



**NFA Self-Exam Checklist - Appendix A  
Anti-Money Laundering Questionnaire**

**2010**

## **Appendix A - Anti-Money Laundering Questionnaire**

Each National Futures Association (“NFA”) Member firm must adopt a written anti-money laundering (“AML”) program tailored to its operations. NFA has developed the following questionnaire to assist firms in meeting that requirement.

The firm should maintain its AML program with other firm procedures. Having a written program is not enough to meet your regulatory requirements, however. You must also implement and follow the program and communicate it to your employees.

Please also consult the following NFA Rule and Interpretive Notice when designing your AML program:

<http://www.nfa.futures.org/nfamanual/NFAManual.aspx#2-9>

<http://www.nfa.futures.org/nfamanual/NFAManual.aspx#45>

A Member firm’s written AML program should answer all of the following questions as completely as possible. Although you may answer “not applicable” to particular questions, you should carefully consider the firm’s operations before doing so.

### **General Questions**

- What is the firm’s policy statement regarding money laundering and terrorist financing?
- What are the consequences if an employee does not follow the firm’s AML policy?
- Who in senior management is responsible for giving written approval of the firm’s AML program?
- Has the firm designated one or more individuals to be responsible for overseeing the day to day operations of the firm’s AML compliance program? Who has the firm designated?
- Does the AML Compliance officer/department report to senior management? If so, who do they report to?
- What are the AML Compliance Officer’s duties and responsibilities?

### **Customer Identification Program (CIP)**

- What identifying information (e.g., name, address, date of birth, tax identification number) does the firm obtain from its new customers?
- Does the firm rely on documentary methods to verify identity? If so:
  - What documents does the firm accept to verify the identity of new customers who are individuals? Be specific.

- What documents does the firm accept to verify the identity of new customers that are not individuals (e.g., corporations, partnerships, trusts)? Be specific.
- Does the firm rely on non-documentary methods to verify identity? If so, what non-documentary methods does the firm use to verify a customer's identity? Be specific.
- Under what circumstances will the firm verify identity:
  - Using documentary methods alone?
  - Using non-documentary methods alone?
  - Using a combination of both methods?
- Does the firm require non-documentary methods in the following situations:
  - The customer is unable to present a current government ID with a photograph or similar safeguard (e.g., a thumbprint)?
  - The firm is not familiar with the documents the customer provides?
  - The firm opens an account without obtaining documents from the customer?
  - A customer opens an account without appearing in person?
  - Other circumstances that increase the risk that the firm will be unable to verify the identity of the customer through documents?

If the firm does not use non-documentary methods in one or more of these situations, why has the firm concluded that non-documentary methods are not necessary?

- What is the firm's deadline for completing the verification process? How does the firm ensure that the customer's identity is verified within a reasonable time before or after the account is opened?
- Does the firm accept individual accounts from people who are applying for taxpayer identification numbers? If so, how does the firm confirm that an application for taxpayer identification number has been filed? How does the firm ensure that it obtains the taxpayer identification number within a reasonable period of time?
- Under what circumstances will the firm require customers that are not individuals (e.g., corporations, partnerships, trusts) to provide information about the account controller in order to verify the customer's identity?
- How does the firm handle an account if the firm does not have a reasonable belief that it knows the customer's identity? Specifically:
  - When will the firm refuse to open an account?

- What restrictions does the firm place on customer transactions while the firm is still verifying the customer's identity?
- Under what circumstances will the firm close an account after the firm's attempts to verify the customer's identity have failed?
- In what situations will the firm file a suspicious activity report?
- Does the firm rely on other financial institutions to carry out its CIP requirements? If so, answer the following questions for each financial institution the firm intends to rely upon:
  - What is the financial institution's name?
  - When will your firm rely on that financial institution to perform some or all elements of the CIP for your firm? If it will perform only some elements, which ones are they?
  - What steps did your firm take to ensure that the financial institution is required to have an AML Compliance program under the Bank Secrecy Act?
  - What Federal agency regulates the financial institution?
  - When did your firm enter into a written agreement with the financial institution requiring it to certify annually that it has implemented an AML program and that it will perform the specified requirements of its own CIP or perform the CIP functions described in the agreement? (You should attach the agreement to the firm's AML procedures.)
  - How does your firm ensure that it obtains a copy of the annual certification?
- Does the firm contractually delegate its CIP functions to other entities? If so, answer the following questions for each entity (including any financial institution not included above) that the firm intends to contractually delegate those functions to:
  - What is the entity's name?
  - What elements of the firm's CIP are delegated to that entity?
  - When did you enter into a written agreement outlining each party's responsibilities? (You should attach the agreement to the firm's AML procedures.)
  - What does your firm do to monitor how the other entity implements the CIP and how effective the CIP is?
  - How does your firm ensure that regulators are able to obtain information and records relating to the CIP performed by that entity?
- How does your firm notify customers about why the firm requests information to verify identity before opening an account? What does the notice say?
- Where, in what form, and for what time period does the firm keep the following information:
  - Identifying information collected from customers (e.g., name, address, date of birth, tax identification number)?

- Documents used to verify identity? Does the firm keep a copy of the documents or does it record the necessary information (e.g., identification number, place issued, date issued, expiration date)?
- Descriptions of the methods used and results obtained when non-documentary methods are used to verify identity?
- Descriptions of how discrepancies in particular customers' verifying information are resolved?

### **Identifying High-Risk Accounts**

- How does the firm identify potentially high-risk accounts?
- What types of accounts does the firm characterize as high risk?
- How does the firm determine whether a customer/prospective customer appears on OFAC's list of Specially Designated Nationals and Blocked Persons (SDN Report) identifying known or suspected terrorists and terrorist organizations?
- How does the firm determine whether a customer is located in a country on OFAC's list of sanctioned countries?
- How does the firm determine whether a customer appears on any list of known or suspected terrorists or terrorist organizations that is issued by the Federal Government and designated by the Treasury Department? How does the firm ensure that it follows all Federal directives issued in connection with the list? (Note: No other lists or federal directives have yet been issued).
- How does the firm determine whether a customer is from a country that appears on FATF's list of uncooperative countries (NCCT list)?
- What kind of due diligence does the firm perform to determine whether to accept a high risk account?
- How does the firm determine whether additional monitoring of account activity is necessary for a high risk account?
- What additional monitoring does the firm perform for account activity in high risk accounts?
- What special steps will the firm take if the customer/prospective customer or its country appears on the following lists:
  - OFAC's SDN Report?
  - OFAC's list of sanctioned countries?
  - A list of known or suspected terrorists or terrorist organizations issued by the Federal Government?
  - FATF's NCCT list?

## **Suspicious Activity**

- What systems and procedures does the firm use to detect and report suspicious activity:
  - During the account opening process?
  - While an account is open?
  - When an account closes?
- What type of transactions will require the firm to file a form SAR-SF?
- How does the firm monitor wire transfer activity for unusual transfers (e.g., unexpected or unusually frequent or large transfers by a particular account during a particular period, transfers involving certain countries identified as high risk or uncooperative)?
- What examples of “red flags” does the firm provide its employees to alert them to suspicious activity?
- What kind of investigation does the firm do when a red flag occurs? Who does it?
- How promptly must employees report potential suspicious activity and who do they report it to?
- Which supervisory personnel evaluate the activity and determine whether the firm is required to file a Suspicious Activity Report (i.e., SAR-SF) with FinCEN?

## **Other**

- If your firm is an FCM, what steps does the firm take to respond to FinCEN information requests (e.g., 314(a) biweekly request)?
- If responsibilities for conducting AML compliance, other than CIP responsibilities, are divided between your firm and an FCM or IB, what documentation does your firm maintain to indicate how those responsibilities are divided? How does the firm ensure the other firm is adhering to the AML procedures?
- If your firm is an FCM that guarantees introducing brokers (“GIB”), how does it ensure that the firm’s GIBs are adhering to their AML procedures?
- If your firm is an FCM, how does your firm comply with the currency transaction reporting and funds transfer recordkeeping requirements set forth in the Bank Secrecy Act?
- Does your firm accept private banking accounts maintained for non-U.S. persons? If so, what kind of special due diligence does the firm perform for those accounts? If not, how does the firm screen new accounts to ensure that it does not accept this type of account?
- Does your firm accept private banking accounts maintained by or on behalf of senior political figures? If so, what enhanced scrutiny does the firm conduct for private banking accounts

maintained by or on behalf of senior political figures? If not, how does the firm screen new accounts to ensure that it does not accept this type of account?

- Which individuals or departments are trained, at least annually, on the firm's overall AML program?
- Which individuals or departments are trained to monitor unusual trading activity to detect suspicious activity? How often do these employees take the training?
- Who conducts the training and what areas does it cover? Be specific for each group of employees who receive training.
- Other than documents obtained or made during the CIP process, what AML documents and records does the firm maintain? How long are they maintained? Be specific.
- Which independent firm personnel or experienced outside party will conduct annual testing on the adequacy of the firm's anti-money laundering program?
- What areas are reviewed in the annual audit?
- Who in senior management or on the audit committee receives the results of the independent audit?
- How will the firm address deficiencies noted in the annual AML audit report?

**Additional Notes**

Please use this area to describe any issues or potential issues which were identified through the questionnaire.