



## Annual Conference

Washington, DC May 27-29, 2015

---

### Enhancing Anti-Money Laundering Procedures

Thursday, May 28

11:15 a.m. – 12:15 p.m.

#### Topics:

- Identify and describe the Enforcement process.
- Discuss and manage how your company responds to Enforcement inquiries.
- Describe best practices when using outside counsel.

#### Speakers:

Sarah Green (*moderator*)  
Senior Director, AML Compliance  
FINRA Enforcement

Blake Snyder  
Director  
FINRA AML Program

Pamela Ziermann  
Senior Vice President Compliance  
Dougherty & Company LLC

Meg Zucker  
Global Platform Anti-Money Laundering Officer  
RBC Capital Markets LLC

# Anti-Money Laundering Focus

**FINRA Annual Conference  
May 28, 2015 • Washington, DC**



# Panelists

## Moderator:

- **Sarah Green, Senior Director, AML Compliance, FINRA Enforcement**

## Panelists:

- **Blake Snyder, Director, FINRA AML Program**
- **Pamela Ziermann, Senior Vice President Compliance, Dougherty & Company LLC**
- **Meg Zucker, Global Platform Anti-Money Laundering Officer, RBC Capital Markets LLC**

# Hypothetical

- **You: Anti-Money Laundering Compliance Officer at ABC Securities, LLC**
- **Facts: A new team of representatives has joined your firm and have informed you that they are onboarding three new customers:**
  - **Customer A: Foreign bank with a DVP (daily versus payment ) / RVP (receive versus payment) correspondent account with an anticipated business in fixed income.**
  - **Customer B: Investment adviser acting on behalf of a family office**
  - **Customer C: A personal friend of one of the registered representatives.**

# Other Frequently Asked Questions

- **Independent testing**
- **Penny stocks**
- **Training tips**
- **Model validation**
- **De-risking**
- **Cash Management accounts**
- **Customer Due Diligence Rule**

<http://www.finra.org/industry/faq-anti-money-laundering-faq>

## Anti Money Laundering FAQ

For further information on Anti-Money Laundering requirements, please visit the [FINRA Anti-Money Laundering web page](#).

### General Requirements

#### 1. What is an AML Compliance Program required to have?

The Bank Secrecy Act, among other things, requires financial institutions, including broker-dealers, to develop and implement AML compliance programs. Members are also governed by the anti-money laundering rule in [FINRA Rule 3310](#).

FINRA Rule 3310 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 Bank Secrecy Act, FINRA Rule 3310 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 annual (on a calendar-year basis) independent testing for compliance to be conducted by member personnel or by a qualified outside party. If the firm does not execute transactions with customers or otherwise hold customer accounts or act as an introducing broker with respect to customer accounts (e.g. engages solely in proprietary trading or conducts business only with other broker-dealers), the independent testing is required every two years (on a calendar-year basis);
- designate and identify to FINRA (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. Such individual or individuals are associated persons of the firm with respect to functions undertaken on behalf of the firm. Each member must review and, if necessary, update the information regarding a change to its AML compliance person within 30 days following the change and verify such information within 17 business days after the end of each calendar year.

#### 2. Are all broker-dealers subject to the Bank Secrecy Act?

Yes. The Bank Secrecy 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 business and risks, considering factors such as size, location, business activities, the types of accounts they maintain, and the types of transactions in which their customers engage.

**3. FINRA Rule 3310 requires that a firm's AML program be approved in writing by a member of senior management. Does a member of senior management also have to approve any subsequent material changes to the AML program?**

Yes. A member of senior management should approve any subsequent material changes to the firm's AML program. Additionally, if there is a change in senior management, the AML program should be re-approved by the new management.

**Designation of an AML Compliance Person**

**4. Does the AML compliance person have to be a registered principal?**

Neither the Bank Secrecy Act nor [FINRA Rule 3310](#) requires AML compliance persons to register either as representatives or principals. Nevertheless, our general registration requirements state that persons who engage in the investment banking or securities business for a member need to register. 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 person in determining whether he or she must register.

Please note that while the AML compliance person is not required to be a registered person solely as a result of serving that function, FINRA anticipates that most AML compliance persons 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 [FINRA Rule 3310](#); [NASD Notice to Members 02-80, fn.5](#); [NASD Notice to Members 06-07](#).)

**5. What information do members have to provide regarding their AML compliance person, and how should this information be provided to FINRA?**

Members are required to provide to FINRA the name, title, mailing address, email address, telephone number, and facsimile number of the AML compliance person. FINRA Rule 3310.02 requires members to review and, if necessary, update their emergency contact information in the manner prescribed by NASD Rule 1160. NASD Rule 1160 requires firms, via the FINRA Contact System, to update designated contact information promptly upon any material change (but no later than 30 days following the change) and verify such information within 17 business days after the end of each calendar year. FINRA

is collecting the contact information through the FINRA Contact System (FCS) available on the FINRA website.

## **Customer Identification Program Requirements**

### **6. Have the customer identification requirements for opening a DVP account been established?**

Customer identification requirements in [31 CFR 1023.220](#) apply to all customers opening a new account as those terms are defined in the Bank Secrecy Act and implementing regulations, including DVP accounts. Firms may use documentary, non-documentary or a combination of both methods to verify the identity of DVP accounts. The documents that may be used can vary widely including, but not limited to, certified articles of incorporation, government-issued business licenses, partnership agreements, or trust formation records. Some firms use outside vendors to conduct non-documentary verification on DVP accounts. Depending on the nature of the account and the risks associated with it, firms may conduct additional due diligence on these types of accounts and obtain information on the beneficial owners. See FinCEN's [Guidance on Obtaining and Retaining Beneficial Ownership Information](#) and [SIFMA's suggested due diligence practices for hedge funds](#) for additional information.

### **7. What are the CIP 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.

With respect to non-documentary verification, the 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 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](#).)

### **8. 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](#).)

### **9. How is "account" defined in the CIP 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 USA 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](#) and the [Adopting Release](#) for the broker-dealer CIP rule.)

#### **10. Who is a "customer" for purposes of the CIP rule?**

The CIP 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. FinCEN has also determined that a fully-disclosed introduced account is not a customer of the clearing firm for CIP purposes so long as the firms enter into a clearing agreement under which the functions of opening and approving customer accounts and directly receiving and accepting orders from the introduced customer will be allocated exclusively to the introducing firm and the function of extending credit, safeguarding funds and securities and issuing confirmations and statements will be allocated to the clearing firm. The introducing broker is a customer of the clearing firm, although a registered US broker-dealer is exempt from CIP. However, the clearing firm should perform due diligence to determine the risk of its introducing brokers. In addition, clearing firms still have responsibility to identify, monitor and report suspicious activity of its introducing brokers and introduced accounts

See FinCEN guidance [FIN-2008-G002](#) (March 4, 2008).

#### **11. What are the CIP requirements if the customer is a trust or omnibus account?**

A broker-dealer is generally 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 generally not required to look through the intermediary to the underlying beneficial owners, if the intermediary is identified as the accountholder.

However, a broker-dealer's AML program must be risk based. If an account, even an omnibus or a trust account, is determined to be higher risk, the firm may require additional information, including identification of the beneficial owners of the account to mitigate that risk. Certain types of private banking accounts for non U.S. persons also require a firm to obtain information on the account's beneficial owners.

(See [Guidance from the Staffs of the Department of the Treasury and the U.S. Securities and Exchange Commission, October 1, 2003](#) and [31 CFR 1010.620](#) and FinCEN's [Joint Guidance on Obtaining and Retaining Beneficial Ownership Information](#).)

**12. 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.

**13. Is there a requirement to verify the identity of those with trading authority over an account?**

The CIP 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 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. (See 31 CFR 1023.220 (a)(2)(ii)(C).) Additionally, the broker/dealer must consider FINRA Rule 4512(a)(1)(E) in that if the customer is a corporation, partnership or other legal entity, the names of any persons authorized to transact business on behalf of the entity must be obtained.

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

The CIP 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 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 Bank Secrecy Act and be regulated by a Federal functional regulator.
- 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 has complied with the requirements above. 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](#) and the [Adopting Release](#) for the broker-dealer CIP rule.)

