Outline of Anti-Money Laundering Obligations of Broker-Dealers

Published by the Broker-Dealer & Investment Management Regulation Group
September 2011

The following is a compendium of anti-money laundering requirements applicable to broker-dealers under the Bank Secrecy Act of 1970 ("BSA"),[1] as amended,[2] and related federal and industry guidelines.

[1] Codified at 31 U.S.C. 5311 *et seq*. The regulations implementing the BSA are codified at 31 C.F.R. 103 *et seq*.

[2] Several anti-money laundering acts amend the BSA including, in particular, Title III of the USA Patriot Act of 2001, also referred to as the International Money Laundering Abatement and Financial Anti-Terrorism Act, 2001.

Kathy H. Rocklen
212.969.3755 — krocklen@proskauer.com

Benjamin J. Catalano
212.969.3980 — bcatalano@proskauer.com

I. GENERAL REQUIREMENTS

A. AML Program Components and Documentation

The USA Patriot Act of 2001 ("the Patriot Act"), requires all financial institutions, including broker-dealers, to establish and implement anti-money laundering ("AML") programs designed to achieve compliance with the BSA and the regulations promulgated thereunder. FINRA requires that its members develop and implement written AML programs that, at a minimum:

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 the implementing regulations thereunder;
3. Provide for annual independent testing for compliance to be conducted by member personnel or by a qualified outside party;
4. 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 must be an associated person of the member) and provide prompt notification to FINRA regarding any change in such designation(s); and
5. Provide ongoing training for appropriate personnel.

Each member's AML program must be approved, in writing, by a member of senior management. *[Ref. FINRA Rule 3310]*

B. FINRA Contact System

A broker-dealer must identify, and update the contact information for, its AML compliance officer through the FINRA Contact System ("FCS").[3]
[Ref. FINRA Rule 3310, Supplementary Material .02; NASD Rule 1160]

[3] Broker-dealers must update AML compliance officer information promptly and, in any event, not later than 30 days following any change in such information. In addition, broker-dealers must review and, if necessary, update the contact information within 17

C. Role of the AML Compliance Officer

The duties of a broker-dealer's AML compliance officer should include monitoring the firm's compliance with AML obligations, making and enforcing the firm's policies and procedures with respect to money laundering, ensuring that AML reports are filed as required and that AML records are properly maintained, and developing communication and training systems for employees. The AML compliance officer should keep current on AML issues, review FinCEN[4] advisories regularly for relevant news and updates,[5] and update the firm's AML Program accordingly.

The AML Compliance Officer should have the requisite authority, knowledge, and training to carry out the duties and responsibilities of the position. The AML Compliance Officer should report to a member of the board of directors or other high level executive officer of the broker-dealer with respect to AML compliance issues. *[Ref. NASD NtM 02-21]*

II. REPORTING OBLIGATIONS

A. Currency Transaction Report ("CTR"): Broker-dealers are required to file CTRs with the IRS for transactions in currency exceeding $10,000. As structuring is prohibited, multiple transactions or transactions involving multiple branches of a broker-dealer are considered a single transaction if they amount to more than $10,000 in any one day, and the broker-dealer has knowledge that they are by or on behalf of the same person. A CTR must be filed within 15 days of the transaction, and a copy retained for a period of 5 years. *[Ref. 31 C.F.R. 103.22; 31 C.F.R. 103.27]*

B. Currency and Monetary Instruments Transportation Report ("CMIR"): CMIR is required to be filed with the Bureau of Customs and Border Protection when a broker-dealer imports or exports, other than through the postal service or by common carrier, currency or other monetary instruments[6] in an aggregate amount exceeding $10,000. A CMIR must be filed on the day of shipment of the monetary instruments or within 15 days after receipt of such, if no report was made of their shipment. *[Ref. 31 C.F.R. 103.23; 31 C.F.R. 103.27]*

C. Report of Foreign Bank and Financial Accounts ("FBAR"): A broker-dealer is required to file a FBAR annually with the IRS in respect of any bank, securities or other financial account in a foreign country with assets exceeding $10,000, where the broker-dealer has a financial interest in or signatory or other authority over the account. The form must be filed by June 30 of the succeeding year, and a record of the account information retained for a period of 5 years. *[Ref. 31 C.F.R. 103.24; 31 C.F.R. 103.32]*

---

business days after the end of each calendar year. Broker-dealers must comply with any FINRA request for such information promptly, but in any event not later than 15 days following such request, or such longer period as may be agreed to by FINRA staff. The FCS may be accessed at: https://firms.finra.org/fcs.

