



NASD Manual | Notices to Members | Rule Filings | Member Alerts | Publications & Guidance | Issue Center | Compliance Tools



Search

Anti-Money Laundering

[Advertising](#)
[Anti-Money Laundering](#)
[Books and Records Amendments](#)
[Breakpoints](#)
[Business Continuity Planning](#)
[College Savings Plans](#)
[Mutual Funds](#)
[Research Analyst Rules](#)
[Securities Futures](#)
[Variable Annuities](#)

[Home](#) > [Rules & Regulations](#) > [Issue Center](#) > [Anti-Money Laundering](#)

Printer-Friendly
 Last Updated: 3/3/04



Anti-Money Laundering Frequently Asked Questions

General

1. Are all broker/dealers subject to the PATRIOT Act?

Yes. The PATRIOT Act applies to all broker/dealers. There are no exceptions. Firms should recognize, however, that AML compliance programs can and should be tailored to fit their businesses, considering factors such as size, location, business activities, the types of accounts they maintain, and the types of transactions in which their customers engage.

2. What is an AML Compliance Program required to have?

The PATRIOT Act required all financial institutions, including broker/dealers, to develop and implement AML compliance programs on or before April 24, 2002. Both NASD and the New York Stock Exchange ("NYSE") have anti-money laundering rules-Rule 3011 and Rule 445, respectively.

NASD Rule 3011 sets forth minimum standards for broker/dealers' AML compliance programs. It requires firms to develop and implement a written AML compliance program. The program has to be approved in writing by a member of senior management and be reasonably designed to achieve and monitor the member's ongoing compliance with the requirements of the Bank Secrecy Act and the implementing regulations promulgated thereunder.

Consistent with the PATRIOT Act, NASD Rule 3011 also requires firms, at a minimum, to:

- establish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of suspicious transactions;
- establish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the Bank Secrecy Act and implementing regulations;
- provide for independent testing for compliance to be conducted by member personnel or by a qualified outside party;
- designate and identify to NASD (by name, title, mailing address, e-mail address, telephone number, and facsimile number) an individual or individuals responsible for implementing and monitoring the day-to-day operations and internal controls of the program and provide prompt notification to NASD regarding any change in such designation(s); and
- provide ongoing training for appropriate personnel.

(See [NASD Rule 3011](#), [NASD Notice to Members 02-21](#), [NASD Notice to Members 02-47](#), [NASD Notice to Members 02-78](#), [NASD Notice to Members 02-80](#); [NASD Notice to Members 03-34](#).)

3. Does the AML compliance officer have to be a registered principal?

Neither the PATRIOT Act nor NASD Rule 3011 require AML Compliance Officers to register either as representatives or principals. Nevertheless, the

NASD's general registration requirements state that persons who engage in the investment banking or securities business for a member need to register. The NASD rules clarify that the activities triggering registration include the functions of supervision, solicitation, or conduct of business in securities, or the training of persons associated with a member for any of these functions. Thus, instructing registered persons on the use of suspicious activity reports would not alone trigger registration requirements, but instructing registered persons on particular securities products could trigger registration requirements. Firms should carefully review NASD Rules 1021 and 1031 and consider the activities conducted by the AML Compliance Officer in determining whether he or she must register.

Please note that while the AML compliance officer is not required to be a registered person as a result of serving that function, NASD anticipates that most AML compliance officers will be registered persons. Whether or not an AML compliance officer is registered with, or an employee of, the firm, an AML compliance officer is an associated person of the firm.

(See [NASD Notice to Members 02-80](#), fn. 5.)

4. Does NASD Rule 3011 require that firms designate an individual responsible for anti-money laundering compliance?

Yes, NASD Rule 3011 requires that each member designate an individual (or individuals) responsible for implementing and monitoring the day-to-day operations of the firm's AML compliance program. NASD amended Rule 3011 to require that members provide to NASD contact information concerning the members' designated AML compliance person(s). (See Question 5 below.) The information will be used by Treasury in connection with its regulatory obligations set forth in Section 314(a) of the PATRIOT Act and Treasury's information sharing rule.

(See [NASD Notice to Members 02-78](#).)

