a broker-dealer is dually-registered as a futures commission merchant ("FCM"), it could consider having one CIP for both aspects of its businesses. Because the various CIP Rules are substantially similar, a firm that complies with the broker-dealer rule would presumably also satisfy the FCM rule.

1.1 Overview of "Customer"

Pursuant to the CIP Rule, a "customer" is defined as a person[11] that opens a new account; and an individual who opens a new account for (1) an individual who lacks legal capacity; or (2) an entity that is not a legal person. Minors and informal groups (non-legal entities) are not generally treated as customers under the CIP Rule. Moreover, generally firms do not have to verify the identity of individuals with trading authority over the account. However, since a CIP is risk-based, a firm's CIP program should identify those situations in which it is appropriate to take additional steps to verify the identity of those with authority or control over the account.[12]

a. Exclusions from the Definition of "Customer"

Certain entities are excluded from the definition of "customer" for purposes of the CIP Rule, including:

---

[10] *See id.*; *see also Customer Identification Programs for Mutual Funds*, 68 Fed. Reg. 25,131 (May 9, 2003); *Customer Identification Programs for Futures Commission Merchants and Introducing Brokers*, 68 Fed. Reg. 25,149 (May 9, 2003); *Customer Identification Programs for Certain Banks Lacking a Federal Functional Regulator*, 68 Fed. Reg. 25,163 (May 9, 2003). FinCEN is also considering whether to apply the CIP requirement to investment advisers, commodity trading advisors, and unregistered investment companies. *See* Proposed Rules: *Anti-Money Laundering Programs for Investment Advisers*, 68 Fed. Reg, 23,646, 23,650 (May 5, 2003); *Anti-Money Laundering Programs for Commodity Trading Advisors*, 68 Fed. Reg. 23,640, 23,644 (May 5, 2003); and *Anti-Money Laundering Programs for Unregistered Investment Companies*, 67 Fed. Reg, 60,617, 60,621 (Sept. 26, 2002).

[11] "Person" is defined as "an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture, or other unincorporated organization or group, an Indian tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal personalities." *See* 31 C.F.R. § 103.11(z).

[12] *See Guidance Issued on Customer Identification Regulations, FAQs: Final CIP Rule*, issued by the Federal Reserve Board, FDIC, the Financial Crimes Enforcement Network ("FinCEN"), NCUA, OCC, OTS, and FinCEN (issued in Jan. 2004 and revised in April 2005) (hereinafter "Banking FAQs") at pg. 2, FAQ #1 of the *Definition of "customer"* section (discussing accounts opened by persons with power of attorney).

1. financial institutions[13] regulated by a Federal functional regulator, i.e., the banking agencies (including the Board of Governors of the Federal Reserve System (the "Federal Reserve Board"), the Office of the Comptroller of the Currency ("OCC"), the Board of Directors of the Federal Deposit Insurance Corporation ("FDIC"), the Office of Thrift Supervision ("OTS"), the National Credit Union Administration ("NCUA")), the SEC, and the Commodity Futures Trading Commission ("CFTC") (these include broker-dealers, FCMs, mutual funds, and federally regulated banks);
2. banks regulated by state bank regulators;
3. departments or agencies of the United States and of any State or political subdivision of any State;
4. entities established under the laws of the United States, State laws, political subdivision of any State, or under an interstate compact, that exercise governmental authority on behalf of the U.S., or any such State, or political subdivision; and
5. "publicly listed" entities, *i.e.*, entities, other than banks, whose common stock or analogous equity interests are listed on the NYSE, or the American Stock Exchange ("AMEX"), or whose common stock or analogous equity interests have been designated as a Nasdaq National Market Security listed on the Nasdaq Stock Market (except stock or interests listed under the separate Nasdaq Small Cap Issues heading).[14] A publicly listed non-bank financial institution is excluded only to the extent of its domestic operations, unless it falls under the first exclusion (*i.e.*, it is a financial institution regulated by a Federal functional regulator).

Subsidiaries of these excluded entities are generally not covered by the parent entity's exclusion. Accordingly, unless a subsidiary of an excluded entity independently falls under an exclusion (e.g., a subsidiary of a publicly listed entity may be independently excluded as a financial institution with a Federal functional regulator), or the relationship itself does not meet the definition of "account," a broker-dealer's CIP will apply to such a subsidiary that opens a new account with the broker-dealer. However, as noted above, a firm, as part of its risk assessment, may determine that in certain situations U.S. subsidiaries present lower risk for verification purposes.

---

[13] "Financial institutions" are defined in 31 U.S.C. §§ 5312(a)(2) and (c)(1).

[14] Companies listed on the over-the-counter bulletin board and pink sheets are not considered listed companies for purposes of this exclusion.

While a firm is not required to obtain identifying information for, or to verify the identity of, entities excluded from the definition of "customer," in practice, it may, in some circumstances, be more burdensome to separate out the excluded entities based on the criteria outlined above. Regardless of how firms determine the status of an entity, each firm should have a comprehensive process for concluding that an entity is excluded. The firm should consider documenting its rationale for excluding from its CIP process entities that do not patently fall within the exclusions.

In addition, U.S. and non-U.S. existing customers, both individuals and entities, that open a new account are not considered "customers" for purposes of the CIP Rule, so long as the firm has a reasonable belief that it knows their true identity. Thus, for example, if an existing brokerage customer opens a new account, the firm would not need to verify the customer pursuant to its CIP if it reasonably believes it knows the customer's true identity.[15] This belief could be based on any number of factors, such as the customer identification procedures in place when the original account was opened, information obtained during the customer's relationship with the firm, and the customer's account history and interactions with the firm.

1.2 Overview of "Accounts"

A. Definition of Account

The CIP Rule defines an "account" as "a formal relationship with a broker-dealer established to effect transactions in securities, including, but not limited to the purchase or sale of securities and securities loaned and borrowed activity, and to hold securities or other assets in safekeeping or as collateral." This definition is very broad and includes not only the wide variety of formal accounts that firms open for both U.S. and non-U.S. persons – such as retail accounts, including cash and margin accounts, and institutional accounts, including omnibus and prime brokerage accounts – but also the various types of non-account relationships firms enter into with their customers, including transactions with counterparties and the provision of certain investment banking services. This *CIP Suggested Practices* attempts to address a firm's CIP obligations in all of these various relationships.

---

[15] A person that has an existing account with the financial institution's affiliate does not qualify as "a person who has an existing account" with the financial institution. However, the financial institution may be able to rely on the affiliate to perform elements of its CIP. *See* the Banking FAQs at pg. 5, FAQ #4 of the *Person with an Existing Account* section (discussing "existing customers.")

B. Exclusions from the Definition of Account

The CIP Rule excludes from the definition of "account" any account opened for the purpose of participating in an employee benefit plan established pursuant to the Employee Retirement Income Security Act of 1974 (*e.g.*, defined benefit or defined contribution plans established pursuant to section 401(k). This would include, for example, plans established pursuant to sections 401(a) and 501(a) of the Internal Revenue Code of 1986, as amended ("IRC"). The exclusion also covers certain trust, custodial or administrative accounts established to maintain and administer assets under a non-ERISA employee retirement, benefit or deferred compensation plan.[16] For purposes of the CIP rule, a participant or beneficiary of such accounts will not be deemed to be the firm's customer. Rather, the customer will be the employer that contracts with the firm to establish the account. In addition, any account that a firm acquires through an acquisition, merger, purchase of assets or assumption of liabilities is excluded from the definition of "account." For example, transfers of accounts that result from an introducing broker-dealer changing its clearing firm would fall within this exclusion.[17] In these situations, firms do not have to obtain information about or verify the identity of the accountholder. There may be situations, however, when it would be appropriate for the firm to verify the identity of the customer associated with the account it is acquiring.[18] In any event, as discussed above, acquired accounts are still subject to other regulatory requirements and must be covered by other elements of a firm's AML Program, including account monitoring and suspicious activity reporting.