[4] The Financial Crimes Enforcement Network ("FinCEN") is the bureau of the Treasury Department charged with administering the BSA.

[5] Available at: http://www.fincen.gov/news_room/advisory/.

[6] Monetary Instruments include traveler's checks, negotiable instruments (checks, promissory notes, money orders) in bearer form or endorsed without restriction, and securities or stocks in bearer form.

D. Suspicious Activity by the Securities and Futures Industries ("SAR-SF"): A SAR-SF is required to be filed with FinCEN in respect of any transaction[7] conducted or attempted to be conducted through a broker-dealer that involves at least $5,000 in funds or other assets and that the broker-dealer knows, suspects or has reason to suspect:

- involves funds derived from illegal activity or is conducted in order to hide funds or assets derived from illegal activity;
- is designed, whether through structuring or otherwise, to evade BSA requirements;
- serves no business or lawful purpose or is not of the sort in which the customer would normally be expected to engage, and the broker-dealer knows of no reasonable explanation for the transaction after examining the available facts;
- involves the use of the broker-dealer to facilitate criminal activity.

A SAR must be filed within 30 days of detection of a suspicious transaction, or within a further 30 days if an extension is needed to enable identification of a suspect. The broker-dealer must retain a copy of the SAR and any supporting documentation, properly identified as such, for a period of 5 years.

Although each broker-dealer involved in a suspicious transaction has an obligation to report it, only one SAR need be filed for any transaction.[8] Broker-dealers and their employees must not disclose to anyone that a SAR has been filed.[9]
[Ref. 31 C.F.R. 103.19; NASD NtM 02-21]

E. Report of Blocked or Rejected Transactions

A Report of Blocked Transactions (or Report of Rejected Transactions) is required to be filed with OFAC if a broker-dealer blocks (or rejects) a transaction of a customer, or person with or for whom a customer is transacting business, as a result of that person being confirmed a valid OFAC match.[10] Such a report must be filed within ten business days of the blocking or rejection.[11] Copies of rejected transactions reports must be

---

7 The rule also covers series of transactions if, taken together, they form a suspicious pattern of activity.

8 FinCEN anticipates that introducing and clearing firms will share information with each other in respect of any given transaction and determine which firm will file a SAR.

9 The person involved in the transaction that is subject of the report must not be notified of the SAR. If subpoenaed, the broker-dealer must refuse to provide the information and notify FinCEN of the request. Where two or more broker-dealers are filing one SAR-SF, the confidentiality provisions apply equally to each broker-dealer participating in the transaction, and not just the broker-dealer that filed the SAR-SF.

10 The Office of Foreign Assets Control ("OFAC") publishes, and updates on a regular basis, a Specially Designated Nationals and Blocked Persons List ("SDN List"), that lists individuals and entities that have connections with countries against which it administers sanctions, together with lists of specially designated terrorists, narcotics traffickers and embargoed countries, governments and regions (collectively, "the OFAC list"). A broker-dealer may not open an account for a person named on the OFAC list; and must search its customer database for potential matches each time the OFAC list is updated. The broker-dealer also must search the OFAC list for potential matches each time it effects a transaction involving a person who is not an existing customer of the broker-dealer. If a potential match is indicated, the broker-dealer must perform additional due diligence to determine if an actual match exists. If an actual match is determined, appropriate action must be taken to block the customer's account and/or block (or reject) the transaction.

