

[Last Updated 1/23/04]

Small Firm Template

[Firm Name]

Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures

8/16/07

Please note: The Financial Crimes Enforcement Network has issued final rules to implement requirements set forth in Sections 311 and 312 of the USA PATRIOT Act, which have not yet been incorporated into the template. These rules include 31 CFR 103.176, 31 CFR 103.188, 31 CFR 103.192, and 31 CFR 103.193. This template does not reflect these recent changes.

FINRA is in the process of updating the template and will notify firms when it becomes available. In the interim, firms should carefully review these rules and update their AML programs, as appropriate. *See generally* [FinCEN's Web site](#); *see also* [FinCEN's Federal Register Web page](#) announcing relevant proposed and approved regulations.

This template is provided to small firms to assist them in fulfilling their responsibilities to establish an Anti-Money Laundering Program as required by the USA PATRIOT Act of 2001 and NASD Rule 3011. Nothing in this template creates any new requirements for AML programs, which are contained in the PATRIOT Act and the rules promulgated under it, and NASD Rule 3011. **On the other hand, following this template does not guarantee compliance with those requirements or create a safe harbor from regulatory responsibility.** There is no exemption from the rules for small broker-dealers, and they are required to follow all of the requirements of AML rules. The obligation to develop an AML plan is not a “one-size-fits-all” requirement, and you must tailor your plan to fit your particular firm's situation. This language is provided as a **helpful starting point** to walk you through developing your firm's plan. If this language does not fit your firm's business situation in any respect, you will need to prepare your own language. **You** are responsible for ensuring that your plan fits your firm's situation and that you implement your plan.

TEXT EXAMPLES are provided to give you sample language that you can modify to create your firm's plan.

Material in *italics* provides instructions, the relevant rules, and other resources that you can use to develop your firm's plan.

General guidance and background are provided by NASD Notices to Members (NtM) [02-21](#), [02-47](#), [02-50](#), [02-78](#) and [02-80](#), which provide extensive guidance on setting up Anti-Money Laundering programs and related relevant information about firms' Anti-Money Laundering obligations. You may also want to consult the [Securities Industry Association's Preliminary Guidance for Deterring Money Laundering Activity](#).

1. Firm Policy

State your firm's commitment to comply with AML rules. This policy should be given to all employees.

TEXT EXAMPLE: It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

Resources: [NtM 02-21](#), page 5; [SIA Preliminary Guidance for Deterring Money Laundering Activity](#) ("SIA Guidance"), at pages 2-3 (Feb. 2002).

2. AML Compliance Officer Designation and Duties

Designate your firm's AML Compliance Officer and describe his or her duties. See [NtM 02-21](#), pages 3-4, 13-14.

TEXT EXAMPLE: The firm designates [Name] as its Anti-Money Laundering Program Compliance Officer, with full responsibility for the firm's AML program. [Name] is qualified by experience, knowledge and training, including [describe]. The duties of the AML Compliance Officer will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees, and [Add any other duties your firm will assign to the AML Compliance Officer; review NASD Rules 1021 and 1031 for any applicable registration requirements]. The AML Compliance Officer will also ensure that proper AML records are kept. When warranted, the AML Compliance Officer [Add if appropriate: "in consultation with {Name or title}" OR "with the approval of {Name or title}"] will ensure Suspicious Activity Reports (SAR-SFs) are filed.

The firm will provide NASD with contact information for the AML Compliance Officer, including name, title, mailing address, e-mail address, telephone number and facsimile number. The firm will promptly notify NASD of any change to this information.

Rule(s): NASD Rule 3011.

Resources: [NtM 02-78](#). Firms can submit their AML Compliance Officer information through FINRA's Contact System at <http://www.finra.org/RegulatorySystems/FCS/index.htm>.

3. Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions

a. FinCEN Requests Under PATRIOT Act Section 314

Describe your firm's procedures for FinCEN requests for information on money laundering or terrorist activity. See: [NtM 02-21](#), pages 12-14, [NASD Member Alert](#) (2/14/03).

TEXT EXAMPLE: Under Treasury's final regulations (published in the Federal Register on September 26, 2002), we will respond to a Financial Crimes Enforcement Network (FinCEN) request about accounts or transactions by immediately searching our records, at our head office or at one of our branches operating in the United States, to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. Upon receiving an information request, we will designate one person to be the point of contact regarding the request and to receive similar requests in the future. Unless otherwise stated in FinCEN's request, we are required to search current accounts, accounts maintained by a named suspect during the preceding 12 months, and transactions conducted by or on behalf of or with a named subject during the preceding six months. If we find a match, we will report it to FinCEN by completing FinCEN's subject information form. This form can be sent to FinCEN by electronic mail at sys314a@fincen.treas.gov, (or if you don't have e-mail,) by facsimile transmission to 703-905-3660. If the search parameters differ from those mentioned above (for example, if FinCEN requests longer periods of time or limits the search to a geographic location), we will limit our search accordingly.

If we search our records and do not uncover a matching account or transaction, then we will not reply to a 314(a) request.

We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. We will maintain procedures to protect the security and confidentiality of requests from FinCEN, such as those established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act.

We will direct any questions we have about the request to the requesting Federal law enforcement agency as designated in the 314(a) request.