1.3 Development of a Risk-Based Approach

Although the AML Committee recognizes that entities serviced by the retail and institutional parts of firms differ in various respects, the information obtained for identification purposes will be similar. However, the verification process may differ based on an assessment of the risks relating to certain of these customers. Certain institutional and retail accounts may present lower risks of money laundering and the firm may view such accounts as subject to lower risk in developing its CIP.[19] For example, retail accounts for individual U.S. employees of broker-dealers could in certain instances be considered low risk because they are subject to

---

[16] This would include "accounts established by governmental entities to administer retirement or benefit plans or by employers to administer stock option or restricted stock plans." See the Banking FAQs at pg. 6, FAQ #7 of the "Definition of Customer" section.

[17] To the extent that the introducing firm and clearing firm intend to rely on each other to undertake the CIP requirements with respect to customers that open accounts after the transfer, they would need to meet the requirements for reliance, as set out below.

[18] *See* 67 Fed. Reg. 48,306, 48,307 n.2 (July 23, 2002) (Proposed Broker-Dealer CIP Rule).

[19] *See* SIA's *Preliminary Guidance* for a fuller discussion of institutional accounts.

screening for employment purposes and therefore their accounts may not require any additional verification of identity.

Further, because some U.S. institutional clients can be either regulated by a Federal functional regulator (e.g., broker-dealers, FCMs, mutual funds, or federally regulated banks) or publicly listed, as discussed in section 1.1, subject to certain exceptions, these clients will be excluded from the CIP Rule.[20] In certain instances, a firm may wish to view a U.S.-based customer that is a wholly-owned subsidiary of, or that is otherwise controlled by, an entity that falls within the CIP exclusions from the definition of "customer" as presenting lower risk, if the subsidiary is itself not excluded. In addition, some of the U.S. institutional clients that are not excluded (e.g., an IA or an insurance company that does not fall within the CIP exclusions) may be opened for well-established, reputable financial services firms that are well-known in the securities industry and thus could be viewed as lower risk for verification purposes.

The CIP Rule recognizes that accounts can be opened by various methods. According to the CIP Rule, a firm's CIP must be based on its assessment of the relevant risks, including the various methods for opening accounts, such as in person, by telephone, by mail or online. For example, for accounts opened in person, firms may find documentary verification appropriate. For accounts opened for individuals by methods other than in person, e.g., by telephone, mail or online, firms may find such documentary identification less useful, or more difficult to obtain, and may be more likely to rely on non-documentary verification.[21] To the extent that the method for opening an account is unusual given a firm's business model, the firm could undertake additional verification steps by either contacting the individual,[22] obtaining references or a financial statement of the individual, or by any other appropriate means based on the firm's risk assessment.[23]

---

[20] See section 1.1(a), above, for a discussion of exclusions from the definition of "customer."

31 C.F.R. § 103.22(d)(2)(iv).

[21] The AML Committee understands that as a matter of industry practice, most firms do not permit persons with non-U.S. addresses or those who do not have a social security number to open accounts online. Those with online business models sometimes choose to require those prospects to download the application and mail it in, rather than open it directly online.

[22] "Contacting the individual" could include, among others, having the individual visit the firm, calling the individual in a manner that adequately identifies the customer, or visiting the individual at his or her place of business or home. It could also include sending a letter to the individual, if combined with additional methods for verifying identification in a manner that adequately identifies the customer.

[23] It should be noted that while some customers may be considered low risk for purposes of the CIP Rule, they may still be considered high risk as part of the firm's AML Program.

1.4 U.S. and non-U.S. Persons

The CIP Rule's information requirements differ depending on whether the firm opens an account for a U.S. person or a non-U.S. person. Unlike the Internal Revenue Service ("IRS") definitions, the CIP Rule defines a "U.S. person" as an individual who is a U.S. citizen or an entity that is established or organized under the laws of a State or the United States.[24] Conversely, individuals who are not U.S. citizens or entities that are not established or organized under the laws of a State or the United States are defined as "non-U.S. persons." Thus, an individual who resides in the U.S., but is not a U.S. citizen, is considered by the CIP Rule to be a "non-U.S. person."[25] Unlike the IRS rules, however, the CIP Rule does not require firms to distinguish among various tax and immigration categories during account opening.

2.0 Accounts for U.S. Individuals

For accounts opened by a U.S. individual, including individual retirement accounts (e.g., IRA, IRA Rollover, and Roth IRA),[26] firms must obtain certain minimum identification for each individual prior to account opening. The minimum identification is not required where an individual is excluded from the definition of either "account" (e.g., where an account is opened pursuant to an ERISA plan) or "customer" (e.g., where a person has an existing account with the firm and the firm has a reasonable belief that it knows the true identity of the customer). The minimum identification required for a U.S. individual is as follows:

1. the individual's name;
2. the individual's date of birth;
3. the individual's residential or business street address (or, if the individual has no residential or business street address, his or her Army Post Office or Fleet Post Office box number or the residential or business street address of next of kin or another contact individual)[27]; and

---

[24] "United States" is defined as the States of the United States, the District of Columbia, the Indian lands, as defined in the Indian Gaming Regulatory Act, and the Territories and Insular Possessions of the United States.

[25] *Compare* IRS definition of "United States Person" under 26 U.S.C. § 7701(a)(30)(A).

[26] In these instances, the customer is ordinarily viewed as the individual for whose benefit the account is opened, not the financial institution in whose name the account is carried (*e.g.*, where an account is opened at ABC Bank/FBO John Doe, John Doe is the individual whose identity should be verified). Nor would the definition of "customer" include any secondary beneficiaries of the account (designated as such in the event of the customer's death).

[27] For persons who live in rural areas and do not have one of these, the number on the roadside mailbox on a rural route is acceptable as an address. A rural route number is a description of the approximate area where the customer can be located. In absence of any of these, a description of the customer's physical location will suffice. *See* Banking FAQs at pg. 5, FAQ #1 of the *Information Required* section.

4. the individual's taxpayer identification number ("TIN") (e.g., social security number). In circumstances where the individual has applied for, but not yet received a TIN, the firm must, before the account is opened, confirm that such application has been filed and obtain a TIN number within a reasonable time after account opening. The firm's CIP should clearly set out the procedures for opening accounts in such circumstances.[28]

The firm must, within a reasonable period of time before or after account opening, verify the identity of the individual using some or all of the identifying information listed above. The firm must verify the identity of the customer in all circumstances, regardless of whether a TIN has been obtained. Pursuant to the CIP Rule, a firm may, utilizing a risk-based approach, use documentary methods, non-documentary methods, or a combination of these methods to verify the identity of the individual, but must address in its written CIP the specific situations when it will use the various methods of verification. In determining what methodology and verification tools it will use, the firm should consider: the types of accounts maintained, the methods of opening accounts, the types of identifying information available, the firm's size, location and customer base. The Preamble to the CIP Rule ("Preamble") references an increase in identity theft and the availability of fraudulent documents suggesting that where a firm uses documentary methods of verification, it should obtain more than one type of documentary verification, so that it has a reasonable belief that it knows the customer's true identity.