Notwithstanding the requirement that the other financial institution must be subject to the BSA, the SEC staff has provided no-action relief to firms who rely on registered investment advisers provided the other requirements of the CIP rule are met.

On January 11, 2013, the no-action position was extended for an additional two years. Specifically, the conditions in paragraph (b)(6) of the CIP Rule have to be met AND the adviser has to agree in the contract that it will promptly

"disclose to the broker-dealer potentially suspicious or unusual activity detected as part of the CIP being performed on the broker-dealer's behalf in order to enable the broker-dealer to file a SAR, as appropriate based on the broker-dealer's judgment" and

"provide its books and records relating to its performance of CIP" to the SEC, an SRO with jurisdiction (e.g., FINRA), or authorized law enforcement agencies at their request.

The current No-Action letter extends the previous letter and grants relief until January 10, 2015. It can be accessed at <http://www.sec.gov/divisions/marketreg/mr-noaction/2013/sifma011113-17a-8.pdf>.

**15. What is a "reasonable time" to verify customers' identities before or after the customer's account is opened?**

The term "reasonable time" is not defined by the 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.

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

The CIP rule includes a provision 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 on-line account, 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, or a tax haven. 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 include 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.

For example, the rule (31 CFR 1023.220(a)(2)(ii)(C)) 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. In addition, a broker-dealer should consider obtaining information concerning the beneficial owners of higher risk accounts. (See [NASD Notice to Members 03-34](#), the [Adopting Release](#) for the broker-dealer CIP rule, and [Joint Guidance on Obtaining and Retaining Beneficial Ownership Information](#)).

**17. 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).

**18. Is there a regulation or guidance that requires member firms to obtain information on the source of account funding? For example, for entity accounts, such as a foundation, charity, or non-profit, would regulators expect to see member firms document the source of funds as part of its CIP requirements or general account due diligence, or would this be a best practice based on the firm's risk assessment of the account/entity?**

In order to implement a properly risk-based AML compliance program, a member firm may document the source of funds as part of general account due diligence based on the firm's risk assessment of the account or the entity. Except in the case of private banking accounts, there is no specific regulation or guidance that requires member firms to obtain information on the source of account funding.

For private banking accounts established for non-U.S. persons, which are specifically defined in the Bank Secrecy Act as accounts with a \$1,000,000 minimum aggregate deposit requirement and the assignment of a liaison for the account, the member firm must "ascertain the source(s) of funds deposited into a private banking account and the purpose and expected use of the account." See [31 CFR 1010.620](#).

**19. How can we obtain the Customer Identification Program Notice in card form?**

FINRA has produced a [Customer Identification Program Notice](#) to assist members in fulfilling the notification requirement in the CIP Rule. This Notice replaces the NASD AML Statement Stuffer that many firms have distributed to their customers. FINRA will print the Notice in bulk at the member's cost. Visit our [AML web page](#) for information on how to order the Notice.

### **Suspicious Activity Reporting**

**20. 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](#).)

**21. Should broker-dealers reject 3rd party wires? If not, what due diligence should be followed before accepting them?**

There is no requirement that broker-dealers reject 3rd party wires; however, [NASD Rule 3012\(a\)\(2\)\(B\)\(i\)](#) requires that firms have procedures that are reasonably designed to review and monitor all transmittals of funds (e.g. wires or checks, etc.) or securities from customers to third party accounts, outside entities, locations other than a customer's primary residence as well as between customers and registered representatives. See the full text of the Rule for further details. Additionally, third party wires and journals are identified as possible money laundering "red flags" in [NASD Notice to Members 02-21](#). These types of red flags may warrant additional due diligence by the broker-dealer before proceeding with the transaction. The broker-dealer's AML procedures should address these types of red flags, how red flags will be detected, and what due diligence and actions will be performed if such red flags are detected. The broker-dealer should maintain evidence of any due diligence performed. There is not any specific due diligence required, so the broker-dealer should assess the risk of the customer and the transaction and conduct appropriate due diligence to determine whether or not the transaction is suspicious and thus reportable on a SAR-SF. Examples of due diligence could include, but not be limited to, contacting the customer, getting a signed Letter of Authorization from the customer, and/or obtaining a written statement from the customer regarding the reason for the third party wire. If the customer's explanation is not reasonable or does not make business sense, the broker-dealer may want to consider whether they are comfortable with the risk associated with the transaction and whether it should file a SAR-SF.

**22. Can an introducing or clearing firm be relieved of AML obligations to the extent that the other is monitoring for suspicious activities?**

No. While a clearing firm can provide tools to help the introducing firm monitor its accounts for potential suspicious activity, all broker-dealers have an independent responsibility to comply with the suspicious activity reporting requirements. Introducing and clearing firms are both responsible for filing SARs for suspicious transactions "conducted or attempted by, at, or through" the firm. Introducing and clearing brokers involved in the same transaction may, but are not required to, file a SAR jointly as long as it includes all relevant facts about the transactions and is otherwise permissible under the law. For example, a SAR-SF filed by the clearing firm in which the introducing broker is the subject could not be shared.

**OFAC**

**23. Are there any tools available to help my firm search the U.S. Treasury's Office of Foreign Asset Control's (OFAC) "Specially Designated Nationals and Blocked Persons" (SDN) list?**

FINRA offers a method of searching the OFAC SDN list. The [FINRA OFAC Search Tool](#) is one option for members to consider using to comply with OFAC economic sanctions. The search tool also includes the Palestinian Legislative Council List. For further information regarding your obligations under the OFAC regulations, please consult the [OFAC website](#).

Specific securities industry guidance from OFAC can be found at the following links:

- [Risk Factors for OFAC Compliance in the Securities Industry](#)

- [Opening Securities and Futures Accounts from an OFAC Perspective](#)
- [OFAC Compliance in the Securities and Investment Sector](#), Journal of Investment Compliance, September 2012

There are many other services available offering search capabilities.

©2015 FINRA. All rights reserved. FINRA is a registered trademark of the Financial Industry Regulatory Authority, Inc.

**INFORMATIONAL**

## Anti-Money Laundering

### NASD Provides Guidance To Member Firms Concerning Anti-Money Laundering Compliance Programs Required By Federal Law

**SUGGESTED ROUTING**

*The Suggested Routing function is meant to aid the reader of this document. Each NASD member firm should consider the appropriate distribution in the context of its own organizational structure.*

- Legal & Compliance
- Operations
- Registration
- Senior Management

**KEY TOPICS**

- Compliance Programs
- Money Laundering

### Executive Summary

On October 26, 2001, President Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act).<sup>1</sup> Title III of the Patriot Act, referred to as the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 (Money Laundering Abatement Act), imposes obligations on broker/dealers under new anti-money laundering (AML) provisions and amendments to the existing Bank Secrecy Act (BSA) requirements.<sup>2</sup>

Among other things, the Money Laundering Abatement Act requires all financial institutions, including broker/dealers, to establish and implement, by **April 24, 2002**, AML programs designed to achieve compliance with the BSA and the regulations promulgated thereunder. The NASD reminds members that violations of the AML laws could lead to criminal prosecution.

On February 15, 2002, the NASD filed with the Securities and Exchange Commission (SEC) a rule proposal to prescribe the minimum standards required for each member firm's AML compliance program. A copy of this rule filing can be found on the NASD Regulation AML Web Page. (See [www.nasdr.com/money.asp](http://www.nasdr.com/money.asp).) NASD Regulation's AML Web Page also provides links to other sites and documents to assist members in understanding their obligations under the AML rules and regulations.

On February 25, 2002, the SEC published the proposed rule change in the *Federal Register*. The SEC received four comment letters in response to the *Federal Register* publication. Before

becoming effective, the proposed rule change must be approved by the SEC.

The Securities Industry Association Anti-Money Laundering Committee recently released a preliminary guide for firms to use when developing their AML programs (SIA Guidance). The SIA Guidance generally discusses key elements for broker/dealers to consider in developing effective AML programs. NASD Regulation's AML Web Page provides a link to the SIA Guidance.

The NASD is issuing this *Notice* to provide guidance to assist members in developing AML compliance programs that fit their business models and needs. A table of contents has been provided for readers' convenience.