Unless otherwise stated in the information request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the request as a list for purposes of the customer identification and verification requirements. We will not use information provided to FinCEN for any purpose other than (1) to report to FinCEN as required under Section 314 of the PATRIOT Act; (2) to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist the firm in complying with any requirement of Section 314 of the PATRIOT Act.

Rules: NASD Rule 3011; Section 314 of the PATRIOT Act; 31 C.F.R. § 103.100.

Resources: www.fincen.gov/314a_announcement021203.pdf;

www.fincen.gov/314a_pressrelease02062003.pdf; NASD Member Alert (2/14/03).

b. Sharing Information With Other Financial Institutions

Treasury regulations allowing information sharing among financial institutions became effective immediately on March 4, 2002. If your firm plans to share information with other financial institutions, describe your firm's procedures for such sharing. See: [NtM 02-21](#), page 13.

TEXT EXAMPLE: We will share information about those suspected of terrorist financing and money laundering with other financial institutions for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities and to determine whether to establish or maintain an account or engage in a transaction. We will file with FinCEN an initial notice before any sharing occurs and annual notices afterwards. We will use the notice form found at www.fincen.gov. Before we share information with another financial institution, we will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. We understand that this requirement applies even with respect to financial institutions *with whom we are affiliated*, and so we will obtain the requisite notices from affiliates and follow all required procedures.

We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, including segregating it from the firm's other books and records and [*describe any other procedures*].

[If an introducing firm:] In addition to sharing information with other financial institutions about possible terrorist financing and money laundering, we will also share information about particular suspicious transactions with our clearing broker for purposes of determining whether one of us will file a SAR-SF. In cases in which we file a SAR-SF for a transaction that has been handled both by us and by the clearing broker, we may share with the clearing broker a copy of the filed SAR-SF, unless it would be inappropriate to do so under the circumstances, such as where we filed a SAR-SF concerning the clearing broker or one of its employees.

Rules: NASD Rule 3011; Section 314 of the PATRIOT Act; 31 C.F.R. §103.19; 31 C.F.R. § 103.110.

Other Resources: The notice form can be found at http://www.fincen.gov/fi_infoappb.html.

4. Checking the Office of Foreign Assets Control (“OFAC”) List

Describe how you will check the OFAC list before opening an account and for existing accounts. See [NtM 02-21](#), page 6.

TEXT EXAMPLE: Before opening an account, and on an ongoing basis, we will check to ensure that a customer does not appear on Treasury's OFAC “Specifically Designated Nationals and Blocked Persons” List (SDN List) (*See* the OFAC Web Site at www.treas.gov/ofac, which is also available through an automated search tool on www.nasdr.com/money.asp), and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC Web Site. Because the OFAC Web Site is updated frequently, we will consult the list on a regular basis and

<http://www.finra.org/index.htm>

subscribe to receive updates when they occur. We may access these lists through various software programs to ensure speed and accuracy. We will also review existing accounts against these lists when they are updated and we will document our review.

In the event that we determine a customer, or someone with or for whom the customer is transacting, is on the SDN List or is from or engaging in transactions with a person or entity located in an embargoed country or region, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC. We will also call the OFAC Hotline at 1-800-540-6322.

Other Resources: [NtM 02-21](#), page 6, n.24;

SDN List- <http://www.treas.gov/ofac/t11sdn.pdf>.

The OFAC Web site -- <http://www.treas.gov/ofac/t11facsc.pdf> -- contains checklists and information for securities firms to follow in checking the OFAC list. You can subscribe to receive updates at <http://www.treas.gov/press/email/subscribe.html>.

NASD provides a search engine to automate OFAC list searches at <http://apps.finra.org/RulesRegulation/OFAC/1/Default.aspx>

Blocked Properties Reporting Form --

<http://www.treas.gov/offices/enforcement/ofac/legal/forms/td902250.pdf>.

Voluntary Form for Reporting Blocked Transactions –

http://www.treas.gov/offices/enforcement/ofac/legal/forms/e_blockreport1.pdf.

Voluntary Form for Reporting Rejected Transactions –

http://www.treas.gov/offices/enforcement/ofac/legal/forms/e_rejectreport1.pdf.

5. Customer Identification and Verification

Firms are required to have and follow reasonable procedures to verify the identity of their customers who open new accounts. These procedures must address the types of information the firm will collect from the customer and how it will verify the customer's identity. These procedures must enable the firm to form a reasonable belief that it knows the true identity of its customers. The final rule, which Treasury and the SEC jointly issued on April 30, 2003, requires firms to be in compliance with the final rule by October 1, 2003.

The CIP must be in writing and be part of the firm's anti-money laundering compliance program. It needs the approval of senior management if it is a material change to the anti-money laundering program.

Note that this regulation applies only to "customers" who open new "accounts" with a broker/dealer. A "customer" is defined as (1) a person that opens a new account or (2) an individual who opens a new account for an individual who lacks legal capacity or for an entity that is not a legal person. ("Customer" does not refer to persons who fill out account opening paperwork or who provide information necessary to establish an account, if such persons are not the accountholder as well. The definition of "customer" also does not include persons with authority over accounts.)