The Preamble also encourages firms to use a variety of methods to verify the identity of a customer, especially when the firm does not have the ability to examine original documents. The number and methods of verification that a firm chooses to use will depend on the firm's risk assessment and whether other factors are present that allow it to form a reasonable belief that it knows the customer's true identity. In any case, the firm's procedures must specify the methods that the firm will use, including the documents it will obtain, if any.

The Preamble also provides an illustrative list of documentary and non-documentary methods of verification that firms can use. In those situations where firms choose to use documentary methods, a firm may verify identity through, among others, the following documents: (1) a driver's license; (2) a passport; or (3) other unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard. A firm generally may rely on the authenticity of government issued identification as verification of a

---

[28] According to guidance issued by FinCEN and the bank supervisory agencies, a financial institution cannot open an account for a U.S. person that does not have a TIN, unless the customer has applied for a TIN, the financial institution has confirmed that an application was filed before the customer opened the account, and the financial institution obtains the TIN within a reasonable period of time after the account is opened. *See* Banking FAQs at pg. 5, FAQ #2 of the *Information Required* section.

customer's identity, so long as the identification creates a reasonable belief that the firm knows the true identity of the customer. However, if a document shows obvious indications of fraud, such reliance would be misplaced, and the firm must consider that factor in determining whether it can form a reasonable belief that it knows the customer's true identity.[29] Once a firm obtains and verifies the identity of a customer through a document, such as a driver's license or passport, the firm is not required to take steps to determine whether the document has been validly issued.

Firms also have the option to verify identification through, among others, the following non-documentary methods: (1) contacting the individual;[30] (2) independently verifying the individual through a consumer reporting agency or public database; (3) checking references with other financial institutions; or (4) obtaining a financial statement (*e.g.*, an account statement from another financial institution).

If a firm relies on documentary verification, the firm's procedures must address the use of non-documentary methods in the following situations: where an individual is unable to present an unexpired government issued identification document that bears a photograph or similar safeguard; where the firm is not familiar with the documents presented; where the account is opened without obtaining documents; where the customer opens the account without appearing in person at the firm; and where the firm is otherwise presented with circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documents. Additionally, as discussed below, the firm must set out procedures for responding to circumstances where the firm cannot form a reasonable belief that it knows the true identity of an individual customer.

In developing a CIP, each firm should assess the identification risks associated with its customers who are individuals to enable it to form a reasonable belief that it knows their true identities.[31] Where there are heightened risks, firms may consider additional verification methods, including additional non-documentary methods and/or requests for other verifying documentation. A firm should also

---

[29] When questions arise with the document presented, a financial institution may use other forms of identification besides government issued identification, if they enable the financial institution to form a reasonable belief that it knows the true identity of the customer, *e.g.,* an employee identification card. Given the availability of counterfeit documents, financial institutions are encouraged to obtain more than a single document. *See* Banking FAQs at pg. 6, FAQ #2 of the *Customer Verification* section.

[30] See n.22 for a discussion of possible means of contacting a customer.

[31] A firm need not establish the accuracy of every element of identifying information obtained, but should be able to form a reasonable belief that it knows the true identity of the customer based on the information obtained. *See* 68 Fed. Reg. at 25,099 (Preamble to CIP Rule for banks). *See* also Banking FAQs at pg. 6, FAQ #1 of the *Customer Verification* section.

consider its business model in determining the extent to which a particular type of customer, account type or a method of account opening is unusual. If a firm believes that, given its business model or clientele, a customer appears to be higher risk, the firm could, for example, undertake additional verification by either contacting the individual, obtaining references or a financial statement of the individual, *e.g.*, a bank statement, or by any other appropriate means that will give the firm a reasonable belief that it knows the true identity of the individual customer.

The AML Committee understands that the general practice among firms in the industry is to verify the identity of an individual through non-documentary methods, such as screening the identifying information of an individual customer through various outside vendors,[32] consumer reporting agencies, and public databases. The AML Committee recognizes that different vendors offer different services. For example, certain services may provide background data but not identity screening. Furthermore, vendors and services may not be appropriate to screen all customers. Although we have prepared a list of public databases that are helpful in connection with a firm's due diligence/CIP verification procedures, the Preamble and CIP Rule do not specify any vendor databases or specify the types of databases that would be suitable for verification. A firm should utilize a risk-based approach in determining whether to use a vendor or public database, or if appropriate both, and, if it chooses to use a vendor, which service to use in screening its individual customers. In some cases, given the availability of verifying data, this may mean only that no inconsistent information has been found with respect to the individual.[33]

2.1 Accounts for Non-U.S. Individuals

For accounts opened by an individual who is a non-U.S. person, including retirement accounts,[34] firms must obtain identification information substantially similar to that required of U.S. persons, including name, date of birth, address and an identification number. The CIP Rule recognizes, however, that for identification purposes, there is no uniform identification number that non-U.S. individuals can provide to a firm. Therefore, firms may choose among a variety of information numbers from non-U.S. individuals, including the following: a TIN, or where

---

[32] Vendors may not necessarily be able to verify newly issued TINs or entities, e.g., such as trusts. Firms should consult with individual vendors to determine the services each vendor provides.

[33] The Preamble to the CIP Rule recommends that firms analyze whether there is logical consistency between the identifying information provided by the customer, *i.e.*, name, address, TIN, date of birth.

[34] Not all retirement accounts are excluded from the definition of "account"; only accounts opened for the purpose of participating in an employee benefit plan established pursuant to ERISA are excluded. *See* n.16.

unavailable, an individual taxpayer identification number ("ITIN");[35] a passport number and country of issuance; 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. The AML Committee recommends that firms consider, where no TIN is available, obtaining and maintaining a copy of either a passport or other government-issued identification of the non-U.S. individual. *See* the SIA's website for a list of the types of available non-U.S. government-issued identification numbers.[36]

The firm must also verify the identity of the non-U.S. individual within a reasonable time before or after account opening. Each firm must also assess the risks associated with its non-U.S. individual customers in determining whether it has a reasonable belief that it knows the true identity of the non-U.S. individual. The firm has the option to verify the identity of non-U.S. individuals by either documentary or non-documentary methods, or both, as described in section 2.0. Although not required to maintain copies of documents used to verify customers, the AML Committee recommends that firms consider verifying a non-U.S. individual by reviewing and obtaining a copy of a passport or other government issued document evidencing nationality and bearing a photograph or similar safeguard, since obtaining a passport is one type of documentary verification. In using non-documentary methods, it should be noted, that databases for screening individuals are not currently as capable of verifying non-U.S. persons as U.S. persons. Accordingly, the AML Committee recommends that firms determine, prior to sending a name for verification, that a database is capable of screening non-U.S. persons.

Where the firm determines that a non-U.S. individual presents heightened risks, the AML Committee recommends that the firm consider conducting additional verification. This may include contacting the customer or conducting additional database searches or other appropriate means.[37] *See* the SIA's website for a list of websites that may be used to conduct a search of background information for individuals that are non-U.S. persons.[38]

---

[35] While the AML Committee believes that ITINs may be used as an identification number, ITINs should not be relied on for the purpose of verifying the identity of a non-U.S. person. The ITIN is designed to facilitate the collection of tax revenue, not to serve as evidence that the IRS has verified the identity of the non-U.S. person. *See* "A Report to Congress in Accordance with § 326(B) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)," Department of the Treasury (Oct. 21, 2002).

[36] The information is available at http://www.sia.com/moneyLaundering/html/related_links.html.

[37] *See* n.22 for a discussion of possible means of contacting a customer.

[38] *See* n.36.