Because the Department of Treasury (Treasury) is still developing AML rules, the NASD will update its guidance as new rules become final. In the interim, firms must comply with the current requirements of the BSA and the provisions of the Money Laundering Abatement Act that now apply to broker/dealers and should familiarize themselves with the proposed rules that Treasury has issued to date. (For links to Treasury's proposed rules, see [www.nasdr.com/money.asp](http://www.nasdr.com/money.asp).)

### Questions/Further Information

Questions regarding this *Notice to Members* may be directed to Nancy Libin, Assistant General Counsel, Office of General Counsel, NASD Regulation, at (202) 728-8835; Grace Yeh, Assistant General Counsel, at (202) 728-6939; or Kyra Armstrong, Senior Attorney, Department of Member Regulation, at (202) 728-6962.



## Anti-Money Laundering Notice to Members

### TABLE OF CONTENTS

BACKGROUND.....	1
INTRODUCTION.....	1
Broker/Dealers And Existing Anti-Money Laundering Laws.....	1
New And Expanded Anti-Money Laundering Laws Applicable To Broker/Dealers.....	2
NASD ANTI-MONEY LAUNDERING PROGRAM RULE.....	4
ANTI-MONEY LAUNDERING PROGRAM GUIDANCE.....	5
Develop Internal Policies, Procedures, And Controls.....	5
<i>Identification And Verification Of Account Holders</i> .....	5
Opening Accounts.....	5
Online Brokers.....	7
Additional Due Diligence When Opening an Account.....	7
<i>Prohibitions On U.S. Correspondent Accounts With Foreign Shell Banks         And Special Due Diligence For Correspondent Accounts</i> .....	8
<i>Special Due Diligence For Private Banking Accounts</i> .....	8
<i>Monitoring Accounts For Suspicious Activity</i> .....	9
Money Laundering “Red Flags”.....	10
Reporting Procedures.....	11
Recordkeeping And Disclosure.....	12
Currency Transaction Reports.....	12
Currency And Monetary Instrument Transportation Reports.....	12
<i>Procedures For Sharing Information With And Responding To Requests         For Information From Federal Law Enforcement Agencies</i> .....	12
<i>Voluntary Information Sharing Among Financial Institutions</i> .....	13
Designate Compliance Officer.....	13
Establish An Ongoing Training Program.....	14
Establish An Independent Testing Function.....	15
INTRODUCING BROKERS AND CLEARING BROKERS.....	15
CONCLUSION.....	16
ENDNOTES.....	17

### BACKGROUND

The PATRIOT Act is designed to detect, deter, and punish terrorists in the United States and abroad and to enhance law enforcement investigation tools by prescribing, among other things, new surveillance procedures, new immigration laws, as well as new and more stringent AML laws. The Money Laundering Abatement Act expands and strengthens the AML provisions put into place by earlier legislation.

Several provisions of the Money Laundering Abatement Act are relevant to NASD members. Among other things, all broker/dealers must implement an anti-money laundering compliance program by April 24, 2002. The Money Laundering Abatement Act also requires Treasury to promulgate rules requiring broker/dealers to file suspicious activity reports (SARs), which identify and describe transactions that raise suspicions of illegal activity, and to establish certain procedures with regard to "correspondent accounts" maintained for foreign banks.<sup>3</sup> In late December 2001, Treasury released proposed rules regarding the filing of SARs by broker/dealers<sup>4</sup> and the maintenance of "correspondent accounts" for foreign banks.<sup>5</sup> In late February 2002, Treasury released proposed and final rules governing information sharing among law enforcement authorities, regulatory organizations, and financial institutions.<sup>6</sup> Treasury will continue to issue proposed and final rules throughout the year governing and providing further guidance with respect to customer identification, "correspondent accounts" with foreign banks, and the application of AML rules to the brokerage industry, among other matters. The NASD will continue to keep members apprised of AML rules and regulations that Treasury proposes and those that Treasury adopts.

### INTRODUCTION

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Money laundering occurs in connection with a wide variety of crimes, including, but not limited to, drug trafficking, robbery, fraud, racketeering, and terrorism.

In general, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash profits from criminal activity are 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 separate further the proceeds from their criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund further criminal or legitimate activities.<sup>7</sup>

### Broker/Dealers And Existing Anti-Money Laundering Laws

Broker/dealers are subject to most of the existing AML rules as well as the new AML provisions of the Money Laundering Abatement Act, which are discussed in detail later in the document.

Firms should be aware that there are potential severe civil and criminal penalties for violations of AML laws. Under the criminal statutes, a person or entity could be criminally prosecuted for assisting or facilitating a transaction involving money laundering by a customer if the firm (or person) knew or was willfully blind to the fact that the transaction involved illegally obtained funds.<sup>8</sup>

---

## Special NASD Notice to Members 02-21

---

All broker/dealers have been and will continue to be subject to existing BSA reporting and recordkeeping requirements, as briefly summarized below:

- **Currency Transaction Report (CTR):** Broker/dealers are required to file CTRs for transactions involving currency that exceed \$10,000. Because structuring is prohibited, multiple transactions are treated as a single transaction if they total more than \$10,000 during any one business day. CTRs are filed with the Financial Crimes Enforcement Network (FinCEN), a bureau of Treasury.
- **Currency and Monetary Instrument Transportation Report (CMIR):** Any person who physically transports, mails, or ships currency or other monetary instruments into or out of the United States, in aggregated amounts exceeding \$10,000 at one time, must report the event on a CMIR. Any person who receives any transport, mail, or shipment of currency, or other monetary instrument from outside the United States in an aggregate amount exceeding \$10,000 at one time also must report the receipt. CMIRs are filed with the Commissioner of Customs.
- **Report of Foreign Bank and Financial Accounts (FBAR):** Any person having a financial interest in, or signature or other authority over, financial accounts in a foreign country is required to report the relationship if the aggregate value of the accounts exceeds \$10,000. FBARs are filed with FinCEN.
- **Funds Transfers and Transmittals:** Broker/dealers effecting transmittals or transfers of funds, including wire fund transfers, of \$3,000 or more must collect, retain and record on the transmittal order certain information regarding the transfer, including 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. Broker/dealers also must verify the identity of transmitters and recipients that are not established customers.

In addition, broker/dealers that are subsidiaries of banks or bank holding companies currently are required under the banking regulations to file SARs with FinCEN. Such broker/dealers currently are required to report known or suspected federal criminal offenses, at specified dollar thresholds, or suspicious transactions involving \$5,000 or more that they suspect (1) involve funds derived from illegal activity or an attempt to hide or disguise funds or assets derived from illegal activity, (2) are designed to evade the requirements of the BSA, or (3) have no apparent lawful or business purpose or vary substantially from normal practice. The NASD previously has recommended that members report suspicious transactions and has advised firms that the failure to do so could be construed as aiding and abetting money laundering violations, subjecting the member to civil and criminal liability.<sup>9</sup> Some firms, in fact, have been submitting SARs on a voluntary basis. As discussed in more detail later in the document, all broker/dealers will soon be required to file SARs.

### **New And Expanded Anti-Money Laundering Laws Applicable To Broker/Dealers**

As noted above, the Money Laundering Abatement Act imposes significant new obligations on broker/dealers through new AML provisions and amendments to the existing provisions of the BSA. A brief summary of the new requirements along with anticipated effective dates is provided below:

- **Section 312 (Due Diligence Requirements):** Section 312 requires special due diligence for all private banking and "correspondent" bank accounts (accounts established to receive deposits from, make payments on behalf of, or handle other financial transactions for a foreign bank) involving foreign persons, even if opened before Congress passed the PATRIOT Act.<sup>10</sup> Treasury is required to delineate, by regulation, the special due diligence

---

## Special NASD Notice to Members 02-21

---

policies, procedures, and controls by April 24, 2002. Regardless of whether final regulations have been promulgated, the minimum due diligence requirements set forth in Section 312 (as discussed below in the “Anti-Money Laundering Program Guidance” section) become **effective on July 23, 2002**.