The following entities, however, are excluded from the definition of "customer:" a financial institution regulated by a Federal functional regulator or a bank 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 a State that exercises governmental authority on behalf of the United States, any State, or any political subdivision of a State; 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 have been designated as a Nasdaq National Market Security listed on Nasdaq (but only to the extent of domestic operations for any such persons that are financial institutions, other than banks), and a person that has an existing account with the broker/dealer, provided that the broker/dealer has a reasonable belief that it knows the true identity of the person.

Broker/dealers will not be required to verify the identities of persons with existing accounts at the firm, as long as the broker/dealer has a reasonable belief that it knows the true identity of the customer.

For purposes of this rule, an "account" is defined 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 loan and borrow activity, and the holding of securities or other assets for safekeeping or as collateral. The following are excluded from the definition of "account:" (1) an account that the broker/dealer acquires through any acquisition, merger, purchase of assets, or assumption of liabilities, and (2) an account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974 ("ERISA").

Describe how you will identify customers and verify their identities. See: NtM 02-21-, NtM 02-50, pages 5-7; 31 C.F.R. §§103.122 et seq.

NOTE: *If your firm does not have customers, describe the internal controls that your firm will implement to detect any attempt to open accounts for customers and what actions the firm will take if such activities occur. Please note that this may be a material change in business requiring an application, review and approval by NASD. (See NASD Rule 1017.)*

TEXT EXAMPLE: In addition to the information we must collect under NASD Rules 2110 (Standards of Commercial Honor and Principles of Trade), 2310 (Recommendations to Customers - Suitability), and 3110 (Books and Records), and SEC Rules 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts) and 17a-3(a)(17) (Customer Accounts), we have established, documented, and maintained a written Customer Identification Program (or CIP). We will collect certain minimum customer identification information from each customer who opens an account; utilize risk-based measures to verify the identity of each customer who opens an account; record customer identification information and the verification methods and results; provide notice to customers that we will seek identification information and compare customer identification information with government-provided lists of suspected terrorists.

a. Required Customer Information

Prior to opening an account, we will collect the following information for all accounts, if applicable, for any person, entity or organization who is opening a new account and whose name is on the account: the name; date of birth (for an individual); an address, which will be a residential or business street address (for an individual), an Army Post Office ("APO") or Fleet Post Office ("FPO") number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business

street address), or a principal place of business, local office or other physical location (for a person other than an individual); an identification number, which will be a taxpayer identification number (for U.S. persons) or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons). In the event that a customer has applied for, but has not received, a taxpayer identification number, we will *[add 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.

When opening an account for a foreign business or enterprise that does not have an identification number, we will request alternative government-issued documentation certifying the existence of the business or enterprise.

Rules: NASD Rule 3011; Section 326 of the PATRIOT Act; 31 C.F.R. §§103.122 et seq.

b. Customers Who Refuse To Provide Information

Describe your firm's policy for customers who do not provide requested information. See [NtM 02-21](#), page 7.

TEXT EXAMPLE: If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our AML Compliance Officer will be notified so that we can determine whether we should report the situation to FinCEN (i.e., file a Form SAR-SF).

c. Verifying Information

Describe information that you will gather to verify customers' identities. The information you gather should vary according to the risks posed by the type of account. The procedures must enable you to form a reasonable belief that you know the true identity of each customer. Among the risks to consider are the various types of accounts maintained by the firm, the various methods of opening accounts provided by the firm, the various types of identifying information available, and the firm's size, location, and customer base. If you believe that some of these risk factors increase the likelihood that you will need more information to know the true identity of your customers, you should determine what additional identifying information might be necessary for a reasonable belief that you know the true identity of your customer and when such additional information should be obtained. See: [NtM 02-21](#), pages 6-7.

TEXT EXAMPLE: Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. In verifying customer identity, we will analyze any logical inconsistencies in the information we obtain.

We will verify customer identity through documentary evidence, non-documentary evidence, or both. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever possible. We may also use such non-documentary means, after using documentary evidence, if we are still uncertain about whether we know the true identity of the customer. In analyzing the verification information, we will consider whether there is a logical consistency among 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.

Appropriate documents for verifying the identity of customers include, but are not limited to, the following:

- For an individual, an unexpired government-issued identification evidencing nationality, residence, and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For a person other than an individual, 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.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

We will use the following non-documentary methods of verifying identity:

- 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.

We will use non-documentary methods of verification in the following situations: (1) when the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard; (2) when the firm is unfamiliar with the documents the customer presents for identification verification; (3) when the customer and firm do not have face-to-face contact; and (4) when there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when

we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering or terrorist financing activity, we will, after internal consultation with the firm's AML compliance officer, file a SAR-SF in accordance with applicable law and regulation.

We recognize that the risk that we 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. We will identify customers that pose a heightened risk of not being properly identified. Therefore, we will take the following 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: *[add additional procedures for verifying identity of certain customers, such as obtaining information about individuals with authority or control over such account]*.

d. Lack of Verification

Describe your procedures for responding to circumstances in which the firm cannot form a reasonable belief that it knows the true identity of a customer.

TEXT EXAMPLE: When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (A) not open an account; (B) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (C) close an account after attempts to verify customer's identity fail; and (D) file a SAR-SF in accordance with applicable law and regulation.

e. Recordkeeping

Describe your recordkeeping procedures.