5. What do members have to provide?

Members are required to provide to NASD the name, title, mailing address, e-mail address, telephone number, and facsimile number of the contact person. Members also will be required to promptly notify NASD of any changes to the information. In addition, NASD anticipates requiring members periodically to review and confirm the accuracy of the contact information. Additional information about this will be provided in the future.

6. How should this information be provided to NASD?

NASD is collecting the contact information through the NASD Contact System (NCS) available on the NASD Web site.

7. Where is the NASD Contact System (NCS)?

Please visit the [NASD Contact System](#) foyer page for access information and further details.

Suspicious Activity Reporting Requirement

8. What is the suspicious activity reporting or "SAR" requirement?

Section 356 of Title III of the PATRIOT Act required the Treasury, in consultation with the SEC and the Board of Governors of the Federal Reserve System, to issue rules requiring broker/dealers to file suspicious activity reports or "SARs" with the Financial Crimes Enforcement Network ("FinCEN"), a bureau of Treasury. On July 1, 2002, Treasury published in the Federal Register its final rule requiring broker/dealers in securities to file reports that identify and describe transactions that raise suspicions of illegal activity. The requirement to file SARs applies to transactions occurring after December 30, 2002. SARs will have to be filed on a specific form called a Form SAR-SF (discussed in Question 13 below).

(See [NASD Notice to Members 02-47](#).)

9. What are the specific requirements for filing SARs?

The final rule requires broker/dealers to report to FinCEN any transaction that, alone or in the aggregate, involves at least \$5,000 in funds or other assets, if the broker/dealer knows, suspects, or has reason to suspect that it falls within one of four classes:

- the transaction involves funds derived from illegal activity or is intended or conducted to hide or disguise funds or assets derived from illegal activity;
- the transaction is designed, whether through structuring or other means, to evade the requirements of the Bank Secrecy Act;
- the transaction appears to serve no business or apparent lawful purpose or is not the sort of transaction in which the particular customer would be expected to engage and for which the broker/dealer knows of no reasonable explanation after examining the available facts; or
- the transaction involves the use of the broker/dealer to facilitate criminal activity.

(See [NASD Notice to Members 02-47](#).)

10. Is the SAR reporting requirement limited to individual transactions?

No. FinCEN's rule extends to patterns of transactions. In its release adopting the final rule, FinCEN explicitly clarifies that "if a broker/dealer determines that a series of transactions that would not independently trigger the suspicion of the broker/dealer, but that taken together, form a suspicious pattern of activity, the broker/dealer must file a suspicious transaction report."

(See [NASD Notice to Members 02-47](#).)

11. How does a firm determine what is a "suspicious activity"?

The release adopting FinCEN's final rule states that broker/dealers should determine whether activities vary substantially from normal practice as to raise suspicions of possible illegality by looking for "red flags" such as those enumerated in [NASD Notice to Members 02-21](#).

12. Are there any exceptions from the SAR reporting requirement?

Yes. The rule contains three exceptions from reporting violations otherwise reported to various law enforcement authorities. They are:

- a robbery or burglary that is reported by the broker/dealer to appropriate law enforcement authorities;
- lost, missing, counterfeit, or stolen securities that are reported by the broker/dealer pursuant to Rule 17f-1 under the Securities Exchange Act of 1934; and
- a violation of the federal securities laws or rules of a self-regulatory organization by the broker/dealer, its officers, directors, employees, or registered representatives, that is reported appropriately to the SEC or a self-regulatory organization ("SRO"), except for a violation of Rule 17a-8 under the Securities Exchange Act of 1934, which must be reported on Form SAR-SF.

(See [NASD Notice to Members 02-47](#).)

13. What is a Form SAR-SF?

Form SAR-SF is the form that broker/dealers must use to report suspicious activity. Treasury has also made the form applicable to futures commission merchants or "FCMs" registered with the Commodity Futures Trading Commission.

14. Who has to file Form SAR-SFs?

Each broker/dealer involved in a transaction has an independent obligation to monitor for, identify and report suspicious activities.