- **Section 313 (Correspondent Account Prohibitions):** Section 313 prohibits certain financial institutions, including broker/dealers, from maintaining a “correspondent account” for, or on behalf of, a foreign “shell” bank (a foreign bank with no physical presence in any country). Financial institutions are also required to take reasonable steps to ensure that they are not indirectly providing correspondent banking services to foreign shell banks through foreign banks with which they maintain correspondent relationships. Section 313 became **effective on December 26, 2001**. Treasury released proposed regulations defining “correspondent account” in late December 2001.<sup>11</sup>
- **Section 314 (Financial Institution Cooperation Provisions):** Section 314 addresses increased cooperation among financial institutions, regulatory authorities, and law enforcement authorities. Treasury published regulations implementing Section 314 in the *Federal Register* on March 4, 2002.<sup>12</sup> Treasury included a proposed rule to establish a communication link between federal law enforcement and financial institutions to better share information relating to suspected terrorists and money launderers. In addition, Treasury issued an interim final rule, **effective March 4, 2002**, requiring financial institutions to file an initial, and annual thereafter, certification (which can be completed online at FinCEN’s Web Site at [www.treas.gov/fincen](http://www.treas.gov/fincen)) if they wish to share information regarding terrorist financing and money laundering with other financial institutions or associations of financial institutions.<sup>13</sup>
- **Section 319(b) (Domestic and Foreign Bank Records Production):** Section 319(b) addresses the production of domestic and foreign bank records. A financial institution is required to produce account information relating to foreign bank accounts **within seven days** in response to requests from federal law enforcement. Section 319 became **effective on December 26, 2001**. As mentioned above, Treasury released proposed rules regarding maintaining “correspondent accounts” in late December 2001.<sup>14</sup>
- **Section 326 (Customer Identification Standards):** Section 326 requires Treasury and the SEC, jointly, to issue regulations that set forth minimum standards for customer identification in the account opening process. The regulations will need to require firms, at a minimum, to implement “reasonable procedures” to verify the identity of the customer opening an account, maintain records used to identify the customer, and consult government-provided lists of known or suspected terrorists. Final regulations prescribed under Section 326 will take effect **not later than October 26, 2002**. Treasury and the SEC have not yet released proposed regulations regarding customer identification.
- **Section 352 (AML Compliance Program Components):** Section 352 requires all financial institutions to develop and implement AML compliance programs **on or before April 24, 2002**. Section 352 requires the compliance programs, at a minimum, to establish (1) the development of internal policies, procedures, and controls, (2) the designation of a compliance officer with responsibility for a firm’s anti-money laundering program, (3) an ongoing employee training program, and (4) an independent audit function to test the effectiveness of the anti-money laundering compliance program. Section 352 further requires Treasury by April 24, 2002, to issue regulations that consider the extent to which these requirements correspond to the size, location, and activities of different financial institutions. Section 352 further allows Treasury, at its discretion, to issue additional requirements for AML compliance programs before the April 24, 2002, deadline. As further discussed later in the document, the NASD has proposed a rule setting forth the minimum standards for its members’ AML compliance programs.

---

## Special NASD Notice to Members 02-21

---

- **Section 356 (Broker/Dealer SAR Regulations):** By *July 1, 2002*, Treasury must publish final regulations requiring broker/dealers to file SARs. Treasury released proposed broker/dealer SAR regulations in late December 2001.<sup>15</sup> Under Treasury's proposed regulations, the suspicious activity reporting requirement would become effective *180 days after the date on which the final broker/dealer SAR regulations are published in the Federal Register*.

### NASD ANTI-MONEY LAUNDERING PROGRAM RULE

On February 15, 2002, the NASD filed with the SEC a rule proposal that would set forth minimum standards for broker/dealers' AML compliance programs.<sup>16</sup> As required by the Money Laundering Abatement Act itself, the rule proposal would require firms to develop and implement a written AML compliance program by April 24, 2002. The proposed rule would require the program 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 BSA and the implementing regulations promulgated thereunder. The proposed rule change would require firms, at a minimum, to:

- (1) establish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of suspicious transactions;
- (2) establish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the BSA and implementing regulations;
- (3) provide for independent testing for compliance to be conducted by member personnel or by a qualified outside party;
- (4) designate an individual or individuals responsible for implementing and monitoring the day-to-day operations and internal controls of the program; and
- (5) provide ongoing training for appropriate personnel.

Each firm's AML program must be designed to ensure compliance with the new provisions of the Money Laundering Abatement Act, the earlier provisions of the BSA, and the regulations promulgated thereunder. To be effective, those procedures must reflect the firm's business model and customer base. Further, in developing program criteria, firms should consider the guidelines established by the United States Sentencing Commission in the U.S. Sentencing Commission Guidelines for organizations, as well as the fiduciary responsibilities of officers and directors to ensure that the firm's compliance programs are viable and effective.<sup>17</sup>

Regardless of when and in what form the SEC approves the NASD proposed AML compliance rule, all firms are required by federal law (the Money Laundering Abatement Act) to have AML programs in place **by April 24, 2002**.<sup>18</sup> These AML programs must meet the minimum requirements articulated in Section 352 of the Money Laundering Abatement Act.<sup>19</sup>

Members should keep in mind that the obligation to develop and implement an AML compliance program is not a "one-size-fits-all" requirement. The general nature of the requirement reflects Congressional intent that each financial institution should have the flexibility to tailor its AML program to fit its business. This flexibility is designed to ensure that all entities covered by the statute, from the very large financial institutions to the small firms, will institute effective and appropriate policies and procedures to monitor for AML compliance.<sup>20</sup> In this regard, each broker/dealer, in developing an appropriate AML program that complies with the Money Laundering Abatement Act, should consider factors such as its size, location, business activities, the types of accounts it maintains, and the types of transactions in which its customers engage.

## **ANTI-MONEY LAUNDERING PROGRAM GUIDANCE**

The required elements of an AML program are discussed in detail below.

### **Develop Internal Policies, Procedures, And Controls**

Broker/dealers must develop internal policies, procedures, and controls to ensure compliance with the AML laws. The AML procedures should contain a statement that sets forth the member's policy of prohibiting money laundering and its overall efforts to detect, deter, and prevent any such violations. Broker/dealers also must establish internal controls to ensure that their AML policies and procedures are being enforced. As with any supervisory procedure, the firm must establish and implement controls and written procedures that explain the procedures that must be followed, the person responsible for carrying out such procedures, how frequently such procedures must be performed, and how compliance with the procedures should be documented and tested.

Firms must determine the manner in which AML procedures that address the following (each of which will be discussed more fully below) will apply to various accounts:

- account opening and maintenance, including verification of the identity of the customer;
- opening and maintaining "correspondent accounts" for foreign banks;
- monitoring of account activities, including but not limited to, trading and the flow of money into and out of the account, the types, amount, and frequency of different financial instruments deposited into and withdrawn from the account, and the origin of such deposits and the destination of withdrawals;
- separating the duties of employees where feasible to ensure a system of checks and balances (for example, firms may want to ensure that persons who handle cash do not open accounts or file CTRs);
- monitoring for, detecting, and responding to "red flags";
- responding to regulatory requests for AML information;
- establishing controls and monitoring employees' trading and financial activity in employee accounts; and
- ensuring that AML compliance programs contain a mechanism or process for the firm's employees to report suspected violations of the firm's AML compliance program procedures and policies to management, confidentially, and without fear of retaliation.

### ***Identification And Verification Of Account Holders***

#### *Opening Accounts*

Prior to the enactment of the Money Laundering Abatement Act, broker/dealers already had significant obligations to gather information about their customers in order to, among other things, know their customers. NASD Rule 3110 requires member firms to obtain certain information about their customers when opening an account, including the following: the customer's name and residence; whether the customer is of legal age; the signature of the registered representative introducing the account and signature of the member or partner, officer, or manager who accepts the account; and if the customer is a corporation, partnership, or other

---

## Special NASD Notice to Members 02-21

---

legal entity, the names of any persons authorized to transact business on behalf of the entity. Member firms are also required to make reasonable efforts to obtain the following additional information (for accounts other than institutional accounts and accounts in which investments are limited to transactions in open-end investment company shares not recommended by the member or its associated persons) prior to the settlement of an initial transaction in the account: a customer's tax identification and Social Security number; the customer's occupation and name and address of the employer; and whether the customer is an associated person of another member.