TEXT EXAMPLE: We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancy in the identifying information. We will keep records containing a description of any document that we relied on to verify a 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. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will maintain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.

f. Comparison with Government Provided Lists of Terrorists and Other Criminals

Describe how you will check government lists within a reasonable period of time after opening an account (or earlier, if required by another Federal law or regulation or Federal directive issued in connection with an applicable list). See [NtM 02-21](#), page 6.

TEXT EXAMPLE: From time to time, we may receive notice that a Federal government agency has issued a list of known or suspected terrorists. Within a reasonable period of time after an account is opened (or earlier, if required by another Federal law or regulation or Federal directive issued in connection with an applicable list), we will determine whether a customer appears on any such 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. We will follow all Federal directives issued in connection with such lists.

We will continue to comply with Treasury's Office of Foreign Asset Control rules prohibiting transactions with certain foreign countries or their nationals.

Other Resources: [NtM 02-21](#), page 6, n.24; 31 C.F.R. §§ 103.122.

g. Notice to Customers

You must notify customers that you are requesting information from them to verify their identities. You may provide notice by a sign in your lobby, through other oral or written notice, or, for accounts opened online, notice posted on your Web site. No matter which methods of giving notice you chose, you must give it before an account is opened or trading authority is granted.

TEXT EXAMPLE: We will provide notice to customers that the firm is requesting information from them to verify their identities, as required by Federal law. We will use the following method to provide notice to customers: [*describe notice you will provide for each method of account-opening your firm uses (i.e., telephone, online, walk-in, etc.); 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 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.].

Rule: 31 C.F.R. §103.122(g).

h. Reliance on Another Financial Institution for Identity Verification

We may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of our customer identification program with respect to any customer 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:

- When such reliance is reasonable under the circumstances;
- When the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements of 31 U.S.C. 5318(h), and is regulated by a Federal functional regulator; and
- When the other financial institution has entered into a contract with our firm requiring it to certify annually to us that it has implemented its anti-money laundering program, and that it will perform (or its agent will perform) specified requirements of the customer identification program.

[You will not be held responsible for the failure of the other financial institution to fulfill adequately your customer identification program responsibilities, provided that you can establish that your reliance was reasonable and you have obtained the requisite contracts and certifications.]

Rule: 31 C.F.R. §§ 103.122 *et seq.*

6. Foreign Correspondent Accounts and Foreign Shell Banks

a. Detecting and Closing Correspondent Accounts of Unregulated Foreign Shell Banks

*Broker/dealers are prohibited from establishing, maintaining, administering, or managing correspondent accounts for unregulated foreign shell banks. Foreign shell banks are foreign banks without a physical presence in any country. A "foreign bank" is any bank organized under foreign law or an agency, branch or office of a bank located outside the U.S. The term does not include an agent, agency, branch or office within the U.S. of a bank organized under foreign law. A "regulated affiliate" of a foreign bank is a foreign bank that (1) is an affiliate of a depository institution, credit union, or foreign bank that maintains a physical presence in the U.S. or a foreign country **and** (2) is subject to supervision by a banking authority in the country regulating such affiliated depository institution, credit union, or foreign bank.*

The prohibition does not include foreign shell banks that are affiliates of a depository institution, credit union, or foreign bank that maintains a physical presence in the U.S. or a foreign country, and are subject to supervision by a banking authority in the country regulating that affiliated depository institution, credit union or foreign bank. Foreign branches of a U.S. broker/dealer are not subject to this requirement, and "correspondent accounts" of foreign banks that are clearly established, maintained, administered or managed only at foreign branches are not subject to this regulation.

Describe how your firm will detect and close U.S. "correspondent accounts" for unregulated foreign shell banks. See: [NtM 02-21](#), page 8.

NOTE: *If your firm does not establish, maintain, administer, or manage correspondent accounts for unregulated foreign shell banks, state that is your firm's policy and describe the internal controls that your firm will implement to detect any attempt to open one of these types of accounts.*

TEXT EXAMPLE: We will detect correspondent accounts (any account that permits the foreign financial institution to engage in securities or futures transactions, funds transfers, or other types of financial transactions) for unregulated foreign shell banks by [*describe procedure to detect such accounts*]. Upon finding or suspecting such accounts, firm employees will notify the AML Compliance Officer, who will terminate any verified correspondent account in the United States for an unregulated foreign shell bank. We will also terminate any correspondent account that we have determined is not maintained by an unregulated foreign shell bank but is being used to provide services to such a shell bank. We will exercise caution regarding liquidating positions in such accounts and take reasonable steps to ensure that no new positions are established in these accounts during the termination period. We will terminate any correspondent account for which we have not obtained the information described in Appendix A of the regulations regarding shell banks within the time periods specified in those regulations.

Rules: NASD Rule 3011; Section 313 of the PATRIOT Act; 31 C.F.R. §§103.175 et seq.

b. Certifications

Describe your process for obtaining certifications from any foreign bank account holders.

TEXT EXAMPLE: We will require our foreign bank account holders to complete model certifications issued by the Treasury. We will send the certification forms to our foreign bank account holders for completion, which requires them to certify that they are not shell banks and to provide ownership and agent information. We will re-certify when we believe that the information is no longer accurate and at least once every three years.