Customer Identification and Verification**15. What are the requirements for customer identification and verification?**

Section 326 provided that Treasury and SEC issue a rule that, at a minimum, requires broker/dealers 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; and (3) determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to brokers or dealers by any government agency. The final rule requires each broker/dealer to establish a written Customer Identification Program ("CIP") to verify the identity of each customer who opens an account. The written CIP must also include recordkeeping procedures and procedures for providing customers with notice that the broker/dealer is requesting information to verify their identity.

[\(See NASD Notice to Members 03-34.\)](#)

16. Who is a "customer" for purposes of the final rule?

The final rule defines "customer" as: (a) a person that opens a new account; and (b) an individual who opens a new account for an individual who lacks legal capacity or for an entity that is not a legal person.

Under this definition, "customer" does not refer to persons who fill out account opening paperwork or who provide information necessary to set up an account, if such persons are not the accountholder as well.

17. What happens if the customer is a trust or omnibus account?

A broker/dealer is not required to look through a trust or similar account to its beneficiaries, and is required only to verify the identity of the named accountholder.

Similarly, with respect to an omnibus account established by an intermediary, a broker/dealer is not required to look through the intermediary to the underlying beneficial owners, if the intermediary is identified as the accountholder.

18. Is there a requirement to identify those with trading authority over an account?

The final rule does not include persons with trading authority over accounts in the definition of "customer." Accordingly, the broker/dealer does not have to verify those individuals' identities. However, the final rule recognizes that situations may arise where a broker/dealer will have to take extra steps to verify the identity of those with trading authority. In these instances, a CIP is required to address situations where the broker/dealer will take additional steps to verify the identity of a customer that is not an individual by seeking information about individuals with authority or control over the account in order to verify the customer's identity.

19. Are there any other exclusions from the definition of "customer?"

The final rule's definition contains the following additional exclusions:

- A person that has an existing account with the broker/dealer, provided the broker/dealer has a reasonable belief that it knows the true identity of the person;
- A financial institution regulated by a Federal functional regulator (defined in Number 20);

- Banks regulated by a state bank regulator;
- A department or agency of the United States, of any State, or of any political subdivision of any State;
- Any entity established under the laws of the United States, of any state, or of any political subdivision of any state, or under an interstate compact between two or more states, that exercises governmental authority on behalf of the United States or any such state or political subdivision; or
- Any entity, other than a bank, whose common stock or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange 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), provided that, for purposes of this provision, a person that is a financial institution, other than a bank, is an exempt person only to the extent of its domestic operations.

(See [NASD Notice to Members 03-34](#).)

20. What is a federal functional regulator?

"Federal functional regulator" is defined as: the SEC; the Commodity Futures Trading Commission; the Board of Governors of the Federal Reserve System; the Office of the Comptroller of the Currency; the Board of Directors of the Federal Deposit Insurance Corporation; the Office of Thrift Supervision; and the National Credit Union Administration.

21. How is "account" defined in the final rule?

The final 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, securities loaned and borrowed activity, and the holding of securities or other assets for safekeeping or as collateral.

Importantly, the final rule contains two exclusions from the definition of "account." The definition excludes: (a) an account that the broker/dealer acquires through any acquisition, merger, purchase of assets, or assumption of liabilities; and (b) an account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974 ("ERISA").

The Adopting Release explains that in acquisitions, mergers, purchases of assets, or assumptions of liabilities, customers do not initiate these transfers and, therefore, the accounts do not fall within the scope of Section 326 of the PATRIOT Act.

In addition, transfers of accounts that result from an introducing broker/dealer changing its clearing firm would fall within this exclusion.

As initially proposed, the definition of "account" contained several examples of types of accounts that would be covered including cash accounts, margin accounts, prime brokerage accounts, and accounts established to engage in securities repurchase transactions. The Adopting Release notes that these types of accounts remain "accounts" for purposes of the final rule, but the final rule does not specifically include them as examples to clarify that the list is not exhaustive.

(See [NASD Notice to Members 03-34](#).)

22. What are the general requirements for a broker/dealer's written CIP?

The final rule requires that broker/dealers establish, document, and maintain a

written CIP. This program must be appropriate for the firm's size and business, be part of the firm's anti-money laundering compliance program, and, at a minimum, must contain procedures for the following: identity verification, recordkeeping, comparison with government lists, and providing customer notice.