Member firms also are required under NASD Rules 2110 and 2310 to obtain additional customer information. Members are required under NASD Rule 2110 to comply with general "Know Your Customer" requirements. Pursuant to these requirements, members must make reasonable efforts to obtain certain basic financial information from customers so that members can protect themselves and the integrity of the securities markets from customers who do not have the financial means to pay for transactions.<sup>21</sup> NASD Rule 2310 relates to a member's suitability obligations to its customers and requires each member to use reasonable efforts to obtain information concerning a customer's financial status, tax status, and investment objectives prior to making any recommendations to the customer regarding the purchase, sale, or exchange of securities.

The information required under NASD Rules 3110, 2110, and 2310 is the starting point for new AML customer identification procedures. The Money Laundering Abatement Act imposes additional customer identification requirements on member firms. Effective October 26, 2002 (or earlier, if final customer identification regulations are effective prior to October 26, 2002), broker/dealers are required to implement reasonable procedures for identifying customers and verifying their information.<sup>22</sup> These procedures, at a minimum, must require a firm:

- to verify, to the extent reasonable and practicable, the identity of any customer seeking to open an account;<sup>23</sup>
- to maintain records of information to verify a customer's identity; and
- to check that a customer does not appear on any list of known or suspected terrorists or terrorist organizations such as those persons and organizations listed on Treasury's Office of Foreign Assets Control (OFAC) Web Site ([www.treas.gov/ofac](http://www.treas.gov/ofac)) (and available on [www.nasdr.com/money.asp](http://www.nasdr.com/money.asp)) under "Terrorists" or "Specially Designated Nationals and Blocked Persons" (SDN List), as well as the list of embargoed countries and regions (collectively, the OFAC List).<sup>24</sup>

Under the new AML customer identification requirements, broker/dealers will be required to make reasonable efforts to obtain and verify information about a customer. If the customer is an individual, a firm will need, to the extent reasonable and practicable, to obtain and verify certain information concerning the individual's identity, such as the individual's name, address, date of birth, and government issued identification number. Possible sources of this information include:

- physical documents, such as a driver's license, passport, government identification, or an alien registration card,<sup>25</sup> or, for businesses, a certificate of incorporation, a business license, any partnership agreements, any corporate resolutions, or other similar documents; or
- databases, such as Equifax, Experian, Lexis/Nexis, or other in-house or custom databases.

Firms opening accounts should verify the identification information at the time the account is opened, or within a relatively short time period thereafter (e.g., within five business days after account opening). Because of the unknown risk that the prospective customer could be involved

---

## Special NASD Notice to Members 02-21

---

in criminal activity, members should consider, depending on the nature of a transaction and an account, not effecting a transaction prior to verifying the information. If a potential customer refuses to provide any of the information described above, or appears to have intentionally provided false or misleading information, a firm should not open the account. If an existing customer fails to provide the requested information, the firm, after considering the known and unknown risks involved, may consider closing the account. Moreover, in either of these situations, the firm's AML compliance personnel should be notified so that a determination can be made as to whether the circumstance should be voluntarily reported to FinCEN or OFAC, as appropriate.

In the context of AML compliance, members should implement procedures that allow the firm to collect and use information concerning the account holder's wealth, net worth, and sources of income to detect and deter possible money laundering activity. Such a review should be integrated into the new accounts supervisor's existing procedures before such supervisor authorizes the opening of an account. Moreover, the supervisor's review should be documented and reviewed to ensure that the account-opening procedures are being conducted properly. Firms should consider using a checklist that lists the types of information required and documents explanations for why an account was opened absent such information.

### *Online Brokers*

Online brokers generally do not meet or speak directly to their prospective or existing clients. These firms must acquire information about customers and, as mentioned earlier, make maximum use of other means of verifying customer identity, such as electronic databases (Equifax, Experian, Lexis/Nexis, or other in-house or custom databases). As is required of all firms, such verification of customer information must take place at the time the account is opened or within a short period thereafter (e.g., five business days). Online firms should also consider conducting computerized surveillance of account activity to detect suspicious transactions and activity. Given the global nature of online brokerage activity, it is essential that online brokers confirm the customer data and review the OFAC List to ensure that customers are not prohibited persons or entities and are not from embargoed countries or regions.

### *Additional Due Diligence When Opening An Account*

Broker/dealers should perform the following additional due diligence when opening an account, depending on the nature of the account, and to the extent reasonable and practicable:

- inquire about the source of the customer's assets and income so that the firm can determine if the inflow and outflow of money and securities is consistent with the customer's financial status;
- gain an understanding of what the customer's likely trading patterns will be, so that any deviations from the patterns can be detected later on, if they occur;
- maintain records that identify the owners of accounts and their respective citizenship;
- require customers to provide street addresses to open an account, and not simply post office addresses, or "mail drop" addresses;
- periodically contact businesses to verify the accuracy of addresses, the place of business, the telephone, and other identifying information; and
- conduct credit history and criminal background checks through available vendor databases.



### ***Prohibitions On U.S. Correspondent Accounts With Foreign Shell Banks And Special Due Diligence For Correspondent Accounts***

Broker/dealers are prohibited from establishing, maintaining, administering, or managing a “correspondent account” (see note 3) in the United States for an unregulated foreign shell bank. Firms should have procedures in place to ensure that this does not occur and should immediately terminate such accounts if they have any. The broker/dealer’s AML compliance personnel should be notified upon discovery or suspicion that the firm may be maintaining or establishing a “correspondent account” in the United States for a foreign shell bank.

The Money Laundering Abatement Act requires broker/dealers to maintain records identifying the owners of foreign banks that maintain “correspondent accounts” in the United States and the name and address of an agent residing in the United States authorized to accept service of legal process for such banks.<sup>26</sup> Broker/dealers should require their foreign bank account holders to complete model certifications issued by Treasury to the extent possible. U.S. depository institutions and broker/dealers can send the certification forms 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.<sup>27</sup> Firms are required to recertify (if relying on the certification forms) or otherwise verify any information provided by each foreign bank, or otherwise relied upon, at least every two years or at any time the firm has reason to believe that the information is no longer accurate.

In addition, broker/dealers will be required under Section 312 of the Money Laundering Abatement Act to establish appropriate, specific, and, where necessary, enhanced due diligence policies, procedures, and controls that are reasonably designed to detect and report instances of money laundering for any “correspondent account” established, maintained, administered, or managed for a foreign bank. *At a minimum*, in the case of foreign banks licensed by certain high-risk jurisdictions or operating under an offshore banking license, broker/dealers are required to take reasonable steps:

- to determine the ownership of the foreign bank;
- to conduct enhanced scrutiny of the account to detect and report suspicious activity; and
- to determine whether the foreign bank maintains “correspondent accounts” for any other bank, and if so, the identity of those banks.<sup>28</sup>

### ***Special Due Diligence For Private Banking Accounts***

Similarly, the Money Laundering Abatement Act requires broker/dealers, *at a minimum*, to take reasonable steps to determine the identity of the nominal and beneficial account holders of, and the source of funds deposited into, a private banking account maintained by or on behalf of a non-U.S. citizen, and to conduct enhanced scrutiny of accounts requested or maintained by, or on behalf of, a senior foreign political figure,<sup>29</sup> or any immediate family member or close associate of a senior foreign political figure. A private bank account is an account (or combination of accounts) that requires an aggregate deposit of funds or other assets of more than \$1,000,000 established on behalf of one or more individuals who have a direct or beneficial ownership interest in the account, and is 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.<sup>30</sup> This enhanced monitoring or scrutiny should be reasonably designed to detect and report transactions that may involve the proceeds of foreign official corruption.<sup>31</sup> Broker/dealers should monitor future pronouncements from Treasury, while also determining the extent to which they offer “private banking accounts,” and ensure that their AML compliance program includes enhanced monitoring and scrutiny of accounts requested or held on behalf of foreign officials who may be involved in corrupt activities. The special due diligence requirements discussed in this section will become effective on July 23, 2002, regardless of whether Treasury has promulgated final regulations.