Rules: NASD Rule 3011; Section 313 of the PATRIOT Act; 31 C.F.R. §§103.175 et seq.

c. Recordkeeping for Foreign Correspondent Accounts

Firms must keep records identifying the owners of foreign banks with U.S. correspondent accounts and the name and address of the U.S. agent for service of legal process for those banks.

TEXT EXAMPLE: We will keep records identifying the owners of foreign banks with U.S. correspondent accounts and the name and address of the U.S. agent for service of legal process for those banks.

Rules: NASD Rule 3011; Sections 313 and 319 of the PATRIOT Act; 31 C.F.R. §§ 103.175, 177.

d. Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationships.

Describe your firm's procedures for providing information to and handling requests from federal law enforcement about correspondent accounts.

TEXT EXAMPLE: When we receive a written request from a federal law enforcement officer for information concerning correspondent accounts, we will provide that information to the requesting officer not later than 7 days after receipt of the request. We will close, within 10 days, any account for a bank that we learn from Treasury or the Department of Justice has failed to comply with a summons or has contested a summons [and *insert any other circumstances where your firm would consider closing*]. We will scrutinize any account activity during that 10-day period to ensure that any suspicious activity is appropriately reported and to ensure that no new positions are established in these accounts.

Rules: NASD Rule 3011; Sections 313 and 319 of the PATRIOT Act; 31 C.F.R. § 103.185.

7. Private Banking Accounts/Foreign Officials

Describe your firm's due diligence program for "private banking" accounts for non-U.S. persons. Firms must have a due diligence program that is reasonably designed to detect and report any known or suspected money laundering conducted through or involving any private banking account maintained by or on behalf of a non-U.S. person, as well as the existence of the proceeds of foreign corruption in any such account. This requirement applies to all private banking accounts for non-U.S. persons, regardless of when they were opened. Accounts requested or maintained by or on behalf of "senior foreign political figures" (including their family members and close associates) require enhanced scrutiny. At the outset, decisions to open accounts for senior foreign political figures should be approved by senior management.

A "private banking" account is an account (or any combination of accounts) that requires a minimum aggregate deposit of \$1,000,000, is established for one or more individuals, and is assigned to or administered or managed by, in whole or in part, an officer, employee, or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account.

A "senior foreign political figure" includes a current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned commercial enterprise; a corporation, business, or other entity formed by or for the benefit of any such individual; an immediate family member of such an individual; or any individual publicly known (or actually known by the firm) to be a close personal or professional associate of such an individual.

NOTE: If your firm does not open or maintain private banking accounts, state that is your firm's policy and describe the internal controls that your firm will implement to detect any attempt to open one of these types of accounts.

TEXT EXAMPLE: EITHER

We will review our accounts to determine whether we offer any "private banking" accounts and we will conduct due diligence on such accounts. This due diligence will include, at

least, (1) ascertaining the identity of all nominal holders and holders of any beneficial ownership interest in the account (including information on those holders' lines of business and sources of wealth); (2) ascertaining the source of funds deposited into the account; (3) ascertaining whether any such holder may be a senior foreign political figure; and (4) detecting and reporting, in accordance with applicable law and regulation, any known or suspected money laundering and/or use of the proceeds of foreign corruption.

We will review public information, including information available in Internet databases, to determine whether any "private banking" account holders are "senior foreign political figures." If we discover information indicating that a particular "private banking" account holder may be a "senior foreign political figure," and upon taking additional reasonable steps to confirm this information, we determine that the individual is, in fact, a "senior foreign political figure," we will conduct additional enhanced due diligence to detect and report transactions that may involve money laundering or the proceeds of foreign corruption.

In so doing, we will consider the risks that the funds in the account may be the proceeds of foreign corruption, including the purpose and use of the private banking account, location of the account holder(s), source of funds in the account, type of transactions conducted through the account, and jurisdictions involved in such transactions. The degree of scrutiny we will apply will depend on various risk factors, including, but not limited to, whether the jurisdiction the "senior foreign political figure" is from is one in which current or former political figures have been implicated in corruption and the length of time that a former political figure was in office. Our enhanced due diligence might include, depending on the risk factors, probing the account holder's employment history, scrutinizing the account holder's sources of funds, and monitoring transactions to the extent necessary to detect and report proceeds of foreign corruption, and reviewing monies coming from government, government controlled, or government enterprise accounts (beyond salary amounts).

If we do not find information indicating that a "private banking" account holder is a "senior foreign political figure," and the account holder states that he or she is not a "senior foreign political figure," then additional enhanced due diligence is not required.

In either case, if due diligence (or the required enhanced due diligence, if the account holder is a "senior foreign political figure") cannot be performed adequately, we will, after consultation with the firm's AML compliance officer and as appropriate, not open the account, suspend the transaction activity, file a SAR, or close the account.

OR:

*We do not open or maintain private banking accounts **[and describe the internal controls that your firm will implement to detect any attempt to open one of these types of accounts].***

Rules: NASD Rule 3011; Section 312 of the PATRIOT Act; 31 C.F.R. §§103.182.

Other Resources: *Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Official Corruption* -

<http://www.ustreas.gov/press/releases/guidance.htm>;

"Private Banking Activities" (June 30, 1997) - www.federalreserve.gov;

Guidance on Enhanced Scrutiny of Transaction That May Involve Proceeds of Foreign Corruption - <http://www.treas.gov/press/releases/docs/guidance.htm>.