The AML Committee recognizes that it may be difficult to distinguish between U.S. citizens and other persons residing in the United States who nevertheless possess a TIN and/or a U.S. government issued identification (*e.g.*, resident aliens). The Preamble acknowledges that under these circumstances, a firm would not need to establish that a customer is a U.S. citizen.[39] The AML Committee recommends that, in this situation, the broker-dealer should obtain from a non-U.S. person a U.S. TIN or another government-issued identification number.

2.2 Joint and Multiple Accounts

For accounts opened by two or more individuals, firms must obtain the required identification information for, and verify the identity of, each individual owner. The same procedure applies to multiple individuals who own the account. Where one individual is a U.S. and one is a non-U.S. person, the firm should follow the respective procedures for U.S. and non-U.S. individuals, as appropriate. If a new person is added to an existing account, firms should apply the same verification procedures, unless the new person already has an existing account with the firm and there is a reasonable basis to know the person's identity.[40]

2.3 Accounts for Minors and Other Similar Accounts

For minor accounts, accounts for which a guardian or custodian is named, *e.g.*, accounts opened as UGMAs, UTMAs, 529 Plans (plans established under Section 529(b) of the IRC as "qualified tuition programs"), and conservator accounts, opened by U.S. persons, firms must obtain the required identification information from the individuals opening the account in the name of the minor, and verify the identity of such individual. According to the Preamble, this generally will be the person who fills out the account opening paperwork and who provides the information to set up such an account, *i.e.*, the custodian. After a minor reaches the age of majority, firms need to verify his/her identity when he/she seeks to set up a new account because he/she has reached the age of majority.

3.0 Accounts for Entities

3.1 Established or Organized in the U.S.

For accounts, including certain non-excluded retirement accounts, opened by entities established or organized under the laws of a State or the United States ("U.S. entity"), including corporations, partnerships, sole proprietorships, limited liability companies, subsidiaries and affiliates, unless excluded under one of the

---

[39] 68 Fed. Reg. at 25,117.

[40] A financial institution may open a joint account using information about each of the accountholders obtained from one accountholder, acting on behalf of the other joint accountholders. *See* Banking FAQs at pg. 8, FAQ #1 of the *Customer Notice* section.

categories set forth in section 1.2(b), the following minimum identification information is required for each such U.S. entity prior to account opening:

1. entity name;
2. address of the entity's principal place of business, local office or other physical location; and
3. entity's employer identification number ("EIN"). Where the entity has applied for, but not yet received, an EIN, the firm must, before the account is opened, confirm that such application has been filed and obtain the EIN within a reasonable time after account opening. Before account opening, a firm may consider obtaining a copy of an application form evidencing that the customer has applied for the EIN. Although identification procedures in this instance vary from the norm, the verification procedures as set forth below should be followed. The firm's CIP should clearly set out the procedures for opening accounts in such circumstances.

As discussed in section 1.1(a), certain U.S. entities (*e.g.*, financial institutions regulated by a Federal functional regulator and certain publicly listed companies) are excluded from the CIP Rule. Because separating these excluded entities from those that are not may be difficult in certain circumstances, some firms may find it easier to screen all entities that own accounts. At a minimum, where the entity is known to be regulated by a Federal functional regulator or listed on one of the exchanges identified in section 1.1(a), the firm should document the basis for its determination that it is not necessary to confirm the status of the entity. In any event, if an entity does not qualify for an exclusion, *e.g.*, it is not a financial institution regulated by a Federal functional regulator, the firm must meet the requirements of the CIP Rule, including obtaining the minimum identification required for U.S. or non-U.S. entities, as appropriate.

Pursuant to the CIP Rule, firms must verify the identity of each entity, unless excluded, within a reasonable period of time before or after account opening based on some or all of the identification information provided. The SIA AML Committee recommends that a firm follow these procedures, regardless of product type made available to the client, *e.g.*, transactions involving foreign currency, futures, index warrants, OTC derivatives and OTC Treasury Options. A firm may use either documentary or non-documentary methods to verify the identity of the entity, or a combination of these methods, but must address the specific situations when it will use the various methods of verification. The Preamble encourages firms to use a variety of methods to verify the identity of a customer, especially when the firm does not have the ability to examine original documents. In either case, the methods that the firm will use, including the documents it will obtain, if any, should be specified in the CIP. The Preamble provides an illustrative list of documentary and non-documentary methods of verification that firms can use for entities. The Preamble encourages firms to obtain more than one type of

documentary verification in determining the entity's true identity. A firm may verify the identity of an entity through, among others, the following documents: (1) certified articles of incorporation; (2) a government-issued business license; (3) a partnership agreement; (4) a trust instrument; or (5) any other document showing the existence of the entity, such as a certificate of incorporation.

Firms also have the option to verify identification through, among others, the following non-documentary methods: (1) contacting the entity; (2) independently verifying the entity through a consumer reporting agency or public or vendor database; (3) checking references with other financial institutions; or (4) obtaining a financial statement (*e.g.*, a bank statement or a document relating to the entity's business prepared by a third party, such as an audited financial statement). Another alternative includes contacting the entity's auditor or its financial regulator to verify its existence. Where a firm cannot verify the customer's true identity using these verification methods, the firm's CIP must include procedures requiring it to obtain information about individuals with authority or control over an account.

As with individual customers, the CIP must also address situations where the firm is not familiar with the documents presented; the account is opened without obtaining documents; the customer opens the account without having an individual appear in person at the firm; and where the firm is otherwise presented with circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documents. The CIP Rule indicates that the firm should provide for non-documentary means of verification in such situations. As a general matter, however, it is not unusual for retail and institutional accounts for U.S. entities to be opened by phone, mail or other means. In these instances, the AML Committee believes that the CIP Rule does not require an individual to appear in person at the firm on behalf of the entity and that it is still appropriate for the firm to verify the identity of such U.S. entities by either documentary or non-documentary means. For example, a firm should be able to rely on documentary verification from customers (*e.g.*, certificates of incorporation), even if an individual from the entity does not appear in person to open an account.

Each firm must assess the risks associated with an entity to enable it to verify its existence. A firm should perform a risk-based assessment to determine whether additional verification is required for a particular client. Factors that might be taken into consideration include the type of business the entity is engaged in, its location, whether it is generally a well-known reputable organization, and whether the firm has any historical experience with or independent knowledge of the entity. Ultimately, a firm must determine whether it has a reasonable belief that it knows the true identity of an entity.

The AML Committee understands that practices with respect to the verification of the identification of U.S. entities vary among firms. Depending on the firm's business and the nature of its clients, some firms verify the identity of an entity

through documentary methods, while others use non-documentary means. Such different approaches are acceptable, provided they meet the goals of the CIP Rule, *i.e.*, verification of customer identity. For example, a firm may decide to verify all of its customers by obtaining documents, regardless of whether such customers are U.S., non-U.S., or excluded. In the alternative, some firms may conduct a database search first, and if the search raises questions, then obtain documents for those customers that could not be verified through the database search. If a firm determines that a particular customer or account presents higher risks, it may wish to consider both documentary and non-documentary methods.

Where non-documentary procedures are used, one practice is for firms to screen the identifying information of entities through various outside vendors or commercial information services. Because there is no readily available service that links EINs to entities, the search is conducted primarily by the entity's name. *See* available public search engines, government and industry resources on the SIA's website.[41] Other acceptable methods of non-documentary verification include reviewing news services and Internet search engines to verify that the entity exists and/or that the information it provided is consistent. In addition to the verification methods listed in the CIP Rule, a firm may wish to verify identification of certain entities by obtaining a certificate of good standing from a State regulator or where available, through a search on a State website. A firm should generally follow its own risk-based procedures, unless it finds, after assessing its vulnerabilities to money laundering, that a specific customer presents reduced or heightened risks.