#### ***Monitoring Accounts For Suspicious Activity***

The Money Laundering Abatement Act requires Treasury to adopt regulations requiring broker/dealers to file SARs.<sup>32</sup> Under Treasury’s proposed regulations, SARs would be filed with FinCEN. Broker/dealers would be required to file SARs for:

- any transaction conducted or attempted by, at or through a broker/dealer involving (separately or in the aggregate) funds or assets of \$5,000 or more for which:
  - the broker/dealer detects any known or suspected federal criminal violation involving the broker/dealer, or
  - the broker/dealer knows, suspects, or has reason to suspect that the transaction:
    - involves funds related to illegal activity,<sup>33</sup>
    - is designed to evade the regulations, or
    - has no business or apparent lawful purpose and the broker/dealer knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

Although the reporting threshold begins at \$5,000, in its proposed regulations, Treasury notes that a risk-based approach to developing compliance procedures that can be reasonably expected to promote the detection and reporting of suspicious activity should be the focus of a broker/dealer’s AML compliance program. Treasury further notes that a compliance program that allows for the review of only those transactions that are above a set threshold, regardless of whether transactions at a lower dollar threshold may involve money laundering or other risks, would probably not be a satisfactory program.<sup>34</sup> Broker/dealers should file a SAR and in some circumstances notify law enforcement authorities of all transactions that arouse articulable suspicion that proceeds of criminal, terrorist, or corrupt activities may be involved.

Treasury could amend its proposed regulations based on comments it receives from interested parties. Treasury is required to issue final SAR regulations by July 1, 2002, and firms will be required to file SARs beginning 180 days after final broker/dealer SAR regulations are published in the *Federal Register*. To demonstrate a strong commitment to compliance with AML principles and goals, broker/dealers should consider filing SARs voluntarily prior to the effective date of the regulations. NASD Regulation will keep members informed as Treasury’s proposed regulations are amended and finalized.

### *Money Laundering “Red Flags”*

Broker/dealers need to look for signs of suspicious activity that suggest money laundering.<sup>35</sup> If a broker/dealer detects “red flags,” it should perform additional due diligence before proceeding with the transaction. Examples of “red flags” are described below:

- The customer exhibits unusual concern regarding the firm’s compliance with government reporting requirements and the firm’s AML policies, particularly with respect to 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 suspect 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 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 equivalents, or asks for exemptions from the firm’s policies relating to the deposit of cash and cash equivalents.
- 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 Financial Action Task Force (FATF).<sup>36</sup>
- 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.

---

## Special NASD Notice to Members 02-21

---

- 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 in such a manner 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" (Reg 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 business purpose or other purpose.
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.<sup>37</sup>

The above-listed money laundering "red flags" are not exhaustive; however, an awareness of the "red flags" will help ensure that broker/dealer personnel can identify circumstances warranting further due diligence. Appropriate "red flags" should be described in the written policies and AML compliance procedures of the broker/dealer.

### *Reporting Procedures*

Although final regulations concerning the filing of SARs may not be adopted until July 1, 2002, voluntary reporting is useful to the government and helpful to firms in order to provide a defense to charges of aiding and abetting money laundering violations. Furthermore, in anticipation of the adoption of the final broker/dealer SAR requirements, all broker/dealers should be preparing to establish and implement procedures to detect and report suspicious transactions by means of SARs. Firms should implement systems, preferably automated ones, that would allow firms to monitor trading, wire transfers, and other account activity to allow firms to determine when suspicious activity is occurring. If a firm decides to monitor customer accounts manually, it must review a sufficient amount of account activity to ensure the detection of suspicious activity by allowing the member to identify patterns of activity and more importantly, new patterns or patterns that are inconsistent with the customer's financial status or make no economic sense.

---

## Special NASD Notice to Members 02-21

---

Exception reports should consider the transaction size, location, type, number, and the nature of the activity. Firms should create guidelines for employees that identify examples of suspicious activity that may involve money laundering and form lists of high-risk clients whose activities may warrant further scrutiny. Firms should develop procedures for following-up on transactions that have been identified as suspicious or high-risk.

Broker/dealers should also develop administrative procedures concerning SARs. The procedures should address the process for filing SARs and reviewing SAR filings and the frequency of filings for continuous suspicious activity. In addition, a broker/dealer should consider requiring that all of its SAR filings be reported periodically to its Board of Directors and/or to senior management. In the event of a high-risk situation, broker/dealers should require that a report be made immediately to the Board of Directors and/or senior management.<sup>38</sup>

### *Recordkeeping And Disclosure*

Firms should develop procedures to maintain the confidentiality of the SAR filings and to maintain copies of SARs for a five-year period. Firms are prohibited from notifying any person involved in a reported transaction that the transaction has been reported on a SAR. In addition, firms may not disclose SARs or the fact that a SAR was filed, other than to law enforcement agencies or securities regulators. Firms must also have procedures in place to ensure the denial of any subpoena requests for SARs or information in SARs, and for informing FinCEN of any subpoena received. It may be advisable to segregate SAR filings and supporting documentation from other books and records of the firm to avoid violating the prohibitions on disclosure of these records. The broker/dealer should also establish procedures and identify a contact person to handle requests for a subpoena or other requests that call for disclosure of a SAR.

### *Currency Transaction Reports*

Broker/dealers should have procedures to ensure compliance with the BSA provision requiring broker/dealers to file CTRs with FinCEN.

### *Currency And Monetary Instrument Transportation Reports*

Broker/dealers should have procedures to ensure compliance with the BSA provision requiring broker/dealers to file CMIRs with the Commissioner of Customs when any person physically transports, receives, mails, or ships currency or other monetary instruments into or out of the United States, in aggregated amounts exceeding \$10,000 at one time.

### ***Procedures For Sharing Information With And Responding To Requests For Information From Federal Law Enforcement Agencies***

Broker/dealers should develop procedures to handle requests for information from FinCEN relating to money laundering or terrorist activity. Under Treasury's *proposed* regulations implementing Section 314, which were published in the *Federal Register* on March 4, 2002, FinCEN may require broker/dealers to search their records to determine whether they maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. If a broker/dealer identifies an account or transaction identified by FinCEN, it would be required to report the identity of the individual, entity, or organization, the account number, all identifying information provided by the account holder when the account was established, and the date and type of transaction. Broker/dealers would be required to report the information to FinCEN as soon as possible either by e-mail to [patriot@fincen.treas.gov](mailto:patriot@fincen.treas.gov), by calling the Financial Institutions Hotline (1-866-556-3974), or by any other means that FinCEN specifies.

Broker/dealers also should identify contact persons and have procedures in place for providing information to and handling requests from enforcement authorities about the firms' AML efforts, as well as customers engaged in possible money laundering. This information must be provided to the appropriate agency and made available at a specified location when requested. Firms should establish procedures to provide such information *not later than seven days* after receiving a written enforcement agency request.

Firms should also have procedures in place to terminate a correspondent relationship with a foreign bank *within 10 business days* of receiving written notice from Treasury or the United States Attorney General that the foreign bank failed either to comply with a summons or subpoena or to contest it in United States court.

Finally, in the course of performing due diligence or during the opening of an account, firms should immediately contact Federal law enforcement by telephone in appropriate emergency situations as described below:

- a customer is listed on the OFAC List;
- a customer's legal or beneficial account owner is listed on the OFAC List;
- a customer attempts to use bribery, coercion, undue influence, or other inappropriate means to induce a broker/dealer to open an account or proceed with a suspicious or unlawful activity or transaction; and
- any other situation that a firm reasonably determines requires immediate government intervention.

#### ***Voluntary Information Sharing Among Financial Institutions***

To the extent desired and/or appropriate, broker/dealers should have procedures in place for sharing information with other financial institutions about those suspected of terrorism and money laundering. Under Treasury's *interim rule*, which became effective on March 4, 2002, broker/dealers that share this information must file an annual certification with FinCEN.<sup>39</sup> The certification requires broker/dealers to take steps necessary to protect the confidentiality of the information and to use the information only for purposes specified in the rule. The certification can be found at: [www.treas.gov/fincen](http://www.treas.gov/fincen). Broker/dealers should have adequate procedures to protect the security and confidentiality of such information.

#### **Designate Compliance Officer**

Every broker/dealer compliance program must designate a compliance officer ("AML Compliance Officer") to help administer the firm's AML compliance program efforts. Broker/dealers should vest this person with full responsibility and authority to make and enforce the firm's policies and procedures related to money laundering. The AML Compliance Officer does not need to be the firm's current compliance officer. Some larger firms have placed this responsibility on the firm's risk manager. Firms may, however, consider incorporating AML compliance requirements into the existing duties of a firm compliance officer. Whomever the firm designates as its AML Compliance Officer should have the authority, knowledge, and training to carry out the duties and responsibilities of his or her position.