8. Monitoring Accounts For Suspicious Activity

Describe how your firm will monitor accounts for suspicious activity. Automated monitoring is preferable. See [NtM 02-21](#), pages 9-12.

TEXT EXAMPLE: We will monitor through the automated means of [*describe*] for unusual size, volume, pattern or type of transactions.

OR

We will manually monitor a sufficient amount of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as “non-cooperative” are involved, or any of the “red flags” identified in Section 8. b. below. We will look at transactions, including trading and wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer. The AML Compliance Officer or his or her designee [*Add if appropriate: “in consultation with {Name or title}” OR “with the approval of {Name or title}”*] will be responsible for this monitoring, will document when and how it is carried out, and will report suspicious activities to the appropriate authorities. Among the information we will use to determine whether to file a Form SAR-SF are exception reports that include transaction size, location, type, number, and nature of the activity. We will create employee guidelines with examples of suspicious money laundering activity and lists of high-risk clients whose accounts may warrant further scrutiny. Our AML Compliance Officer will conduct an appropriate investigation before a SAR is filed. Our monitoring of specific transactions includes: [*describe.*]

a. Emergency Notification to the Government by Telephone

Describe when and how your firm will call Federal law enforcement in emergencies. See: [NtM 02-21](#), page 13.

TEXT EXAMPLE: When conducting due diligence or opening an account, we will immediately call Federal law enforcement when necessary, and especially in these emergencies: a legal or beneficial account holder or person with whom the account holder is engaged in a transaction is listed on or located in a country or region listed on the OFAC list, an account is held by an entity that is owned or controlled by a person or entity listed on the OFAC list, a customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity, we have reason to believe the customer is trying to move illicit cash out of the government’s reach, or we have reason to believe the customer is about to use the funds to further an act of terrorism. We will first call the OFAC Hotline at 1-800-540-6322. The other contact numbers we will use are: Financial Institutions Hotline (1-866-556-3974), local U.S. Attorney’s Office (*insert contact number*), local FBI Office (*insert contact number*), and local SEC Office (*insert contact number*).

Other Resources: SDN List -- <http://www.treas.gov/ofac/t11sdn.pdf>.

b. Red Flags

TEXT EXAMPLE: Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

- The customer exhibits unusual concern about the firm's compliance with government reporting requirements and the firm's AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the firm's policies relating to the deposit of cash.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the \$10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the FATF.

- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- The customer's account shows numerous currency or cashiers check transactions aggregating to significant sums.
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven.
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed to avoid the firm's normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation S stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

c. Responding to Red Flags and Suspicious Activity

TEXT EXAMPLE: When a member of the firm detects any red flag he or she will investigate further under the direction of the AML Compliance Officer. This may include gathering

additional information internally or from third-party sources, contacting the government, freezing the account, or filing a Form SAR-SF.

9. Suspicious Transactions and BSA Reporting

Describe your firm's procedures for finding suspicious transactions and determining if they need further investigation or warrant filing a SAR-SF. These procedures should also cover the maintenance of SAR documentation and the preservation of its confidentiality, and BSA reporting. Note that firms must exercise due diligence in monitoring suspicious activity as the regulations require firms to file a SAR-SF when they "know, suspect, or have reason to suspect" that transactions involve certain suspicious activities. See: [NtM 02-21](#), pages 11-12; NtM 02-47.

a. Filing a Form SAR-SF

TEXT EXAMPLE: We will file Form SAR-SFs for any account activity (including deposits and transfers) conducted or attempted through our firm involving (or in the aggregate) \$5,000 or more of funds or assets where we know, suspect, or have reason to suspect: 1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation, 2) the transaction is designed, whether through structuring or otherwise, to evade the any requirements of the BSA regulations, 3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or 4) the transaction involves the use of the firm to facilitate criminal activity.

We will not base our decision on whether to file a SAR-SF solely on whether the transaction falls above a set threshold. We will file a SAR-SF and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities. [See: [NtM 02-21](#), page 9.] In high-risk situations, we will notify the government immediately (See Section 8 for contact numbers) and will file a SAR-SF with FinCEN. Securities law violations that are reported to the SEC or a Self-Regulatory Organization (SRO) may also be reported promptly to the local U.S. Attorney, as appropriate.

We will not file SAR-SFs to report violations of Federal securities laws or SRO rules by our employees or registered representatives that do not involve money laundering or terrorism, but we will report them to the SEC or SRO. [See: [NtM 02-21](#), page 10, n.35.]

All SAR-SFs will be periodically reported to the Board of Directors and senior management, with a clear reminder of the need to maintain the confidentiality of the SAR-SF.

We will report suspicious transactions by completing a SAR-SF and we will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR-SF no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR-SF. If no suspect is identified on the date of initial detection, we may delay filing the SAR-SF for an additional 30 calendar days pending identification of a suspect, but in no case, will the reporting be delayed more than 60 calendar days after the date of initial detection.

We will retain copies of any SAR-SF filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-SF. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, or federal or state securities regulators, upon request.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR-SF or the information contained in the SAR-SF, except where disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency or an SRO registered with the SEC, will decline to produce to the SAR-SF or to provide any information that would disclose that a SAR-SF was prepared or filed. We will notify FinCEN of any such request and our response.