11 In some cases, an underlying transaction may be prohibited, but there is no blockable interest in the transaction (*i.e.*, the transaction should not be accepted, but there is no OFAC requirement to block the assets). In these cases, the transaction is simply rejected, or not processed. For example, the Sudanese Sanctions Regulations prohibit transactions in support of commercial activities in Sudan. A U.S. financial institution would have to reject a wire transfer between two third-country companies (non-SDNs) involving an export to a non-SDN company in Sudan because, whilst there is no interest of the Government of Sudan or an SDN and, therefore, no blockable interest in the funds, the transaction would constitute a transaction in support of a commercial activity in Sudan, which is prohibited.

retained for a period of five years. Copies of blocked transactions reports must be retained for the period the property is blocked and for five years after the property is unblocked.
[Ref. Foreign Assets Control Regulations for the Securities Industry, OFAC Industry Brochure (Apr. 29, 2004)]

F. Annual Report of Blocked Property

If a broker-dealer holds an account for a person who is confirmed a valid OFAC match, it must immediately block the account such that only OFAC-authorized debits may be made. The blocked account must be clearly labeled as such, and established in the name of, or contain a means of clearly identifying the interest of, the individual or entity subject to the blocking. Similarly, the broker-dealer must transfer any blocked transaction funds into a blocked account. It must file with OFAC, by September 30 each year, an annual report of all blocked property held as of June 30, and retain a copy of the report for the period the property is blocked and for five years after the property is unblocked.
[Ref. Foreign Assets Control Regulations for the Securities Industry, OFAC Industry Brochure (Apr. 29, 2004)]

G. Emergency Reporting to the Government by Telephone

A broker-dealer is required to immediately contact federal law enforcement by telephone[12] in situations involving violations that require immediate attention, including where:

- 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 the broker-dealer to open an account or proceed with a suspicious or unlawful activity or transaction;
- Any other situation that the broker-dealer reasonably determines requires immediate government intervention. *[Ref. 31 C.F.R. 103.19(b)(3)]*

III. RECORDKEEPING REQUIREMENTS

A. For **Purchases of Bank Checks and Drafts, Cashier's Checks, Money Orders and Traveler's Checks for $3,000 or More in Currency,** a broker-dealer must obtain certain information[13] from, and verify the identification of, the purchaser. No report is required, but a record of the information must be retained for 5 years.
[Ref. 31 C.F.R. 103.29]

B. For **Extensions of Credit Greater than $10,000 (Unsecured),** a broker-dealer must retain for 5 years a record of the name and address of the recipient, the date, the amount extended and the nature or purpose thereof.
[Ref. 31 C.F.R. 103.33(a); 31 C.F.R. 103.38(d)]

---

[12] In August 2008, the Securities and Exchange Commission ("SEC") introduced a centralized phone line for broker-dealers to alert the SEC to the filing of a SAR that may require immediate attention by the SEC. Firms may, but are not required to, contact the SEC in such instances. Calling the *SEC SAR Alert Message Line* does not relieve the broker-dealer of its obligation to file a SAR or to notify an appropriate law enforcement authority.

[13] The information varies depending on whether or not the purchaser has an account with the broker-dealer. Multiple purchases must be aggregated if the broker-dealer knows they are by the same person.

C. For **Transfers of Currency, Checks, Securities or Credit Greater than $10,000 Into or Outside of the U.S.**, a broker-dealer must retain for 5 years a record of the advice, request or instruction resulting in or intended to result in such transfer. *[Ref. 31 C.F.R. 103.33(b) & (c); 31 C.F.R. 103.38(d)]*

D. For **Transfers of $3,000 or More Under the Joint and Travel Rules,** a broker-dealer must retain for 5 years a record of the following information regarding the transmittal:

- the original or copy transmittal order;
- the name and address of the transmitter, amount, execution date, payment instructions and identity of the recipient's financial institution;
- the name, address, account number and any other identifying information of the recipient;
- any form relating to the transmittal that is completed or signed by the person placing the transmittal order.[14]

[Ref. 31 C.F.R. 103.33(f) & (g) & 31 C.F.R. 103.38(d)]

IV. SHARING OF INFORMATION WITH FEDERAL LAW ENFORCEMENT AGENCIES AND OTHER FINANCIAL INSTITUTIONS

A. Responding to FinCEN Requests under Section 314(a) of the PATRIOT Act

Federal law enforcement agencies investigating terrorist activity or money laundering may request that FinCEN solicit certain information from financial institutions, including broker-dealers. FinCEN sends information requests to designated contacts[15] at financial institutions once every 2 weeks. Upon receipt, a broker-dealer is required to search its records for any accounts maintained by a named suspect during the preceding 12 months, and any transactions conducted by or on behalf of the suspect during the preceding 6 months.[16] If the broker-dealer identifies a pertinent account or transaction, it must report to FinCEN as soon as possible and, in any event, no later than 2 weeks from the date of transmission of the request:

- the identity of the individual, entity, or organization;
- the account number or date and type of transaction; and
- all identifying information provided by the suspect when the account was established or the transaction conducted.

---

[14] 31 C.F.R. 103.33(f) contains detailed procedures for verifying the identity of transmitters/ recipients who are not established customers of the broker-dealer, and for retrieving records. 31 C.F.R. 103.33(g) specifies the information that transmitting and intermediary institutions must provide in transmittal orders. Transfers between domestic financial institutions as transmitter and recipient are excluded from the Rule.

[15] A broker-dealer must identify to FinCEN its designated point of contact person for receiving section 314(a) requests, and make any changes thereto by updating its Anti-Money Laundering Compliance Contacts (Primary and Alternate) in the FINRA Contact System.

[16] The broker-dealer may contact the specified federal law enforcement agency with any questions regarding the scope or terms of the request.

The broker-dealer must have procedures in place for handling requests and providing information, and for protecting the security and confidentiality thereof.[17] If a search does not uncover any matching of accounts or transactions, the broker-dealer is instructed not to reply to the section 314(a) request.
[Ref. 31 C.F.R. 103.100; FinCEN News Release 02/06/2003; Changing Your Point of Contact for 314(a), FinCEN Release 02/05/2008]

B. Voluntary Information Sharing With Other Financial Institutions under Section 314(b) of the PATRIOT Act

The PATRIOT Act encourages information sharing among financial institutions for the purpose of identifying and reporting activities that may involve terrorist financing or money laundering. If a broker-dealer intends to engage in information sharing, it must file an annual notification to that effect with FinCEN, and confirm that it has established adequate procedures to safeguard the security and confidentiality of the shared information. Prior to sharing any information, the broker-dealer must verify that its counterpart financial institution has also filed a notification with FinCEN.[18] Proof of such verification should be retained by the broker-dealer.
[Ref. 31 C.F.R. 103.110; NASD NtM 02-21]

C. The 120 Hour Rule

Section 319(b) of the PATRIOT Act requires that certain financial institutions, including broker-dealers, comply, within 120 hours, with any Federal banking agency request for information and documentation concerning any account opened, maintained, administered or managed in the U.S. by that financial institution.

V. CUSTOMER IDENTIFICATION PROGRAM ("CIP")

A broker-dealer is required to establish and maintain a written Customer Identification Program ("CIP"), appropriate for its size and business. The broker-dealer must employ risk-based procedures for verifying the identity of its customers so that it can form a reasonable belief that it knows the true identity of each customer. The procedures must be based on the broker-dealer's assessment of the risks applicable to its business, including those presented by the types of accounts[19] maintained, the methods of opening accounts, the types of identifying information available, and the broker-dealer's size, location and customer base.
[Ref. 31 C.F.R. 103.122; NASD NtM 03-34; NASD NtM 02-21]

A. Required Documentation

The CIP should contain procedures for account opening that specify the identifying information that will be sought for each type of account maintained by the broker-dealer:

---

[17] The broker-dealer will satisfy its obligations in this regard if it applies to the information those procedures that it has established under section 501 of the Gramm-Leach-Bliley Act regarding the protection of its customers' non-public personal information. The broker-dealer must not disclose to any person, other than FinCEN or the federal law enforcement agency on whose behalf FinCEN is requesting information, that FinCEN has requested or has obtained information. If the broker-dealer is authorized to share information with other financial institutions (see Section IV.B.), it may share information concerning an individual, entity, or organization named in a FinCEN request, but such sharing must not disclose the fact that FinCEN has requested information concerning such individual, entity, or organization.

[18] It may do this by confirming that the other financial institution appears on the section 314(b) list published quarterly by FinCEN, or by requesting a copy of FinCEN's Confirmation of the Notice of Intent to Share Information directly from the other financial institution.

[19] An account is defined broadly as any formal relationship to effect securities transactions. The definition encompasses retail, cash, margin and institutional accounts as well as non-account relationships including transactions with counterparties and the provision of certain investment banking services.

ERISA and Non-ERISA Employee Benefit Accounts (the customer is the employer contracting with the broker-dealer)

- Business name
- Business address/principal place of business
- Taxpayer identification number
- Certificate of incorporation, business license, partnership agreement or trust instrument

U.S. and Non-U.S. Individuals

- Name and date of birth
- Residential or business street address
- Identification number (taxpayer identification number for U.S. persons; passport number, alien identification card number or other unexpired government ID for non-U.S. persons)
- Unexpired government-issued photo ID

Joint and Multiple Accounts

- Name and date of birth of each individual owner
- Residence or business address/principal place of business of each individual owner
- Identification number (taxpayer identification number, passport number, alien ID card number or other unexpired government ID) for each individual owner
- Unexpired government-issued photo ID, certificate of incorporation, business license, partnership agreement or trust instrument for each individual owner

Accounts for Minors/Custodial Accounts

- Information for the individual opening the account (the custodian) until the minor reaches the age of majority, then the broker-dealer must verify his/her identity when he/she seeks to set up a new account

Accounts for Entities (Corporations, Partnerships, Limited Liability Companies, Sole proprietorships, Subsidiaries and Affiliates)[20]

- Entity name
- Business address/principal place of business
- Entity's employer identification number ("EIN") (As there is no uniform identification number for non-U.S. entities, the broker-dealer may choose from a variety of identification numbers, so long as the number allows it to reasonably establish the true identity of the customer)

[20] Certain U.S. entities, including financial institutions regulated by a Federal functional regulator and certain publicly listed companies, are excluded from CIP requirements.

- Certificate of incorporation, business license, partnership agreement or trust instrument
- Foreign entities may add references such as a bank reference

U.S. and Non-U.S. Non-Operating Entities (Personal Investment Vehicles (PIVs) such as, personal holding companies, personal investment companies, international business corporations, trusts, partnerships, LLCs, and special purpose vehicles) (PIVs are organized to carry out the investment or trading activity of the beneficial owners of the entity and do not operate in a commercial capacity)

- Entity name
- Business address/principal place of business
- Taxpayer identification number
- Certificate of incorporation, business license, partnership agreement or trust instrument
- Foreign entities may add references such as bank reference
- The broker-dealer may also want to look through the entity to identify and verify the beneficial owners or control persons

Trusts

The trust is considered the customer for CIP purposes. However, depending on the risk assessment, procuring information regarding the individuals with control or authority over the account may be necessary. Where the trust is a revocable trust, information regarding the settlor, grantor, trustee or other persons with the authority to direct the trustee, and who thereby have authority or control over the account, may be required.

- Trust name
- Trust instrument

U.S. and Non-U.S. Unregistered Investment Companies (UICs) (hedge funds, private equity funds, venture capital funds and REITs)

- Formation documents
- Offering memorandum
- Operating agreement
- Subscription agreement
- Name of the general partner, management company, investment manager of the investment adviser and/or members of the board or principals

[Ref. Suggested Practices for Customer Identification Programs, Anti-Money Laundering Committee of the Securities Industry Association]

B. Verification of Identity

1. Documentary/Non-Documentary Methods

The CIP must contain procedures for verifying the identity of each customer either before the account is opened or within a reasonable period thereafter.[21] It must describe when the broker-dealer will use documentary methods, non-documentary methods, or a combination of both to verify customers' identities. The CIP must specify the documents that the broker-dealer will use for verification. These documents may include, in respect of an individual, an unexpired government-issued photograph identification evidencing nationality or residence (such as a driver's license or passport), and for an entity, a certificate of incorporation, business license, partnership agreement or trust instrument.

The CIP also must specify the non-documentary methods that will be used for verification, and the situations in which non-documentary methods may be required. Non-documentary methods may include:

- contacting a customer;
- comparing information provided by the customer against information provided by consumer reporting agencies or other public databases;
- checking references with other financial institutions; or
- obtaining financial statements.

Non-documentary methods must be used where:

- an individual is unable to present an unexpired government issued ID that bears a photograph or similar safeguard;
- the broker-dealer is not familiar with the documents presented;
- the account is opened without documentation;
- the customer opens the account without appearing in person;
- any other circumstances that increase the risk that the broker-dealer will be unable to verify the true identity of a customer through documents.

The CIP must 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 the individuals having authority or control over the account. This verification method applies only where the broker-dealer cannot verify the customer's true identity using the methods described above.

2. Risk-Based Procedures

A risk-based approach provides a framework for identifying the degree of potential money laundering risk associated with customers and transactions, and enables the broker-dealer to focus on those customers and transactions that potentially pose the greatest risk of money laundering. In developing its CIP, a broker-dealer should first conduct a risk assessment of its operations. If heightened risks are identified, the broker-dealer should then document the additional diligence procedures to be applied in respect of those customers or situations.[22]

---

[21] FINRA proposes that verification should take place within 5 business days after the opening of the account. (NASD NtM 02-21)

[22] While the risk assessment is initially performed as part of the CIP, for some customers, a comprehensive risk profile may only become evident once the customer begins transacting through the account, making monitoring of customer transactions and on-going reviews a fundamental component of the risk-based approach.

Country/Geographic Risk

Geographic locations that pose a heightened risk of money laundering would include:

- Countries subject to sanctions, embargoes or similar measures issued by OFAC or the United Nations;
- Countries lacking appropriate AML laws and other measures, as identified by Treasury through FinCEN, or the Financial Action Task Force on Money Laundering ("FATF");[23]
- Countries identified as providing funding or support for terrorist activities that have designated terrorist organizations operating within them;
- Countries identified as having significant levels of corruption or other criminal activity;
- Domestic high-risk geographic locations (high intensity drug trafficking areas or high intensity financial crime areas).

Customer Risk

Categories of customers whose activities might indicate a higher risk would include:

- Customers conducting their business relationship or transactions in unusual circumstances, including:
  - significant and unexplained geographic distance between the broker-dealer and the location of the customer;
  - frequent and unexplained movement of accounts to different financial institutions;
  - frequent and unexplained movement of funds between financial institutions in various geographic locations;
- Customers where the structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests;
- Customers who by virtue of their business or occupation pose a specific risk including, in particular, cash (and cash equivalent) intensive businesses such as money services businesses (e.g. currency exchanges, casas de cambio, or other businesses offering money transfer facilities), casinos or other gambling related activities, or businesses that generate substantial amounts of cash for certain transactions;
- Charities and other 'not for profit' organizations that are not subject to monitoring or supervision, especially those operating on a cross-border basis;
- Gatekeepers such as accountants, lawyers, or other professionals holding accounts on behalf of their clients, where unreasonable reliance is placed on the gatekeeper;
- Use of intermediaries within the relationship who are not subject to adequate AML laws and measures and who are not adequately supervised;

[23] FATF is an intergovernmental organization whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing.

- Senior foreign political figures or their family members or close associates (commonly known as Politically Exposed Persons (PEPs)).

Product/Service Risk

Potential higher risk products/services would include:

- International correspondent banking services involving transactions such as commercial payments for non-customers (for example, acting as an intermediary bank);
- International private banking services;
- Services that inherently have provided more anonymity or can readily cross international borders, such as private investment companies and trusts, online services and international wire transfers.

The broker-dealer may also take into account risk variables specific to a particular customer or transaction, such as:

- the purpose of an account or relationship;
- the level of assets to be deposited by the customer or the size of transactions undertaken. Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of customers with a similar profile may indicate that a customer not otherwise seen as higher risk should be treated as such;
- the level of regulation or other oversight or governance regime to which a customer is subject;
- the regularity or duration of the relationship. Long standing relationships involving frequent customer contact may present less risk from a money laundering perspective;
- the use of intermediate corporate vehicles or other structures that have no apparent commercial or other rationale or that unnecessarily increase the complexity or otherwise result in a lack of transparency. The use of such vehicles or structures, without an acceptable explanation, increases the risk.

The broker-dealer should implement appropriate measures and controls to mitigate the potential money laundering risks of those customers that are determined to be higher risk as the result of the firm's risk-based approach. These measures and controls may include:

- Increased awareness by the broker-dealer of higher risk customers and transactions;
- Increased levels of 'Know Your Customer' or enhanced due diligence;
- Escalation for approval of the establishment of an account or relationship;
- Increased monitoring of transactions;
- Increased levels of ongoing controls and frequency of reviews of relationships.

Where possible, the procedures setting out how a broker-dealer will manage its money laundering and terrorist financing risks should be documented on a group-wide basis.
[Ref. Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing (High Level Principles And Procedures), FATF (June 2007)]

3. Notification to Customers

The CIP must include procedures for providing customers with notice that the broker-dealer is requesting information to verify their identities. This may encompass notices posted in the offices of the broker-dealer, notices inserted on account applications, or web site notices.

4. Lack of Verification

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

- when the broker-dealer should not open an account;
- the terms under which the broker-dealer may execute transactions whilst it attempts to verify a customer's identity;
- when the broker-dealer should close an account after attempts to verify a customer's identity fail;
- when a SAR should be filed.

C. Consulting Government Provided Lists of Known or Suspected Terrorists

The CIP must include procedures for determining, within a reasonable period of time after an account is opened (or earlier, if required by federal law), whether a customer appears on any list of known or suspected terrorists or terrorist organizations issued by any federal agency and by the Treasury Department in consultation with the SEC.[24]

D. Coordination with Other Financial Institutions

1. Reliance on Another Financial Institution to Perform All or Part of the CIP

The CIP may include procedures specifying when the broker-dealer will rely on the performance by another financial institution (including an affiliate) of any element of the broker-dealer's CIP. This may include circumstances in which the other financial institution is opening an account for a customer, or where it is already providing financial services to such customer. Reliance must be reasonable under the circumstances, and the other financial institution must be regulated by a Federal functional regulator and have established AML procedures. In addition, the other financial institution must enter into a contract with the broker-dealer that requires it to certify annually that it has implemented its AML program and that it will perform specified requirements of the broker-dealer's CIP.

2. Introducing/Clearing Firm Relationships

In fully disclosed clearing arrangements in which the functions of opening and approving customer accounts and directly receiving and accepting orders from the introduced customer are allocated exclusively to the introducing firm, and the functions of extending credit, safeguarding funds and securities, and issuing confirmations and statements are allocated to the clearing firm, only the introducing firm will be responsible for CIP requirements with respect to the introduced customers.
[Ref. FinCEN Guidance - FIN-2008-G002, Mar. 4, 2008]

[24] At present, there are no designated government lists to verify specifically for CIP purposes. Comparison to the OFAC list is a separate and distinct requirement.

E. Recordkeeping

The CIP must include procedures for making and maintaining a record of all information obtained during the account opening process. Records of all identification information obtained from a customer must be retained for 5 years after the account has been closed. Records of the following documents must be retained for 5 years from the time that they were created:

- any document that was relied upon to verify identification;
- a description of any non-documentary procedures used to verify identification and the results of those procedures;
- a description of the measures used to verify the identity of individuals with authority or control over accounts, and the results of those measures;[25]
- a description of the resolution of each substantive discrepancy discovered when verifying identifying information.

VI. CONTINUING DUE DILIGENCE - MONITORING ACCOUNTS FOR SUSPICIOUS ACTIVITY/RED FLAGS

Broker-dealers must monitor accounts on an on-going basis for suspicious activity that might indicate money laundering. A broker-dealer should have automated systems in place to monitor trading, wire transfers and other account activity so as to detect when suspicious activity is occurring. If the broker-dealer monitors customer accounts manually, it must review a sufficient amount of account activity to allow identification of patterns of activity, new patterns or patterns that are inconsistent with the customer's financial status or that make no economic sense.

The Broker-dealer's procedures should contain appropriate examples of "red flags"[26] and contain lists of high-risk customers so that employees may identify circumstances in which additional due diligence is required. The Broker-dealer's procedures also should identify all situations in which the firm's AML compliance officer is required to be notified. *[Ref. NASD NtM 02-21]*

VII. SPECIAL DUE DILIGENCE PROGRAMS FOR SELECT ACCOUNTS

A. Correspondent Accounts for Foreign Financial Institutions

A foreign correspondent account is an account established to receive deposits from, make payments on behalf of, or handle other financial transactions for a foreign financial institution. For broker-dealers, this means any formal relationship established to provide regular services to effect transactions in securities, including, but not limited to, the purchase or sale of securities and securities loaned and borrowed activity, and to hold securities or other assets for safekeeping or as collateral. A broker-dealer must establish a due diligence program for all foreign correspondent accounts that encompasses appropriate, specific, risk-based and, where necessary, enhanced policies, procedures and controls to detect money laundering. The due diligence program must assess the money laundering risk posed by each correspondent account on the basis of all relevant factors, including:

---

[25] See section V.B.1. above.

[26] FINRA has provided its members with extensive guidance on money laundering red flags. (*See* NASD NtM 02-21)

- the nature of the foreign financial institution's business and the markets it serves;
- the type, purpose and anticipated activities of the account;
- the nature and duration of the broker-dealer's relationship with the foreign financial institution and its affiliates;
- the AML regime of the jurisdiction that issued the foreign financial institution's license; and
- the foreign financial institution's AML record.

The broker-dealer must then apply risk-based controls to each correspondent account, including periodic reviews to determine whether activity is consistent with the type, purpose and anticipated activity of the account. The program must include special procedures for when the broker-dealer cannot perform due diligence with respect to an account, including procedures for refusing to open an account, suspending an account, filing a SAR, and closing an account.

So-called 'special correspondent accounts' are accounts of foreign banks that operate under off-shore banking licenses, licenses issued by countries that have been designated non-cooperative with respect to international AML laws,[27] or licenses issued by countries that have been designated by the Treasury Department as warranting special concerns on money laundering. A broker-dealer must implement additional enhanced due diligence measures with respect to such accounts that include:

- ascertaining for foreign banks whose shares are not publicly traded, the identity of each of the owners and the nature and extent of their ownership (identifying all 10% holders);
- conducting enhanced scrutiny of the account;
- determining whether the foreign bank in turn maintains correspondent accounts for other foreign banks and, if so, identifying those banks and conducting related due diligence in respect thereof.

[Ref. 31 C.F.R. 103.176]

B. Private Banking Accounts for Non-U.S. Persons/Foreign Officials

A broker-dealer must adopt due diligence procedures to detect money laundering in private banking accounts[28] of non-U.S. persons. The procedures must enable the broker-dealer to:

- ascertain the identity of the nominal and beneficial owners of an account and the sources of funds deposited into the account;
- conduct enhanced scrutiny of any such account that is maintained by a senior foreign political figure, or any immediate family member or close associate of such individual, with a view towards detecting and reporting transactions that may involve the proceeds of foreign corruption.

Procedures for refusing to open an account, suspending an account, filing a SAR, and closing an account must also be established.

---

[27] FATF is the only intergovernmental organization of which the U.S. is a member that currently designates countries as noncooperative with international AML standards. The U.S. has concurred with all designations made to date.

[28] An account with a minimum deposit requirement of $1 million on behalf of one or more beneficial owners and being administered, in whole or in part, by an employee of the broker-dealer.

C. Foreign Shell Banks

Section 313 of the PATRIOT Act prohibits financial institutions, including broker-dealers, from maintaining correspondent accounts for, or on behalf of, foreign shell banks (a foreign bank with no physical presence in any country). Broker-dealers must have procedures in place to ensure that they are not indirectly providing correspondent banking services to foreign shell banks through foreign banks with which they maintain correspondent relationships. A broker-dealer that operates correspondent accounts should obtain certification from each foreign bank, at least once every two years, confirming that it is not a shell bank and that it is not using its correspondent account for shell banks. The broker-dealer must retain all documents provided by a foreign bank upon which it has relied for 5 years after the foreign bank has closed all of its correspondent accounts with the broker-dealer.
[Ref. 31 C.F.R. 103.177; NASD NtM 02-21]

VIII. AML TRAINING

The PATRIOT Act requires broker-dealers to develop ongoing employee training on AML matters. Training programs should be developed under the leadership of the broker-dealer's AML compliance person or senior management, and may vary based upon the type of firm, its size and its customer base. FINRA provides guidance to broker-dealers with respect to the content of training programs, frequency of training, supplementary training for designated employees, and updating of training programs in accordance with developments in AML law. *[NASD NtM 02-21]*

IX. INDEPENDENT TESTING OF BROKER-DEALER PROCEDURES

Broker-dealers are required to implement an independent audit function to test the effectiveness of their AML procedures. FINRA has instructed its members on the criteria for establishing auditor independence, and on the requisite frequency for testing.[29] Audit findings should be reported to senior management of the broker-dealer, and procedures should be in place for implementing any recommendations.
[Ref. FINRA Rule 3310 and Supplementary Material .01]

* * *

Please contact us if you would like to discuss the issues raised herein in more detail.

[29] FINRA requires that testing be performed annually, or more frequently if circumstances warrant.