The AML Compliance Officer should monitor compliance with the firm's AML program and help to develop communication and training tools for employees. The AML Compliance Officer should also regularly assist in helping to resolve or address heightened due diligence and "red flag" issues.

The AML Compliance Officer should ensure that AML records are maintained properly and that SARs are filed as required pursuant to the firm's procedures. In short, the AML Compliance Officer should be the primary contact for the firm on AML compliance implementation and oversight.

Finally, to the extent applicable, the AML Compliance Officer should report to a member of the Board of Directors (or other high level executive officer) on AML compliance issues. This senior officer or director should communicate with firm employees on AML issues to further demonstrate the firm's commitment to AML compliance. The firm's senior management should work with the AML Compliance Officer to help ensure that the firm's AML policies, procedures, and programs meet all applicable government standards and that they are effective in detecting, deterring, and punishing or correcting AML misconduct. The firm's senior management also should work with the AML Compliance Officer to ensure that the AML compliance policies, procedures, and programs are updated and reflect current requirements.

### **Establish An Ongoing Training Program**

The Money Laundering Abatement Act requires firms to develop ongoing employee training programs on AML issues. The AML employee training should be developed under the leadership of the AML Compliance Officer or senior management. Educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos are all appropriate training vehicles for AML training. The training may vary based on the type of firm and its size, its customer base, and its resources. The NASD urges its members to instruct their employees about the following topics, at a minimum:

- how to identify "red flags" and possible signs of money laundering that could arise during the course of their duties;
- what to do once the risk is identified;
- what their roles are in the firm's compliance efforts;
- how to perform their roles;
- the firm's record retention policy; and
- disciplinary consequences, including civil and criminal penalties for non-compliance with the Money Laundering Abatement Act.

The NASD advises its members, *at a minimum*, to implement AML training on an annual basis. Frequent evaluation of training programs may be necessary to ensure that firms are informing employees about any new developments with the rules and regulations. As noted above, firms should update their training materials, as necessary, to reflect new developments in the law. Incorporation of money laundering compliance training into continuing education programs is recommended for both registered representatives and supervisors.

A broker/dealer should scrutinize its operations to determine if there are certain employees who may need additional or specialized training due to their duties and responsibilities. For example, employees in Compliance, Margin, and Corporate Security may need more comprehensive training. The firm should train these employees or have these employees receive the appropriate instruction to ensure compliance with the Money Laundering Abatement Act.

### **Establish An Independent Testing Function**

In addition to the firm's overall supervisory responsibility to ensure that its procedures are being followed properly, broker/dealers must have an independent testing function to review and assess the adequacy of and level of compliance with the firm's AML compliance program. Either member personnel or a qualified outside party may perform the testing function, depending in part on the firm's size and resources. Smaller firms, for example, may consider using a qualified outside party to complete this function or they may find it more cost effective to use appropriately trained firm personnel. If a firm uses internal personnel, sufficient separation of functions should be maintained to ensure the independence of the internal testing personnel.

The independent testing should be performed annually. After a test is complete, the internal testing personnel or qualified outside party should report its findings to senior management or to an internal audit committee, as appropriate. The firm should ensure that there are procedures for implementation of any of the internal testing personnel's or third party's recommendations and corrective or disciplinary action as the case may warrant.

### **INTRODUCING BROKERS AND CLEARING BROKERS**

The NASD wishes to emphasize that both introducing brokers and clearing brokers have responsibilities under the Money Laundering Abatement Act. **All** broker/dealers should devote special attention to potentially high-risk areas for money laundering. Both introducing brokers and clearing brokers must establish and implement the appropriate AML procedures identified above to comply with the Money Laundering Abatement Act's requirements.

In order to detect suspicious activity, it is imperative that introducing and clearing brokers work together to achieve compliance with the Money Laundering Abatement Act. For instance, introducing brokers generally are in the best position to "know the customer," and thus 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.<sup>40</sup> In essence, introducing brokers 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 brokers and, more importantly, satisfy their own obligations under federal law, clearing firms should establish both automated systems to detect suspicious activity and procedures to share AML information and responsibilities with introducing brokers, consistent with the Money Laundering Abatement Act. For example, both the introducing broker and clearing firm may have information concerning a customer relevant to an assessment of whether a wire transfer out of an account to a particular destination raises any AML concerns.

Importantly, introducing brokers 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. Responsibilities relating to AML compliance should be clearly allocated between the parties, and such responsibilities should be specified in the parties' clearing agreements pursuant to NASD Rule 3230. Any such allocation, however, would not relieve either party from its independent obligation to comply with AML laws.

In short, introducing brokers and clearing firms need to work together to allow each firm to meet its obligation to comply with the AML laws.



**CONCLUSION**

As stated above, the NASD will update its guidance as new AML rules and regulations become final. In the interim, the NASD reminds members to comply with the provisions of the Money Laundering Abatement Act that currently apply to broker/dealers. Although the obligation to develop and implement an AML compliance program is not a “one-size-fits-all” requirement, all broker/dealers must have an AML compliance program designed to achieve compliance with the BSA and the regulations promulgated thereunder.

### ENDNOTES

- 1 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
- 2 31 U.S.C. §§ 5311, *et seq.*
- 3 In its proposed rules released in December 2001, Treasury defines “correspondent account” for purposes of broker/dealers as “an account established to receive deposits from, make payments on behalf of a foreign bank, or handle other financial transactions related to such bank.” See 66 Fed. Reg. 67,459 (December 28, 2001). The NASD will keep members apprised of any changes to the definition of “correspondent account” when Treasury releases its final rules in this area. Please also note that Treasury’s definition is different from the definition of correspondent brokerage accounts.
- 4 See 66 Fed. Reg. 67,669 (December 31, 2001). NASD Regulation’s AML Web Page provides links to Treasury’s proposed and final regulations.
- 5 See 66 Fed. Reg. 67,459 (December 28, 2001).
- 6 See 67 Fed. Reg. 9873 (March 4, 2002); 67 Fed. Reg. 9879 (March 4, 2002).
- 7 See *generally Anti-Money Laundering, Efforts in the Securities Industry*, Report to the Chairman, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate, GAO-02-111 (October 2001).
- 8 Title 18 U.S.C. §§ 1956 and 1957 make knowingly engaging in, or attempting to engage in, financial transactions involving the proceeds of certain unlawful activities a criminal offense. Therefore, under the criminal statutes, a person or entity could be prosecuted for assisting or participating in money laundering perpetrated by its customer if the firm (or person) knew or was willfully blind to the fact that the transaction involved illegal funds. Criminal penalties include fines up to \$500,000 or twice the value of the property involved in the transaction, whichever is greater, and prison sentences as long as 20 years. In addition to criminal penalties, violators may face civil penalties up to the greater of the value of the property, funds, or monetary interests involved in the transaction or \$10,000, as well as forfeiture of any property involved in the transaction. The BSA also imposes criminal and civil penalties for violations of the BSA or its implementing regulations. Generally, a person can be subject to a criminal fine of up to \$250,000 or imprisonment of up to 5 years, or both. A person who violates the BSA while violating another law of the United States, or engaging in a pattern of illegal activity, is subject to a criminal fine of up to \$500,000 or imprisonment of up to 10 years, or both. The Money Laundering Abatement Act adds additional criminal and civil penalties that can be up to two times the amount of the transaction, not to exceed \$1,000,000 for violations of certain BSA provisions.
- 9 See *NASD Notice to Members 89-12, Reporting Suspicious Currency and Other Questionable Transactions to the IRS/Customs Hotline*.
- 10 See note 3.
- 11 See 66 Fed. Reg. 67,459 (December 28, 2001).
- 12 See 67 Fed. Reg. 9873 (March 4, 2002); 67 Fed. Reg. 9879 (March 4, 2002).
- 13 See 67 Fed. Reg. 9873 (March 4, 2002); 67 Fed. Reg. 9879 (March 4, 2002).
- 14 See 66 Fed. Reg. 67,459 (December 28, 2001).
- 15 See 66 Fed. Reg. 67,669 (December 31, 2001).
- 16 See File No. SR-NASD-2002-24.
- 17 The U.S. Sentencing Commission Guidelines for organizations set out the following criteria for an effective corporate compliance program: (1) whether the company’s compliance standards and procedures are reasonably capable of reducing the prospect of criminal activity; (2) whether there is oversight of the compliance program by high-level personnel; (3) whether the company exercises due care in delegating substantial authority; (4) whether the company communicates effectively to all levels of employees; (5) whether the company has in place viable systems for monitoring, auditing, and reporting suspected misconduct without fear of reprisal; (6) whether the company enforces compliance standards in a consistent manner using appropriate disciplinary measures; and (7) whether the company has taken reasonable steps to respond to and prevent further similar offenses upon detection of a violation. See also *In Re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996); *McCall V. Scott*, 250 F. 3d 1997 (9th Cir. 2001).
- 18 The New York Stock Exchange (NYSE) has also proposed Rule 445, which mirrors the NASD’s proposed rule. See File No. SR-NYSE-2002-10 (filed with the SEC on February 27, 2002).
- 19 31 U.S.C. § 5318(h) (amended by Section 352 of the Money Laundering Abatement Act).
- 20 See *USA Patriot Act of 2001: Consideration of H.R. 3162 Before the Senate* (October 25, 2001) (statement of Sen. Sarbanes); *Financial Anti-Terrorism Act of 2001: Consideration Under Suspension of Rules of H.R. 3004 Before the House of Representatives* (October 17, 2001) (statement of Rep. Kelly) (provisions of the Financial Anti-Terrorism Act of 2001 were incorporated as Title III in the PATRIOT Act).
- 21 See *Notice to Members 96-32; Notice to Members 96-70; and Notice to Members 99-11*.