Rules: NASD Rule 3011; Section 356 of the PATRIOT Act; 31 C.F.R. §103.19.

Other Resources: FinCEN's Web Site contains additional information (See www.fincen.gov), including annual SAR Activity Reviews and SAR Bulletins, which discuss trends in suspicious reporting and give helpful tips. [NTM 02-21](#), page 12, n.38; NtM 02-47.

SAR-SF Form (fill-in version) -- http://www.fincen.gov/fin101_formandinstructions.pdf
http://www.fincen.gov/fin101_form_only.pdf

SAR Activity Reviews -- http://www.fincen.gov/pub_main.html

SAR Bulletins -- http://www.fincen.gov/pub_main.html

b. Currency Transaction Reports (CTR)

CTRs are filed only for certain transactions involving "currency." "Currency" is defined as "coin and paper money of the United States or of any other country" that is "customarily used and accepted as a medium of exchange in the country of issuance." Currency includes U.S. silver certificates, U.S. notes, Federal Reserve notes, and official foreign bank notes that are customarily used and accepted as a medium of exchange in a foreign country.

TEXT EXAMPLE: *[{Include this language if your firm prohibits the receipt of currency}]*

Our firm prohibits the receipt of currency and has the following procedures to prevent its receipt: *{Describe}*. If we discover currency has been received, w] We will file with FinCEN CTRs for transactions involving currency that exceed \$10,000. Multiple transactions will be treated as a single transaction if they total more than \$10,000 during any one business day. We will use the CTR form at http://www.fincen.gov/reg_bsaforms.html#4789.

Rules: 31 C.F.R. §§103.11, 103.22

c. Currency and Monetary Instrument Transportation Reports (CMIR)

CMIRs are filed for certain transactions involving "monetary instruments." "Monetary instruments" include the following: currency (defined above); traveler's checks in any form; all negotiable instruments (including personal and business checks, official bank checks, cashier's checks, third-party checks, promissory notes, and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such

form that title passes upon delivery; incomplete negotiable instruments that are signed but omit the payee's name; and securities or stock in bearer form or otherwise in such form that title passes upon delivery.

TEXT EXAMPLE: **[{Include this language if your firm prohibits the receipt of currency:}**

Our firm prohibits the receipt of currency and has the procedures described in the previous subsection to prevent its receipt. If we discover currency has been received, w] We will file with the Commissioner of Customs a CMIR whenever the firm transports, mails, ships or receives or causes or attempts to transport, mail, ship or receive monetary instruments of more than \$10,000 at one time (on one calendar day or, if for the purposed of evading the reporting requirements, on one or more days) in or out of the U.S. We will file a CMIR for all such shipments or receipts of monetary instruments, except for currency or monetary instruments shipped or mailed through the postal service or by common carrier. We will, however, file a CMIR for such receipts of currency and monetary instruments and for shipments and deliveries made by the firm by means other than the postal service or common carrier, even when such shipment or transport is made by the firm to an office of the firm located outside the U.S. We will use the CMIR Form at http://www.fincen.gov/reg_bsaforms.html#4790.

Rules: 31 C.F.R. §§103.11, 103.23.

d. Foreign Bank and Financial Accounts Reports (FBAR)

TEXT EXAMPLE: We will file with FinCEN an FBAR for any financial accounts of more than \$10,000 that we hold, or for which we have signature or other authority over, in a foreign country. We will use the FBAR Form at <http://www.fincen.gov/f9022-1.pdf>.

Rules: 31 C.F.R. §103.24.

e. Transfers of \$3,000 or More Under the Joint and Travel Rule

TEXT EXAMPLE: When we transfer funds of \$3,000 or more, we will record on the transmittal order at least the following information: the name and address of the transmitter and recipient, the amount of the transmittal order, the identity of the recipient's financial institution, and the account number of the recipient. We will also verify the identity of transmitters and recipients who are not established customers of the firm (i.e., customers of the firm who have not previously maintained an account with us or for whom we have not obtained and maintained a file with the customer's name, address, taxpayer identification number, or, if none, alien identification number or passport number and country of issuance).

Rules: 31 C.F.R. §103.33(f)

10. AML Record Keeping

Your firm must establish procedures to maintain AML program records and reviews. This requirement includes the records required to be kept as part of the firm's CIP. See: [NtM 02-21](#), page 12.

a. SAR-SF Maintenance and Confidentiality

Describe your firm's retention and confidentiality requirements for SAR-SFs. See: [NtM 02-21](#), page 12.

TEXT EXAMPLE: We will hold SAR-SFs and any supporting documentation confidential. We will not inform anyone outside of a law enforcement or regulatory agency or securities regulator about a SAR-SF. We will refuse any subpoena requests for SAR-SFs or SAR-SF information and immediately tell FinCEN of any such subpoena we receive. We will segregate SAR-SF filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR-SF filings. Our AML Compliance Officer will handle all subpoenas or other requests for SAR-SFs. *[Describe any other retention or confidentiality procedures of your firm for SAR-SFs.]* We will share information with our clearing broker about suspicious transactions in order to determine when a SAR-SF should be filed. As mentioned earlier, we may share with the clearing broker a copy of the filed SAR-SF – unless it would be inappropriate to do so under the circumstances, such as where we file a SAR-SF concerning the clearing broker or its employees.