3.2 Accounts for Non-U.S. Entities

The CIP Rule is also applicable to accounts, including certain non-excluded retirement accounts,[42] opened by entities that are not established or organized in the U.S. ("non-U.S. entities"). Firms must obtain the required identification information for each such entity prior to account opening, and verify the identity of each entity within a reasonable period of time before or after account opening. Such entities include all non-U.S. companies, public companies listed on a non-U.S. exchange, non-U.S. regulated entities, non-U.S. subsidiaries and affiliated companies of U.S. companies, non-U.S. banks, non-U.S. branches of U.S. banks, non-U.S. operations of certain U.S. publicly listed financial institutions, non-U.S. partnerships, non-U.S. sole proprietorships, and non-U.S. limited liability companies.

---

41 *See* n.36.

42 *See* n.34.

The CIP Rule recognizes that there is no uniform identification number that non-U.S. entities can provide to a firm.[43] Therefore, the CIP Rule allows firms to choose among a variety of information numbers from non-U.S. entities, so long as such number allows them to reasonably establish the true identity of the customer. *See* the SIA's website for the types of identification numbers that the AML Committee believes are available for use with respect to non-U.S. entities.[44] If a firm opens an account for a non-U.S. entity that does not have any identification number, the CIP Rule requires the firm to request alternative government-issued documentation certifying the existence of the business, and if available, obtain such documents within a reasonable period of time after account opening.

The firm must also verify the identity of the non-U.S. entity, and has the option to use the documentary and non-documentary methods outlined for U.S. entities in section 3.1. Firms may verify the identity of publicly listed or regulated non-U.S. entities by verifying that such entities are publicly listed or regulated. This can be done by contacting regulators in the non-U.S. countries or reviewing their websites. *See* listing of regulators with their contact information on the SIA's website.[45] Utilizing a risk-based assessment, a firm should determine whether additional verification is necessary for a non-U.S. client by taking into account the following: whether the institution is a registered financial institution based in a major regulated financial center or in a Financial Action Task Force ("FATF") member country; whether the institution is reputable; whether the institution is from a jurisdiction or country characterized as an offshore banking or secrecy haven or is designated as non-cooperative. For example, a firm may, based on its risk assessment, require more information for entities in jurisdictions determined by the firm to be high risk. The AML Committee recommends that firms consider verifying the existence of non-U.S. entities which are not publicly listed or regulated by obtaining the formation, organization or comparable documents showing the existence of the entity, or by obtaining appropriate references from a third party, such as a bank reference. If a document is in a foreign language, the AML Committee recommends that the firm have an understanding of the document in order to rely on it, including the ability to translate it.

Additionally, the AML Committee notes that if the firm determines that an entity is a non-U.S. bank, it must obtain the information required pursuant to sections 313 and 319, (*e.g.*, by obtaining a foreign bank certification) in order to

---

[43] 68 Fed. Reg. at 25,118 n. 64 (*citing* "A Report to Congress in Accordance with Section 326(b) of the USA PATRIOT Act," Department of the Treasury (Oct. 21, 2002)).

[44] *See* n.36.

[45] *See* n.36

take advantage of the safe harbor pursuant to these sections. While information obtained pursuant to these sections could be part of the identification and verification process, it is not simply enough to rely on such certifications for purposes of identification and verification.

3.3 U.S. and Non-U.S. Closely-Held Operating Entities

Accounts opened by closely-held operating entities (*i.e.*, entities with a commercial operating business, including partnerships, family partnerships, sole proprietorships, and limited liability companies) may be verified by obtaining f ormation documents (*e.g.*, a partnership agreement, certificate of incorporation). For U.S. entities, firms may obtain a certificate of good standing from a State regulator, or where available, search State websites.

If a firm cannot adequately verify the existence of the closely-held operating entity, it must conduct additional verification, such as by obtaining a partnership agreement or a business license of the entity, or additional information relating to the owners or the identity of individuals with authority or control over the entity.[46]

Similarly, if the closely-held entity is located in a high risk jurisdiction, firms should consi der whether it is appropri ate or necess ary to look through the operat ing ent ity to ident ify and ver ify the beneficial owners or control persons of the entity in accordance with procedures set forth above for individuals and entities.

3.4 U.S. and Non-U.S. Non-Operating Entities

Accounts opened by non-operating entities, either U.S. or non-U.S. personal investment vehicles ("PIVs"), may present higher risks of money laundering than accounts opened by operating entities. PIVs can include: domestic and non-U.S. offshore personal holding companies ("PHCs"), personal investment companies ("PICs"), international business corporations ("IBCs"), trusts, partnerships, limited liability companies, and special purpose vehicles ("SPVs").[47] PIVs are organized for the pu rp ose of carrying on the investment and / or tradi ng act ivity of the benefici al owners of the entity and do not operate in any commercial capacity (*i.e.*, they do not carry a trade or business). PIVs are vehicles which for various estate planning and other purposes allow the beneficial owners to conduct financial transactions in the name of the business entity, rather than in the beneficial owners' names. Firms

---

[46] *See* Banking FAQs at pgs. 10-11, FAQs #4 and #5 of the *Customer Verification* section. (A financial institution opening an account for a partnership/sole proprietorship for which there are no documents or non-documentary methods to establish their identity must undertake additional verification by obtaining information about the identity of any individual with authority or control over the partnership/sole proprietorship account to verify its identity.)

[47] This section is not intended to address UICs; *see* separate discussion in section 3.9.

may encounter difficulties in obtaining the required identification for entities such as PHCs. Where a PHC fails to provide an address of a physical location, firms must consider obtaining an alternate address, such as the residential or business address of the settlor, grantor, or beneficial owner. Given the nature of such entities and the risks that may be associated with their location or place of organization, it may be more difficult to verify the identity of such entities.[48] Accordingly, firms must consider whether it is appropriate or necessary to look through non-operating entities to identify and/or verify the beneficial owners of non-operating entities in accordance with procedures set forth above respectively for individuals and entities. For example, in some circumstances, firms may also consider identifying and verifying any control persons of the non-operating entity.[49]

3.5 U.S. and Non-U.S. Informal Groups

For accounts opened by informal groups (*i.e.*, non-legal entities) with a common interest, such as a civic club or investment club, firms must obtain the required identification information from the individual who opens the account on the group's behalf and verify the identity of such individual within a reasonable period of time before or after account opening.[50] The CIP Rule does not require firms to verify the informal group itself. However, if based on its risk assessment, a firm determines to verify the informal group, the firm could obtain the group's formation documents or other evidence of its existence, if available.

3.6 U.S. and Non-U.S. Trusts

For accounts opened by trusts, including trusts created during one's lifetime (both revocable and irrevocable) and trusts created under a will, firms must obtain the required identification information for the trust prior to account opening and verify the identity of the trust within a reasonable period of time before or after account opening. The trust is considered the "customer" for CIP purposes.[51] Therefore, firms are not required to look through a trust to verify the identities of its trustee, trustor/grantor, or beneficiaries.

---

[48] *See* "Suspicious Banking Activities, Possible Money Laundering by U.S. Corporations Formed for Russian Entities, by the United States General Accounting Office Report to the Ranking Minority Member Permanent Subcommittee on Investigations," Committee on Governmental Affairs, United States Senate (Oct. 2000) (discussing U.S. corporations which are not operating businesses that create a risk of money laundering).

[49] *See generally* "A Report To Congress in Accordance with § 356(c) of the Uniting And Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)" (Dec. 31, 2002) (discussing PHCs).

[50] Generally, the person who opens the account is the person who fills out the account opening paperwork, or who provides the information to set up an account.

[51] *See* Banking FAQs at pg. 7, FAQ #9 of the definition of Customer Section.

Depending on the circumstances and the firm's risk assessment, a firm may verify a trust by obtaining or reviewing the trust instrument or alternative instrument where recognized by state law by confirming the name and title, and existence of the trust, or the title and signature pages of the trust instrument with an acknowledgment. Because some firms may want to avoid the burden of obtaining and reviewing trust documents, they might consider verifying the identity of the trustee and obtaining a certification by the trustee as to the existence and validity of the trust. In appropriate circumstances (*e.g.*, where the trust is formed in a high risk jurisdiction), firms may also consider verifying the identity of the trustee, the settlor or any other person with control over the trust, particularly if the trust is associated with a PHC/PIV (such as where an account for a PHC is owned by a trust). Where the firm cannot obtain or review adequate documentation, it may consider contacting the trustee, checking public or vendor databases, consumer reporting agencies, and/or references, for both the trust and the trustee, as appropriate. If a trust is associated with a PHC/PIC (*e.g.*, an account for a PHC owned by a trust), the firm may consider whether it is appropriate to look through and also obtain and verify the identity of the settlor or any other person with control over the trust.

3.7 U.S. and Non-U.S. Estates

For accounts opened on behalf of estates, firms must obtain the required identification information for the estate prior to account opening and verify the identity of the estate within a reasonable period of time before or after account opening. Under the CIP Rule, a firm is not required to look through the estate to its beneficiaries and is required only to verify the identity of the estate. A firm may verify the identity of the estate by obtaining the estate documents (*e.g.*, letters of administration, letters testamentary, or the death certificate) and/or the will. In appropriate circumstances, *e.g.*, where the estate is formed in a high risk jurisdiction (*see* discussion re high risk accounts below), the firm may consider verifying the identity of the executor or administrator. If the firm cannot obtain adequate documentation or verification, it must conduct additional verification such as by contacting the executor or administrator or by checking public databases, consumer reporting agencies and/or references of the executor or administrator, and must document that additional verification.

3.8 U.S. and Non-U.S. Charitable or Other Non-Profit Organizations

For an account opened in the name of a charitable or non-profit organization (*e.g.*, educational institution, religious group, or foundation), firms must obtain the required identification information for each charitable or non-profit organization prior to account opening and verify its identity within a reasonable period of time before or after account opening. *See* the SIA's website for a listing of databases that

firms may use to verify charities.[52] The CIP Rule does not require that firms look through the charitable or non-profit organization to its beneficiaries. A firm is required to verify only the identity of the named customer, *i.e.*, the charitable or non-profit organization. Many charitable and non-profit organizations are well-known and reputable and should not be difficult to verify. However, certain charitable and non-profit organizations have been implicated in a number of terrorist investigations, and firms may therefore face higher risks when dealing with smaller or less well-known organizations. Firms should take this into account when developing their CIP procedures and, based on their risk analysis, may determine to look through the charitable or non-profit organization to ascertain the nature of the charitable giving.

3.9 U.S. and Non-U.S. Unregistered Investment Companies ("UICs")

A UIC is a company that would be an investment company under the Investment Company Act of 1940, but for the exemptions in sections 3(c)(1) and 3(c)(7) of that Act. UICs may include hedge funds, private equity funds, venture capital funds, and real estate investment trusts ("REITs"). For an account opened on behalf of a UIC, firms must obtain the required identification information for the UIC prior to account opening and verify the identity of the UIC within a reasonable period of time before or after account opening. In order to verify the identity of the UIC, a firm may obtain the formation documents, an offering memorandum, an operating agreement (*e.g.*, partnership agreement for U.S. entities or articles of association or by-laws for non-U.S. entities), and/or subscription agreements from the UIC. In addition, for U.S. entities, firms may obtain the name of the General Partner, the Management Company, the Investment Manager or Investment Adviser and/or Principals. For non-U.S. entities, firms may obtain the name of the Investment Manager or Investment Adviser and/or Members of the Board of Directors and/or Principal(s). Firms may screen these names against commercial databases or by comparison against documents (*e.g.*, driver's license). Firms would not ordinarily need to obtain the names of the limited partners or investors in the UIC. Where a UIC is acting as a PHC, a firm should follow the procedures discussed in section 3.4 above.

---

52 *See* n.36.

4.0 Timing of Verification

Firms should reasonably exercise the flexibility provided by the CIP Rule to undertake verification before or after an account is opened. The appropriate time frame may depend on various factors, such as the type of account opened, the method by which the account is opened, the type of identifying information available, the verification method used, and the location of the customer. A firm should also consider whether it has met its obligations under the OFAC sanctions programs before allowing a customer to transact business.[53]

A firm should use a risk-based approach in determining what constitutes a reasonable period of time to verify its customers. The AML Committee recommends that, in general, firms verify the identification of customers either before account opening or within a reasonable period after account opening. More time may be necessary to verify non-U.S. individuals and entities because documents from other countries may not be readily available or may require more time to review for reliability. Similarly, where an account involves certain non-U.S. persons (*e.g.*, persons who may be senior foreign political figures or persons from high risk jurisdictions), a firm may need additional time to undertake verification.[54] In situations where a firm needs additional time to undertake verification, it should consider setting restrictions on transactions in the account until such verification can be completed or requiring some higher level of management pre-approval, either of the entire account or of specific transactions such as withdrawals or funds transfers.

5.0 Omnibus Accounts

An omnibus account is generally an account for an entity (such as a mutual fund, IA or another broker-dealer) that is acting as an intermediary on behalf of multiple individuals or entities. In this situation, the firm may have little or no information about the identity of the underlying participants or beneficiaries. Consequently, in an omnibus account relationship, the firm's customer is the intermediary firm, and not the individual participants. Even if the firm has some information about a beneficial owner of assets in an omnibus account (*e.g.*, batch execution account) or a sub-account, the financial intermediary (not the beneficial owner) is considered the customer for purposes of the CIP Rule, so long as the omnibus relationship meets the criteria set forth in guidance that has been issued jointly by Treasury and the SEC.[55]

---

[53] The Preamble to the CIP Rule discusses the obligation of firms to comply with existing requirements under OFAC. *See* 68 Fed. Reg. at 25,122 n.120.

[54] Firms should be conscious of identity theft issues in drafting their CIP.

[55] Guidance from the Staff of the Department of the Treasury and the U.S. Securities and Exchange Commission, *Question and Answer Regarding the Broker-Dealer Customer Identification Program Rule* (31 C.F.R. § 103.122) (Oct. 1, 2003).

In the circumstances where a firm has some limited information about the beneficial owners, the firm may still treat the intermediary as its customer for CIP purposes so long as the following circumstances are met: (1) where the omnibus account or relationship is established by or on behalf of a financial intermediary for the purpose of executing transactions that will clear or settle at another financial institution, or the omnibus accountholder provides limited information to the broker-dealer solely for the purpose of delivering assets to the custody account of the beneficial owner at another financial institution; (2) the limited information given to the broker-dealer about the beneficial owner is used primarily to assist the financial intermediary with recordkeeping or to establish sub-accounts that hold positions for a limited duration to facilitate the transfer of assets to another financial institution; (3) all transactions in the omnibus account or sub-accounts at the broker-dealer are initiated by the financial intermediary; and (4) the beneficial owner has no direct control over the omnibus account or sub-accounts at the broker-dealer.

6.0 Reliance on Other Financial Institutions

Under a safe harbor contained in the CIP Rule, a firm may rely on another financial institution to meet some or all of its CIP obligations. Reliance is permitted if a customer is opening, or has opened, an account or has established a similar relationship with certain other financial institutions to provide or engage in services, dealings, or other financial transactions.

In order to take advantage of the CIP Rule's safe harbor, a firm must meet the following conditions when relying on the performance by another financial institution (including an affiliate) of the elements of its CIP requirements: reliance must be reasonable under the circumstances; the other financial institution must be subject to the AML Program requirement[56] and be regulated by a Federal functional regulator;[57] and the firm must enter into a contract with the other financial institution requiring the other financial institution to certify annually to the firm that: it has implemented its own AML Program and that it will implement and perform (or its agent will perform) the requirements of the CIP Rule.[58] The contract between the firm and the financial institution must clearly specify the terms of the

---

[56] IAs are not yet subject to the AML Program requirement. However, on February 10, 2005, the SEC issued an extension of its previously issued No-Action Letter allowing financial institutions to rely on IAs pursuant to section 31 C.F.R. § 103.122(b)(6) of the CIP Rule. *See* SEC's Division of Market Regulation No-Action Letter in response to the SIA's letter asking for No-Action relief; *see also* SIA's No Action Request under the Broker-Dealer CIP Rule to the SEC's Division of Market Regulation (Jan. 6, 2004).

[57] *See* discussion in section 1.2 relating to the definition of "Federal functional regulator."

[58] When a financial institution relies on another financial institution to perform its CIP, the relied-upon institution does not have to duplicate the procedures of the relying financial institution's CIP. *See* Banking FAQs at pg. 9, FAQ #1 of the *Reliance* section.

reliance and affirm that the other financial institution's performance of those terms complies with the CIP Rule. The firm will not be responsible for the failure of the other financial institution to fulfill its obligations, so long as the firm's reliance is reasonable and it has obtained the necessary contract and certification. However, where the firm fails to satisfy the conditions for reliance, the firm will be fully responsible for satisfying its CIP.

Thus, for example, in a clearing firm relationship, a clearing broker may rely on an introducing broker with respect to shared accounts. Likewise in a prime brokerage arrangement, prime brokers and executing brokers that share accounts may rely on one another with respect to the CIP requirements. A firm's CIP must specify when the firm will rely on the performance of another financial institution, including an affiliate, of any elements of the firm's CIP obligations.

6.1 Use of Other Financial Institutions, Third-Parties or Service Providers Without Safe Harbor Protection

The safe harbor provision does not preclude firms from delegating part or all of their CIP functions to U.S. financial institutions not subject to the AML Program requirement or not supervised by a Federal functional regulator, or to non-U.S. financial institutions. Firms may also contractually delegate the implementation and operation of their CIPs to U.S. or non-U.S. service providers or other third-party, regardless of whether the entity satisfies the reliance elements outlined above. For example, a firm may delegate to a transfer agent, an outside commercial vendor, or a non-U.S. affiliated entity.

However, in such circumstances, the firm cannot take advantage of the safe harbor protection provided in the CIP Rule, and remains solely responsible for applying its own CIP to each customer in accordance with the rule. Thus, while delegation to entities that do not meet the requirements of the safe harbor is generally permissible, the broker-dealer will remain ultimately responsible for assuring compliance with the CIP Rule. In general, the AML Committee recommends that such delegation be risk-based and that firms follow the same procedures outlined above for U.S. financial institutions that qualify for the safe harbor, *i.e.*, determining that it is reasonable to do so, and obtaining a contract and certification containing representations similar to those from a U.S. entity qualifying for the safe harbor. Firms should also consider requiring non-U.S. financial institutions or non-regulated entities to agree to produce documentation promptly upon request by federal examiners, SROs, or by the firm.

7.0 Higher Risk Accounts

Certain accounts, such as accounts opened by certain types of non-U.S. persons or entities or accounts with addresses in high risk locations, depending on the nature of the firm's business, may present a higher risk of money laundering or

terrorist financing. In such situations, the firm should carefully assess the risks associated with a particular account or customer by, for example, assessing its business model and its vulnerabilities to money laundering and terrorist financing, in addition to the information it has about the customer, to determine whether it has a reasonable belief that it knows the true identity of the customer. Where the firm does not have a reasonable belief that it knows the true identity of the customer, the firm must conduct additional verification, by utilizing documentary and/or non-documentary means, such as by contacting the customer, conducting an additional database search, or looking through an entity to verify the principals or beneficiaries of the entity and/or obtaining representations from such persons concerning its activities and/or its client base.[59] Certain non-U.S. entities such as non-U.S. charitable organizations or foreign banks operating under an offshore banking license[60] may present a heightened risk of money laundering and terrorist financing. The firm may wish to consider requiring higher-level management and, in some situations, compliance department pre-approval for those accounts which it views as presenting the highest risks of money laundering or terrorist financing.

Moreover, a firm's CIP must incorporate procedures for scrutinizing accounts opened for customers originating from or located in certain high risk jurisdictions. High risk jurisdictions include those designated by the U.S. government as higher risk, *i.e.*, by FinCEN through its Advisories or its special measures pursuant to section 311 of the PATRIOT Act, or by international organizations such as FATF through its designation of non-cooperative countries and territories or by the firm itself based on its own risk assessment. A firm should assess the risks inherent in these jurisdictions and determine whether additional verification is necessary for a customer from one of these jurisdictions. A firm also needs to determine whether documents presented by a customer from a specific high risk jurisdiction are reliable for verification purposes.

8.0 Relationships Other Than Traditional Brokerage Accounts

As the definition of an "account" includes any "formal relationship with a broker-dealer established to effect transactions in securities," the CIP Rule applies to various types of relationships beyond the traditional brokerage accounts. The AML Committee recognizes that firms enter into various relationships with their

---

[59] *See* n.22 for a discussion of possible means of contacting a customer.

[60] An offshore banking license is defined under section 312 of the PATRIOT Act as a license to conduct banking activities that prohibits the licensed entity from conducting banking activities with the citizens of, or in the local currency of, the jurisdiction that issued the license.

customers that are not traditionally viewed or considered "accounts," including through various transactions with institutional parties that are in the nature of counterparty transactions and through the provision of certain investment banking and other capital market services. These appear to be within the CIP definition of "account."

In addition, certain transactions between financial institutions that arise out of a contractual relationship, *e.g.*, structured notes, swaps, principal investments and private placements, would also fall under the broader CIP Rule definition of "account." A firm may sell structured notes, Treasuries or private placements directly to another institution or private client without opening an account. Where these transactions take place in an account or securities are carried in an account, the firm's CIP directed to its traditional brokerage accounts should capture those transactions. To the extent they are not, however, the firm must adopt CIP procedures specifically applicable to these types of transactions. Regardless of whether such transactions are conducted within or outside of the account, the firm must verify the customer in accordance with the procedures set out for the entities above, as appropriate.

8.1 Counterparty Relationships

Counterparty relationships are "accounts" for CIP purposes. However, in counterparty relationships, the counterparty is oftentimes an entity that is excluded from the definition of "customer," such as a broker-dealer or a bank that is regulated by a Federal functional regulator or state bank regulator, or a U.S. publicly listed company. Therefore, as a practical matter, the CIP requirements may not apply to most of a broker-dealer's counterparty relationships. Examples of such counterparty transactions include: stock loan borrowings, transactions in Treasuries, derivatives, forex, and commodities done through broker-dealers. However, firms also deal with U.S. and non-U.S. counterparties which are not excluded from the CIP.