[\(See NASD Notice to Members 03-34.\)](#)

23. What kinds of identifying information will be required of customers?

A broker/dealer's CIP must specify the identifying information that will be obtained from each customer and must contain procedures for obtaining this identifying information. At a minimum, the following information must be obtained from a customer prior to opening an account:

- A name;
- A date of birth, for an individual;
- An address, which will be:
 - For an individual, a residential or business street address;
 - For an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential or business street address of a next of kin or another contact individual; or
 - For a person other than an individual (such as a corporation, partnership or trust), a principal place of business, local office or other physical location; and
- An identification number, which will be:
 - For a U.S. person, a taxpayer identification number; or
 - For a non-U.S. person, one or more of the following: a taxpayer identification number, 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.

[\(See NASD Notice to Members 03-34.\)](#)

24. With regard to the required basic identification information that must be obtained, are there any exceptions?

There is an exception for persons who have applied for, but not received, a taxpayer identification number. Instead of obtaining a taxpayer identification number from a customer prior to opening an account, a CIP may include procedures for opening an account for a customer that has applied for, but has not received, a taxpayer identification number. In this case, the CIP must include procedures to confirm that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.

25. Is it appropriate to rely on the fact that a potential customer is a personal acquaintance of a registered representative to meet identity verification obligations?

No. The Adopting Release states that it would be inappropriate to provide special treatment to personal acquaintances. In addition, the Adopting Release notes that the rule is sufficiently flexible to make identity verification for personal acquaintances as unobtrusive as possible.

26. What procedures must a firm have for verifying customers' identities?

The final rule requires that a CIP contain procedures for verifying the identity of each customer, to the extent reasonable and practicable, using the required

identification information described above. The procedures must enable the firm to form a reasonable belief that it knows the true identity of each customer. The verification must be done within a reasonable time before or after the customer's account is opened and may be accomplished through documentary methods, non-documentary methods, or a combination of both. The procedures must describe when the firm will use these different methods.

(See [NASD Notice to Members 03-34](#).)

27. What is a "reasonable time"?

The term "reasonable time" is not defined by the final rule. The Adopting Release emphasizes that broker/dealers must reasonably exercise the flexibility to undertake verification before or after an account is opened. The amount of time may depend on various factors, which are part of a firm's risk assessment.

28. How does risk assessment fit into a firm's CIP?

The appropriate procedures for the verification aspect of a CIP are governed by a risk-based assessment. A CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. The procedures must be based on the broker/dealer's assessment of the relevant risks, including those presented by the various types of accounts maintained by the broker/dealer, the various methods of opening accounts, the various types of identifying information available and the broker/dealer's size, location and customer base.

Treasury and the SEC recommend that firms analyze whether there is a logical consistency between the identifying information provided, such as the customer's name, street address, zip code, telephone number (if provided), date of birth, and Social Security number (e.g., zip code and city/state are consistent).

29. How is verification accomplished through documents?

The final rule requires that a CIP contain procedures that, if the broker/dealer is using documentary means for verification, describe the documents the broker/dealer will use for verification. Each broker/dealer must conduct its own risk-based analysis of the types of documents that it believes will enable it to verify the true identities of customers. Examples of documents that firms may use for verification include:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For a person other than an individual (such as a corporation, partnership, or trust), documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or a trust instrument.

These documents are merely examples of reliable documents. A firm may use other documents for verification provided that the documents allow a firm to establish a reasonable belief that it knows the true identity of the customer.

The Adopting Release encourages firms to obtain more than one type of documentary verification. This will increase the likelihood of finding inconsistencies if a person is attempting to provide false information. Also the Adopting Release suggests that firms should use a variety of methods to verify the identity of a customer, especially when the broker/dealer does not have the ability to examine the original documents.

The final rule generally does not require a firm to ensure the validity of documents. The Adopting Release explains that, once a firm obtains and verifies the identity of a customer through a document, such as a driver's license or passport, a firm is not required to take steps to determine whether the document has been validly issued. A firm may rely on a government-issued identification as verification of a customer's identity. If, however, a firm

notes that the document shows some obvious form of fraud, the firm must consider that factor in determining whether it can form a reasonable belief that it knows the customer's true identity.

([See NASD Notice to Members 03-34.](#))

30. How is verification accomplished through non-documentary means?

If a firm is using non-documentary methods of verification, the final rule requires a firm's CIP to contain procedures that describe those non-documentary methods. Examples of non-documentary methods of verification include:

- Contacting a customer;
- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
- Checking references with other financial institutions; or
- Obtaining a financial statement.

([See NASD Notice to Members 03-34.](#))

31. Are there situations where it may be appropriate to use non-documentary means of verification?

The broker/dealer's procedures must address the following situations when non-documentary methods may be used:

- An individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard;
- The broker/dealer is not familiar with the documents presented;
- The account is opened without obtaining documents;
- The customer opens the account without appearing in person at the broker/dealer; and
- Where the broker/dealer is otherwise presented with circumstances that increase the risk that the broker/dealer will be unable to verify the true identity of a customer through documents.

Due to the prevalence of identity theft and because identification documents may be obtained illegally and be fraudulent, firms are encouraged to use non-documentary methods even when a customer has provided identification documents.

([See NASD Notice to Members 03-34.](#))

32. Are there situations where firms may need to implement additional verification steps?

Treasury and the SEC added a new provision to the final rule regarding additional verification for certain customers. The Adopting Release explains that, while firms may be able to verify the majority of customers adequately through documentary and non-documentary methods, there may be instances where those methods are inadequate. The risk that a firm may not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership, or trust that is created or conducts substantial business in a jurisdiction that has been designated by the U.S. as a primary money laundering concern or has been designated as non-cooperative by an international body. Treasury and the SEC emphasize that a firm must take further steps to identify customers that pose a heightened risk of not being properly identified. A firm's CIP must

prescribe additional measures that may be used to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient.

Therefore, the final rule requires that a CIP address situations where, based on the broker/dealer's risk assessment of a new account opened by a customer that is not an individual, the broker/dealer will obtain information about individuals with authority or control over such account. This verification method applies only when the broker/dealer cannot verify the customer's true identity using documentary and non-documentary verification methods.

(See [NASD Notice to Members 03-34](#).)

33. What should a firm do if it cannot form a reasonable belief that it knows the true identity of a customer?

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

- When the broker/dealer should not open an account;
- The terms under which a customer may conduct transactions while the broker/dealer attempts to verify the customer's identity;
- When the broker/dealer should close an account after attempts to verify a customer's identity fail; and
- When the broker/dealer should file a Suspicious Activity Report (Form SAR-SF) in accordance with applicable law and regulation.

34. What are the final rule's recordkeeping requirements?

A CIP must include procedures for making and maintaining a record of all information obtained to verify a customer's identity. At a minimum, the record must include all the identifying information gathered by the firm about a customer.

With regard to verification, a firm's records must contain a description of any document that was relied on to verify the customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and, if any, the date of issuance and expiration date. (This differs from the proposed rule, which required that firms keep copies of verification documents.)

With respect to non-documentary verification, the final rule requires that records contain a description of the methods and the results of any measures undertaken to verify the identity of a customer.

Finally, the final rule requires, with respect to any method of verification chosen, a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained

(See [NASD Notice to Members 03-34](#).)

35. How long must a firm retain customer identification records?

A broker/dealer must retain records of all of the identification information obtained from the customer for five years after the account is closed. In addition, records made about information that verifies a customer's identity only have to be retained for five years after the record is made. In all other respects, the records must be maintained pursuant to the provisions of SEC Rule 17a-4.

(See [NASD Notice to Members 03-34](#).)

36. What does the final rule require regarding the need to check government lists?

A 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 designated as such by Treasury in consultation with the Federal functional regulators. The procedures must require that the broker/dealer make such a determination within a reasonable period of time after the account is opened, or earlier if required by another Federal law or regulation or Federal directive issued in connection with the applicable list. The procedures also must require that the broker/dealer follow all Federal directives issued in connection with such lists.

The Adopting Release notes that Treasury and the Federal functional regulators have not yet designated any government lists. The Adopting Release also notes that firms do not have an affirmative duty to seek out all lists of known or suspected terrorists or terrorist organizations compiled by the federal government. Instead, firms will receive notification from the federal government regarding the lists that they must consult for purposes of this provision.

The Adopting Release also cautions that this does not mean that firms do not have obligations under other laws to screen their customer against government lists. It mentions, as an example, compliance with the Office of Foreign Assets Control ("OFAC") rules prohibiting transactions with certain foreign countries and nationals. Firms must check the OFAC List to ensure that potential customers and existing customers, on an ongoing basis, are not prohibited persons or entities and are not from embargoed countries or regions before transacting any business with them.

(See [NASD Notice to Members 03-34.](#))

37. Is there a customer notice requirement?

Yes, there is. A CIP must include procedures "for providing customers with adequate notice that the broker/dealer is requesting information to verify their identities." Notice must occur before the account is opened. Notice is adequate if the broker/dealer generally describes the identification requirements of the final rule and provides such notice in a manner reasonably designed to ensure that a customer is able to view the notice, or otherwise be given notice, before opening an account. For example, depending upon the manner in which the account is opened, a broker/dealer may post a notice in the lobby or on its Web site, include the notice on its account applications, or use any other form of oral or written notice.

The final rule provides the following sample language for notice to be provided to a firm's customers, if appropriate:

Important Information About Procedures for Opening a New Account

To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.

What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

(See [NASD Notice to Members 03-34.](#))

38. Can a firm rely on the performance by another financial institution of some or all of the elements of a firm's CIP?

The final rule acknowledges that there may be circumstances in which a firm may be able to rely on the performance by another financial institution of some or all of the elements of a firm's CIP. Therefore, the final rule provides that a CIP may include procedures specifying when the broker/dealer will rely on the performance by another financial institution (including an affiliate) of any procedures of the broker/dealer's CIP, with respect to any customer of the

broker/dealer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions.

In order for a broker/dealer to rely on another financial institution, the following requirements must be met:

- Reliance must be reasonable under the circumstances;
- The other financial institution must be subject to a rule implementing the anti-money laundering compliance program requirements of the PATRIOT Act and be regulated by a Federal functional regulator; and
- The other financial institution must enter into a contract requiring it to certify annually to the broker/dealer that it has implemented its anti-money laundering program, and that it will perform (or its agent will perform) specified requirements of the broker/dealer's CIP.

The Adopting Release notes that the contract and certification will provide a standard means for a firm to demonstrate the extent to which it is relying on another financial institution to perform its CIP, and that the other institution has agreed to perform those functions. If it is not clear from these documents, a broker/dealer must be able to otherwise demonstrate when it is relying on another financial institution to perform its CIP with respect to a particular customer. A broker/dealer will not be held responsible for the failure of the other financial institution to fulfill adequately the broker/dealer's CIP responsibilities, provided that the broker/dealer can establish that its reliance was reasonable and that it has obtained the requisite contracts and certifications. Treasury and the SEC emphasize that the broker/dealer and the other financial institution upon which it relies must satisfy all of the conditions set forth in this final rule. If they do not, then the broker/dealer remains solely responsible for applying its own CIP to each customer in accordance with the rule.

[\(See NASD Notice to Members 03-34.\)](#)

Introducing/Clearing Firms

39. How can both introducing and clearing broker/dealers establish anti-money laundering compliance programs if they play different roles with respect to the customer and have access to different types of customer or activity information?

To detect suspicious activity, introducing and clearing broker/dealers must work together to achieve compliance with the PATRIOT Act. For instance, introducing firms generally are in the best position to "know the customer," and therefore to identify potential money laundering concerns at the account opening stage, including verification of the identity of the customer and deciding whether to open an account for a customer. In essence, introducing firms should understand that they are the first line of defense in detecting and deterring suspicious activity. Clearing firms, in turn, may be in a better position to monitor customer transaction activity, including but not limited to, trading, wire transfers and the deposit and withdrawal into and out of accounts of different financial instruments. To assist introducing firms and, more importantly, satisfy their own obligations under Federal law, clearing firms should establish both automated systems allowing for the detection of suspicious activity, and procedures that include sharing AML information and responsibilities with introducing brokers, consistent with the PATRIOT Act and NASD Rule 3011.

[\(See NASD Notice to Members 02-21.\)](#)

40. Does this mean that an introducing or clearing firm would be relieved of AML obligations to the extent that the other is monitoring for suspicious activities?

No, it does not. Introducing firms must have a basis for assuring themselves that their clearing firms are monitoring customer account activity on their behalf. Similarly, clearing firms must have a basis for assuring themselves that their introducing firms are following appropriate customer identification procedures. Functions relating to AML compliance should be clearly allocated between the parties in a written document. Any allocation, however, will not relieve either party from its independent obligation to comply with AML laws.

Information Sharing

41. What are the requirements regarding information sharing?

On September 26, 2002, FinCEN issued a final rule regarding information sharing among financial institutions and federal government law enforcement agencies for the purpose of identifying, preventing, and deterring money laundering and terrorist activity. In general, a financial institution may share information with another financial institution about those suspected of terrorism or money laundering. In order to do this, financial institutions must do the following:

- A broker/dealer must submit to FinCEN an initial, and thereafter annual, notice, which can be completed online at FinCEN's Web site at www.fincen.gov. Firms must submit the notice to FinCEN prior to sharing information.
- Prior to sharing information, a broker/dealer must take reasonable steps to ensure that the other firm with which it intends to share this information has submitted the requisite notice to FinCEN. This can be done by confirming that the other firm appears on a list that FinCEN will make available on a periodic basis to firms that have filed a notice with them, or by confirming directly with the other firm that the requisite notice has been filed. A firm can obtain a copy of the other firm's notice, or by other reasonable means, including accepting the representations of the other firm that a notice was filed after the most recent list has been distributed by FinCEN
- Information received by a broker/dealer under a sharing agreement cannot be used for any other purpose other than identifying and where appropriate, reporting on money laundering or terrorist activities, determining whether to establish or maintain an account or engage in a transaction, or assisting the financial institution in complying with any requirement of the section. Firms that engage in the sharing of information will have to maintain adequate procedures to protect the security and confidentiality of that information.

(See 67 Fed. Reg. 60,579.)

42. Does this information have to be safeguarded?

Yes, integral to this requirement is the need to safeguard the confidentiality of customer information. The final rule states that its safeguarding requirements will be satisfied to the extent that a broker/dealer applies to information requests those procedures that an institution has established to satisfy the requirements of section 501 of the Gramm-Leach-Bliley Act regarding the protection of customers' nonpublic personal information. This means compliance with the privacy provisions of Regulation S-P.

43. Is there a safe harbor from liability?

Firms that share information under this section will be protected from liability for sharing the information, or for any failure to provide notice of such sharing to an individual, entity, or organization that is suspected of terrorism or money laundering. However, the safe harbor will not apply if the firm has failed to comply with the requirements set forth in the rule.

(See 67 Fed. Reg. 60,579.)

Private Banking Accounts/Correspondent Accounts

44. What are private banking accounts?

Private banking accounts are accounts, or a combination of accounts, that:

- have an aggregate deposit of funds or other assets of more than \$1 million; and
- are established on behalf of one or more individuals who have a direct or beneficial ownership in the account; and
- are assigned to, or administered by, in whole or in part, an officer, employee or agent of a financial institution, acting as a liaison between the institution and the direct or beneficial owner of the account.

45. What are correspondent accounts?

Correspondent accounts are accounts established to receive deposits from a foreign bank to make payments on behalf of that same foreign bank or to handle other financial transactions related to a foreign bank.

Under the PATRIOT Act, broker/dealers are prohibited from establishing, maintaining, administering, or managing a correspondent account in the United States for an unregulated foreign shell bank.

Treasury created certification forms that broker/dealers can send to their foreign bank account holders for completion. The certification forms generally ask the foreign banks to confirm that they are not shell banks and to provide the necessary ownership and agent information. Use of the certification forms will help firms ensure that they are complying with requirements concerning correspondent accounts with foreign banks and can provide a broker/dealer with a safe harbor for purposes of complying with such requirements.

46. What is a shell bank?

Shell banks are defined as banks with no physical presence in any country.

47. Are there special requirements for private banking and correspondent accounts?

Yes. Section 312 of the PATRIOT Act requires each U.S. financial institution that establishes, maintains, administers, or manages a private banking account or correspondent account in the United States to take certain anti-money laundering measures with respect to such accounts. In particular, financial institutions must establish appropriate, specific and where necessary, enhanced due diligence policies, procedures and controls that are reasonably designed to enable the financial institutions to detect and report instances of money laundering through those accounts.

In addition to this general requirement, which applies to all correspondent and private banking accounts for non-U.S. persons, Section 312 of the Act specifies additional standards for correspondent accounts maintained for certain foreign banks. For a correspondent account maintained for a foreign bank operating under an offshore license or a license granted by a jurisdiction designated as being of concern for money laundering, a financial institution must take reasonable steps to identify the owners of the foreign bank, to conduct enhanced scrutiny of the correspondent account to guard against money laundering, and to ascertain whether the foreign bank provides correspondent accounts to other foreign banks and, if so, to conduct appropriate related due diligence.

Section 312 also sets forth minimum standards for the due diligence requirements for a private banking account for a non-U.S. person. Specifically, a financial institution must take reasonable steps to ascertain the identity of the nominal and beneficial owners of, and the source of funds deposited into, the private banking account, as necessary to guard against money laundering. The institution must also conduct enhanced scrutiny of private banking accounts requested or maintained by or on behalf of senior foreign political figures (or their family members or close associates). Enhanced scrutiny must be reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.

48. Are these requirements final?

Treasury and FinCEN issued these requirements as an interim final rule, effective on July 23, 2002. The interim final rule temporarily defers for certain financial institutions the application of certain of these requirements. The interim final rule states that securities brokers and dealers, futures commission merchants, and introducing brokers must comply with the provisions of Section 312 relating to due diligence and enhanced due diligence for private banking accounts, but their compliance with provisions related to correspondent accounts is deferred.

(See 67 Fed. Reg. 48,347.)

AML Resources**49. Is there any service available that can help firms search for names found on the OFAC List?**

NASD offers an [OFAC search tool](#) that enables members to search for names found on the OFAC List. It is available without charge.

There are many other services commonly available offering search capabilities. Firms should also check the [Treasury's Web site](#) for more information.

50. Are there any AML resources available for small firms?

Yes. In addition to Notices to Members concerning AML, small firms can use the NASD Anti-Money Laundering Small Firm Template, the OFAC Search Tool, and various other helpful resources found on the NASD AML Web page.

51. We would like to obtain more information about anti-money laundering service providers. Can you provide us with a list of vendors?

NASD does not recommend or endorse any manufacturer, vendor, or product, nor will it receive any consideration as a result of providing the information about any such manufacturer or vendor. However, NASD is aware of several vendors that offer anti-money laundering services. They are listed below. When NASD becomes aware of other vendors that offer anti-money laundering services, they will be added to the list maintained by NASD. Note that there is no safe harbor available or created for firms that use these vendors.

AML Compliance/OFAC Compliance Tools:

[Actimize](#)
[Americas Software](#)
[Bankers Systems](#)
[Complinet](#)
[eMind](#)
[Equifax](#)
[Experian](#)
[Financial Industry Service Group](#)
[Financial Registrations, Inc.](#)
[FircoSoft](#)
[Lexis-Nexis](#)
[Mantas](#)
[McDonald Information Service](#)
[Net Economy](#)
[P.A. Compliance](#)
[Prime Associates](#)
[Protiviti](#)
[Regulatory DataCorp, International, LLC](#)
[Risk Values](#)
[RSM McGladrey, Inc.](#)
[Safe Banking Systems \(SBS\)](#)
[SAS](#)
[Search Space](#)
[STB Systems Group](#)

[Sybase Solutions](#)
[Thomson Financial](#)
[World-Check](#)

[About NASD](#) | [Press Room](#) | [Resources](#) | [Career Opportunities](#) | [FAQ](#) | [Site Map](#) | [Contact Us](#)
©2004 NASD. All rights reserved. | [Legal Notices](#) and [Privacy Policy](#).