## Special NASD Notice to Members 02-21

- 22 Treasury has until October 26, 2002 to promulgate additional customer identification requirements.
- 23 Firms should authenticate customer identity at the time of account opening, and not just when an account shows suspicious activity.
- 24 See *Notice to Members 01-67, Terrorist Activity*. Executive Order 13224 prohibits transactions with those persons and organizations listed on the OFAC Web Site on the SDN List as well as with the listed embargoed countries and regions; See also Section 326 of the Money Laundering Abatement Act. The OFAC Web Site is updated frequently, so members should consult the list on a regular basis. Software programs that allow firms to perform this function in a more user friendly and automated manner are available.
- 25 Note that under the BSA, firms must record a current passport number or other valid government identification number for transfers or transmittals of \$3,000 or more by or for non-resident alien accounts. See 31 C.F.R. 103.33 (2001).
- 26 31 U.S.C. § 5318(k) (amended by Section 319(b) of the Money Laundering Abatement Act).
- 27 31 U.S.C. § 5318(j) (amended by Section 313 of the Money Laundering Abatement Act). Please note that Treasury included a model certification form in its December 2001 rule proposal, available at [www.nasdr.com/money.asp](http://www.nasdr.com/money.asp).
- 28 31 U.S.C. § 5318(i) (amended by Section 312 of the Money Laundering Abatement Act).
- 29 Treas. Dept., Bd. of Gov. of Fed. Res., Comp. Of the Currency, F.D.I.C., O.T.S. and State Dept., *Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Official Corruption*, (Jan. 2001) and at [www.ustreas.gov/press/releases/guidance.htm](http://www.ustreas.gov/press/releases/guidance.htm).
- 30 31 U.S.C. § 5318(i) (amended by Section 312(a)(i)(4)(B) of the Money Laundering Abatement Act).
- 31 31 U.S.C. § 5318(i) (amended by Section 312(a)(i)(3) of the Money Laundering Abatement Act).
- 32 31 U.S.C. § 5318(g).
- 33 Evidence that a broker/dealer knows that the property involved in a financial transaction constitutes the proceeds of unlawful activity and nonetheless conducts (or attempts to conduct) the financial transaction with the unlawful proceeds with the intent to promote the unlawful activity or knowing that the transaction is designed to conceal or disguise the nature, source, or ownership of the unlawful proceeds, can subject a broker/dealer to criminal prosecution. See 18 U.S.C. § 1956.
- 34 66 Fed. Reg. 67,669 at 67,674 (Dec. 31, 2001).
- 35 Firms are also reminded to notify self-regulatory organizations and the SEC if they detect indicators of securities laws violations. Firms should note that there are exceptions to the proposed broker/dealer SAR requirements, including that a broker/dealer is not required to file a SAR to report a possible violation of any of the federal securities laws or rules of a self-regulatory organization by the broker/dealer or any of its officers or directors, employees, or other registered representatives, other than certain rules, so long as such violation is properly reported to the SEC or a self-regulatory organization. See 66 Fed. Reg. 67,669 at 67,676-677 (Dec. 31, 2001).
- 36 The FATF is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering. The FATF monitors members' progress in implementing anti-money laundering measures, reviews money laundering techniques and counter-measures, and promotes the adoption and implementation of anti-money laundering measures globally. See links to the FATF Web Site at [www.nasdr.com/money.asp](http://www.nasdr.com/money.asp).
- 37 See Speech by Lori Richards, Director of Securities and Exchange Commission's Office of Compliance Inspections and Examinations, *Money Laundering: It's on the SEC's Radar Screen* (May 8, 2001); See also SIA, *Preliminary Guidance for Deterring Money Laundering Activity*, at 12-13 (Feb. 2002); Sarah B. Estes, Sutherland, Asbill & Brennan LLP, *Securities Broker-Dealers and Money Laundering: The Obligations of Broker-Dealers Under Money Laundering Laws* at 5-6 (2001).
- 38 Firms may wish to consult FinCEN's Web Site for more information (see [www.treas.gov/fincen](http://www.treas.gov/fincen)), including, annual SAR Activity Review reports and SAR Bulletins, which discuss trends in suspicious activity reporting and give helpful tips.
- 39 See 67 Fed. Reg. 9873 (March 4, 2002).
- 40 All broker/dealers should consider using electronic databases (such as Equifax, Experion, Lexis/Nexis, or other in-house or custom databases) to verify customer identity.

© 2002 National Association of Securities Dealers, Inc. (NASD). All rights reserved. Notices to Members attempt to present information to readers in a format that is easily understandable. However, please be aware that, in case of any misunderstanding, the rule language prevails.



## Annual Conference

Washington, DC May 27-29, 2015

---

### Enhancing Anti-Money Laundering Procedures

Thursday, May 28

11:15 a.m. – 12:15 p.m.

#### Resources

##### FINRA Resources

- *Notice to Members 02-21 (NASD Provides Guidance to Member Firms Concerning Anti-Money Laundering Compliance Programs Required by Federal Law)* (April 2002)

[www.finra.org/sites/default/files/NoticeDocument/p003704.pdf](http://www.finra.org/sites/default/files/NoticeDocument/p003704.pdf)

- Anti-Money Laundering FAQ

[www.finra.org/industry/faq-anti-money-laundering-faq](http://www.finra.org/industry/faq-anti-money-laundering-faq)

- FINRA AML Small Firm Template

[www.finra.org/sites/default/files/Industry/p011419.doc](http://www.finra.org/sites/default/files/Industry/p011419.doc)

##### SEC Resources

- Responses to Frequently Asked Questions about a Broker-Dealer's Duties When Relying on the Securities Act Section 4(a)(4) Exemption to Execute Customer Orders (October 2014)

[www.sec.gov/divisions/marketreg/faq-broker-dealer-duty-section4.htm](http://www.sec.gov/divisions/marketreg/faq-broker-dealer-duty-section4.htm)

- Anti-Money Laundering (AML) Source Tool for Broker-Dealers (June 2012)

[www.sec.gov/about/offices/ocie/amlsourcetool.htm](http://www.sec.gov/about/offices/ocie/amlsourcetool.htm)

- Question and Answer Regarding the Broker-Dealer Customer Identification Program Rule (31 CFR 103.122) (October 2003)

[www.sec.gov/divisions/marketreg/qa-bdidprogram.htm](http://www.sec.gov/divisions/marketreg/qa-bdidprogram.htm)