Where a counterparty is not excluded from the CIP Rule, the firm must obtain identification information and verify the identity of the counterparty as outlined above. Firms should keep in mind that information must be obtained prior to establishing a formal relationship with the counterparty and verification must be performed within a reasonable time before or after entering into the relationship. Where a non-U.S. counterparty presents higher risk of money laundering or terrorist financing (*e.g.*, due to its location in a high risk jurisdiction), the firm must consider conducting additional verification such as by requiring additional documentation, conducting additional database searches, and/or contacting the counterparty at his or her place of business (*e.g.*, calling the customer,[61] or having the customer visit the firm, where possible).

[61] *See* n.22 for a discussion of possible means of contacting a customer.

8.2 Capital Markets Services

Because of the CIP Rule's broad definition of "account," firms that provide services relating to mergers and acquisitions, underwriting services for initial public offerings and secondary offerings, and other advisory services involving such securities transactions through the firm must address such activities in their CIP. While in such circumstances a firm will most likely be dealing with an excluded entity, *i.e.*, one that is regulated by a Federal functional regulator or that is a U.S. public company, the firm nevertheless should determine whether the entity is excluded from the CIP Rule. For entities that are not excluded, including non-U.S. entities, the firm must comply with the CIP requirements outlined above. In most cases, firms have been verifying such clients through normal due diligence procedures (*e.g.*, by obtaining corporate governance documents, financial statements, proof of regulation/public listing, and/or meeting the client in person). Such firms may satisfy their CIP obligations through these existing practices.

9.0 Other Requirements Under the CIP

9.1 Lack of Verification

Pursuant to the CIP Rule, the CIP must include procedures for responding to circumstances in which the firm cannot form a reasonable belief that it knows the true identity of the customer, including procedures for when the firm will not open an account or when it should close an account. The AML Committee recognizes that it may sometimes be difficult to close an account or to block assets, *e.g.*, where an account has illiquid positions. However, each firm's CIP should specify the circumstances under which a firm will take steps to close an account. The CIP should also outline the terms under which a customer may conduct transactions while the firm verifies the customer's identity, where applicable. When a firm cannot verify the customer's true identity after using standard documentary and non-documentary methods, it need not undertake additional verification if it chooses not to open an account.

Finally, the firm's CIP should describe when it will file a suspicious activity report. Where there is activity (or attempted activity) of $5,000 or more and suspicions arise as to the identity of a customer or the firm discovers negative information about such customer, firms should consider whether a SAR should be filed. A firm should file a SAR in accordance with its procedures pursuant to section 356 of the PATRIOT Act.

9.2 Comparison with Government Lists

Under the CIP Rule, the CIP must include procedures for determining whether a customer appears on any list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and which has been specifically designated as a 326 list by Treasury in consultation with the Federal functional regulators. The determination must take place within a reasonable period of time after the account is opened, or earlier if required by another federal law, regulation, or federal directive. Firms will not have an affirmative duty to seek out lists of known or suspected terrorists or terrorist organizations compiled by the federal government, but will receive notification through separate guidance regarding the lists they must consult. It is the AML Committee's understanding that the lists covered by the CIP Rule are separate from those issued by OFAC and that firms remain separately subject to compliance with all applicable requirements under OFAC.

9.3 Customer Notice

Under the CIP Rule, a firm's CIP must include procedures for notifying customers that the firm is requesting information to verify their identities.[62] The notice requirement will be satisfied if the firm provides notice "in a manner reasonably designed to ensure that a customer views the notice, or is otherwise given notice, before opening an account." Depending on the manner in which the account is opened, a firm can post notice in the lobby, on its website, include the notice on its account applications, or use any other form of oral or written notice. A firm may use the sample language provided in the final regulations.[63]

Firms should consider providing their institutional clients with notice by any of several alternative means, such as by putting the notice on the firm's website, including it in standard agreements, or on other documents, including confirms, which customarily are provided to clients at the outset of the relationship or at the time of the initial transaction.

---

[62] Notice must be provided to all owners of a joint account. A financial institution may satisfy the requirement by directly providing the notice to any one accountholder of a joint account for delivery to the other owners of the account. *See* Banking FAQs at pg. 8, FAQ #1 of the *Customer Notice* section.

[63] The CIP Rule provides the following sample language:

"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."

See also the NASD's CIP Notice at http://www.nasdr.com/pdf-text/2003_cip_notice.pdf.

9.4 Retention of Records

Under the CIP Rule, a firm must make a record of the identifying information obtained for each customer and a description of the documents the firm used for verification purposes, including the type of document, any identification number contained in the document, the place of issuance and the date of issuance and expiration date, if applicable.[64] The firm is not required to retain the actual documents used to verify the customer, just a record of such documents, although Treasury has noted that firms may want to retain photocopies of identification documents in instances where risk factors are present, so long as such retention is consistent with any applicable laws.[65] If the firm uses non-documentary methods of verification, the firm must record a description of the methods used and the results of any verification measures.[66] The firm must also record the resolution of any substantive discrepancies found during the verification process, excluding minor discrepancies such as typographical mistakes.

Each firm must retain the records relating to the identification of the customer for five years after the account is closed,[67] and the records verifying the identity of the customer for five years after the record is made.[68] In all other respects, the records must be maintained pursuant to the SEC's books and records rules (17 C.F.R. § 240.17a-4). A firm may use electronic records as permitted under Rule 17a-4(f).

9.5 Approval of the CIP

Under the CIP Rule, the firm must incorporate the CIP into its overall AML Program. The AML Program must also be approved in writing by a member of the firm's senior management pursuant to NASD Rule 3011 and NYSE Rule 445. Because the CIP would be a material change to the AML Program, a firm must also obtain approval in writing of the CIP pursuant to these SRO rules.

---

[64] If a financial institution requires a customer to provide more identifying information than the minimum during the account opening process, it must maintain such additional information. *See* Banking FAQs at pg. 8, FAQ #2 of the *Retention of Records* section.

[65] *See* Department of Treasury's *Notice of Inquiry*, 68 Fed. Reg. 39,039 (July 1, 2003). Although copies are not required, a financial institution may keep copies of identifying documents that it uses to verify a customer's identity, in addition to the description that is required under the record-keeping requirement. *See* Banking FAQs at pg. 7, FAQ #2 of the *Required Records* section.

[66] It is acceptable to retain a description of the non-documentary customer verification method used in a general policy or procedure instead of recording the fact that a particular method was used on each individual customer's record, provided that the record cross-references the specific provision of the risk-based procedures contained in the financial institution's CIP used to verify the customer's identity. *See* Banking FAQs at pg. 7, FAQ #1 of the *Required Records* section.

[67] If several accounts are opened for a customer simultaneously, all identifying information about a customer obtained must be retained for 5 years after the last account is closed. *See* Banking FAQs at pg. 8, FAQ #3 of the *Retention of Records* section.

[68] The original information obtained at the time of account opening must be retained. The financial institution cannot satisfy the recordkeeping requirement simply by keeping updated information about the customer, i.e., the customer's current address.

Securities Industry Association

120 Broadway - 35 Fl. • New York, NY 10271-0080 • (212) 608-1500, Fax (212) 968-0703

1401 Eye Street, NW • Washington, DC 20005-2225 • (202) 296-9410, Fax (202) 296-9775

www.sia.com, info@sia.com