Rules: 31 C.F.R. §103.19; 67 Fed. Reg. 126, 44501-44502 (July 1, 2002).

b. Responsibility for AML Records and SAR Filing

TEXT EXAMPLE: Our AML Compliance Officer and his or her designee will be responsible to ensure that AML records are maintained properly and that SARs are filed as required. See: [NtM 02-21](#), page 14.

c. Records Required

TEXT EXAMPLE: As part of our AML program, our firm will create and maintain SAR-SFs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification (See Section 5 above) and funds transfers and transmittals as well as any records related to customers listed on the OFAC list. We will maintain SAR-SFs and their accompanying documentation for at least five years. We will keep other documents according to existing BSA and other record keeping requirements, including certain SEC rules that require six-year retention.

Rules: NASD Rule 3011; 31 C.F.R. §103.19; 31 C.F.R. §103.33(f).

11. Clearing/Introducing Firm Relationships

Describe how you and your clearing firm have arranged to comply with AML requirements. See [NtM 02-21](#), page 15. See also Section 3.b. above regarding information sharing.

TEXT EXAMPLE: We will work closely with our clearing firm to detect money laundering. We will exchange information, records, data and exception reports as necessary to comply with AML laws. Both our firm and our clearing firm have filed (and kept undated) the necessary annual certifications for such information sharing, which can be found at http://www.fincen.gov/fi_infoappb.html. As a general matter, we have agreed that our clearing firm will monitor customer activity on our behalf, and we will provide our clearing firm with proper customer identification information as required to successfully monitor customer transactions. We have allocated these functions and set them forth in a written

document. We understand that the allocation of functions will not relieve either of us from our independent obligation to comply with AML laws, except as specifically allowed under the PATRIOT Act and its implementing regulations.

Rules: NASD Rule 3011; Sections 314(b) and 352 of the PATRIOT Act; Section 3.b. above.

12. Training Programs

Describe your AML ongoing employee training and programs. See [NtM 02-21](#), pages 14-15.

TEXT EXAMPLE: We will develop ongoing employee training under the leadership of the AML Compliance Officer and senior management. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources.

Our training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees' duties; what to do once the risk is identified; what employees' roles are in the firm's compliance efforts and how to perform them; the firm's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PATRIOT Act.

We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos. Currently our training program is: *[insert specifics, such as "all registered representatives must view the video entitled "Spotting Money Laundering" by X date or within two weeks of being hired, etc.]* We will maintain records to show the persons trained, the dates of training, and the subject matter of their training.

We will review our operations to see if certain employees, such as those in compliance, margin, and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

Rules: NASD Rule 3011; Section 352 of the PATRIOT Act.

13. Program to Test AML Program

Describe your firm's independent testing function to assess its AML compliance program. You must choose whether your firm's personnel or a qualified outside party will perform this function. Your decision will depend on your firm's size and resources. Smaller firms may find it more cost effective to use a qualified outside party rather than training firm staff to perform the test and keeping that staff sufficiently separate from other firm activities to ensure they are independent. It is recommended that the independent testing be performed annually. See: [NtM 02-21](#), page 15.

a. Staffing

TEXT EXAMPLE: EITHER

The testing of our AML program will be performed by *[Name]*, an independent third party. Their qualifications include *[describe]*.

OR

The testing of our AML program will be performed by [Names], personnel of our firm. Their qualifications include [describe.] To ensure that they remain independent, we will separate their functions from other AML activities by [describe.]

b. Evaluation and Reporting

TEXT EXAMPLE: After we have completed the testing, staff will report its findings to senior management [or to an internal audit committee]. We will address each of the resulting recommendations.

Rules: NASD Rule 3011; Section 352 of the PATRIOT Act.

14. Monitoring Employee Conduct and Accounts

Describe how your firm will monitor employee accounts for potential signs of money laundering. Your firm must subject employee accounts to the same account identifying and monitoring procedures as customer accounts. Your firm should also review supervisors' performance of their AML responsibilities.

TEXT EXAMPLE: We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the AML Compliance Officer. We will also review the AML performance of supervisors, as part of their annual performance review. The AML Compliance Officer's accounts will be reviewed by [Name – another member of senior management.]

Rules: NASD Rule 3011; Section 352 of the PATRIOT Act.

15. Confidential Reporting of AML Non-Compliance

Describe how you ensure that employees who report suspected violations of AML compliance are protected from retaliation.

TEXT EXAMPLE: Employees will report any violations of the firm's AML compliance program to the AML Compliance Officer, unless the violations implicate the Compliance Officer, in which case the employee shall report to [the president/ chairman of the board/ audit committee chair]. Such reports will be confidential, and the employee will suffer no retaliation for making them.

Rules: NASD Rule 3011; Section 352 of the PATRIOT Act.

16. Additional Areas of Risk

TEXT EXAMPLE: The firm has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above. The major

<http://www.finra.org/index.htm>

additional areas of risk include [*describe*]. Additional procedures to address these major risks are [*describe*].

17. Senior Manager Approval

Approve the firm's AML program by signing below.

TEXT EXAMPLE: I have approved this AML program as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the BSA and the implementing regulations under it.

Rules: NASD Rule 3011.

Signed:

Title:

Date: