



NATIONAL  
FUTURES  
ASSOCIATION®

# **Self-Examination Checklist**

---

For FCMs, IBs, CPOs and CTAs

June 2005

# Table of Contents

---

Introduction .....	2
Sample Attestation .....	3
General Self-Examination Checklist for All Registration Categories ....	4
Registration .....	4
Supervision .....	5
Ethics Training.....	6
Business Continuity and Disaster Recovery .....	7
Account Opening .....	8
Privacy Rules .....	8
Cash Flow .....	8
Promotional Material .....	9
E-Mails .....	11
Web Sites .....	11
Security Futures Products .....	11
Supplemental Checklist for FCMs .....	14
Financial .....	14
Supervision .....	15
Due Diligence Prior to Trading .....	15
Anti-Money Laundering .....	16
Customer Trading .....	19
Margins .....	21
Account Statements .....	21
Cash Flow .....	21
Give-up Transactions .....	22
Automatic Order Routing System .....	22
Supplemental Checklist for IBs .....	24
Supervision .....	24
Due Diligence Prior to Trading .....	24
Anti-Money Laundering .....	25
Cash Flow .....	28
Customer Trading .....	28
Financial (Independent IBs only) .....	30
Automatic Order Routing System .....	31
Supplemental Checklist for CPOs .....	32
Account Statements .....	32
Financial .....	32
Disclosure Document .....	33
Supplemental Checklist for CTAs .....	34
Disclosure Document .....	34
Bunched Orders .....	34
Post-Execution Allocation of Bunched Orders .....	34
Appendix A -- Anti-Money Laundering Questionnaire .....	35
Appendix B -- Business Continuity & Disaster Recovery Plan .....	41
Appendix C -- Ethics Training Policy Questionnaire .....	43
Appendix D -- Privacy Policy Questionnaire .....	44
Sources of Additional Information .....	46
Copyright 2005 by National Futures Association	

NFA Compliance Rule 2-9 places a continuing responsibility on every Member to diligently supervise its employees and agents in all aspects of their futures-related activities. NFA recognizes that, given the differences in the size and complexity of the operations of NFA Members, there must be some degree of flexibility in determining what constitutes “diligent supervision” for each firm. It is NFA’s policy to leave the exact form of supervision to the Member thereby providing the Member with flexibility to design procedures that are tailored to the Member’s own situation. However, NFA believes that all Members should regularly review the adequacy of their supervisory procedures.

In order to satisfy their continuing supervisory responsibilities under Compliance Rule 2-9, NFA Members must review their operations on a yearly basis using a self-examination checklist. The checklist will aid Members in recognizing potential problem areas and alert them to procedures which need to be revised or strengthened. The checklist focuses on the Member’s regulatory responsibilities and solicits information regarding whether the Member’s internal procedures are adequate for meeting these responsibilities.

The checklist has been divided into five sections. The first section is a general checklist that should be used by all registration categories. In addition, NFA has developed a separate supplemental checklist for each of the four registration categories (FCM, IB, CPO and CTA). Please complete each checklist that is applicable to your registration status.

After the annual review of the Member’s operations, the appropriate supervisory personnel must then sign and date a written attestation that they have reviewed the Member’s operations in light of the matters covered by the checklist. Although a checklist may be completed for several registration categories, only one attestation is necessary per office. A separate attestation must be made for each branch office. If the branch office reviews its own operations, the main office must receive a copy of the attestation. Guarantor FCMs must obtain copies of the signed attestation from guaranteed IBs, including branch offices of these guaranteed IBs. These attestations should not be forwarded to NFA but should be retained by the Member. Signed attestations should be readily available for the last two years and retained for the last five.

As necessary, NFA updates these checklists to reflect new and amended rules. NFA encourages you to visit NFA’s Web site ([www.nfa.futures.org](http://www.nfa.futures.org)) for the most recent version of the checklists.

If you have questions, please contact the NFA Compliance Department at (800) 621-3570.

Sample Attestation

(On Member's Letterhead)

Appropriate supervisory personnel for Member's Name have reviewed and evaluated the current procedures of Member's Name (and branch location, if applicable) using the NFA Self-Examination Checklist. Based on that review, it appears that Member's Name current procedures are adequate to meet its supervisory responsibilities.

\_\_\_\_\_  
*Signed*

\_\_\_\_\_  
*Date*

Remember, a review of operations must be performed annually. A signed and dated attestation such as this, must be prepared each year and kept on file.

## General Self-Examination Checklist for All Registration Categories

---

### Registration

- List all individuals as principals on the Member's Form 7-R:
  - who hold the following positions with the Member:
    - sole proprietor of a sole proprietorship;
    - general partner of a partnership;
    - director, president, chief executive officer, chief operating officer, chief financial officer or a person in charge of a business unit, division or function subject to regulation by the Commission of a corporation, limited liability company or limited partnership; or
    - manager, managing member or a member vested with the management authority for a limited liability company or limited liability partnership.
  - who directly or indirectly, through agreement, holding companies, nominees, trusts or otherwise, have the following financial relationships to the Member:
    - own 10 percent or more of the outstanding shares of any class of the Member's stock;
    - are entitled to vote 10 percent or more of any class of the Member's voting securities;
    - have the power to sell or direct the sale of 10 percent or more of any class of the Member's voting securities;
    - have contributed 10 percent or more of a Member's capital;
    - are entitled to receive 10 percent or more of a Member's net profits.
  - who have the power to exercise a controlling influence over an applicant's or registrant's activities that are subject to regulation by the Commission.
- List all entities as principals on the Member's Form 7-R that are:
  - a general partner of a partnership;
  - the direct owner of 10 percent or more of any class of an entity's securities; or
  - entities that have directly contributed 10 percent or more of a Member's capital unless such capital contribution consists of subordinated debt contributed by:
    - an unaffiliated bank insured by the Federal Deposit Insurance Corporation;
    - a United States branch or agency of an unaffiliated foreign bank that is licensed under the laws of the United States and regulated, supervised and examined by United States government authorities having regulatory responsibility for such financial institutions; or
    - an insurance company subject to regulation by any State.

- Ensure that all individuals who are responsible for supervising APs are registered as APs.
- List all branch office locations and branch office managers on the Member's Form 7-R.
- Require all branch office managers to meet the branch office manager proficiency requirements of NFA Compliance Rule 2-7.
- Ensure that branches hold themselves out in the name of the Member.
- Ensure all doing business as names are listed.
- Review all parties which you are doing business with to ensure those that are required to be registered are registered, and, if required to be an NFA Member, are such.
- Review commission payouts and other disbursements to ensure that only NFA Members are being paid for customer business.
- Require APs to attend ethics training in accordance with the CFTC's Statement of Acceptable Practices and NFA's Interpretive Notice on Ethics Training Requirements.
- File with the CFTC a Statement of Reporting Trader for reportable positions (CFTC Form 40).
- Allow only registered APs to handle customer accounts.
- Permit unregistered individuals to accept customer orders only if they are acting in a purely clerical manner.
- File all guarantee agreements and terminations with NFA.
- Maintain a copy of the signed guarantee agreement.
- File with NFA either a Notice of Termination (CFTC Form 8-T) or a Uniform Termination Notice for Securities Industry Registration (NASD Form U-5) within 20 days after principals, branch managers or APs terminate their affiliation with the Member.
- Promptly correct any deficiency or inaccuracy on the Member's Form 7-R which no longer renders accurate and current information contained therein on NFA's Online Registration System.

#### Supervision

- Designate a "compliance officer" who is responsible for handling customer complaints or inquiries of a compliance nature.
- Establish policies and procedures to handle customer complaints and inquiries.
- Maintain a compliance procedures manual or other written documentation which outlines the Member's policy with respect to handling compliance matters, such as customer complaints or inquiries.
- Establish a systematic method of recording, investigating and responding to customer complaints or inquiries.

- Require branches to forward complaints to the home office.
- Establish an Internal Audit Department or other designated individual (“Auditor”) who monitors branches and guaranteed IBs.
- Have the Auditor report to a partner or officer.
- Give the Auditor responsibility for conducting on-site inspections of branch offices and guaranteed IBs.
- Perform on-site inspections annually.
- Use a written audit program when conducting on-site inspections.
- Prepare written summaries of findings noted during on-site inspections of branch offices and guaranteed IBs.
- Take appropriate corrective action in the event the Auditor finds problems at a branch or guaranteed IB.
- Familiarize the Auditor with NFA Notices regarding Branch Office On-site Visits.
- Establish policies and procedures regarding the hiring and supervision of APs who have been or whose past employers have been disciplined by NFA or the CFTC for fraud.
- If you are a one-person office, inform customers when you will be unavailable to service your customer accounts (i.e., vacations) and whom they should contact in your absence.
- Distribute changes in rules or regulations to appropriate personnel.
- Supervise sales solicitations by any, or all, of the following methods: direct listening, reviewing taped solicitations, silent phone monitoring and customer contact.
- Provide APs with training on the futures and options markets.
- Provide sales solicitation training to APs.
- Monitor incoming and outgoing mail so customer complaints, etc. would be intercepted.
- If a predispute agreement is included in the customer account documentation, provide customers with a list of three forums, one of which is NFA arbitration, in the event the customer gives notice of its intent to file a claim.
- Require an officer or other supervisory personnel to regularly review trading in non-customer and proprietary trading accounts.

#### Ethics Training

- Establish policies and procedures regarding the ethics training requirements for APs, detailing areas such as content, frequency and format of training. For further assistance in drafting these ethics training procedures, see Appendix C on page 43.

- Ensure APs receive ethics training in accordance with the firm's procedures and maintain records documenting compliance with these procedures, including dates and providers of training and materials used or distributed.
- Ensure ethics training provider (either internal or external) is qualified to conduct training.

#### Business Continuity and Disaster Recovery Plan

- Establish a written business continuity and disaster recovery plan. For further assistance in drafting a business continuity and disaster recovery plan, see Appendix B on page 41.
- Periodically test the plan.
- Periodically review and revise the plan when necessary.
- Distribute the plan to key employees to maintain copies off-site.
- Communicate the recovery plan to all employees.
- Duplicate essential computer and telecommunication systems at a backup facility.
- Establish primary and backup facilities reasonably geographically apart. For example, the primary and backup facilities should be located in different power grids, and different telecommunication vendors should be utilized.
- Periodically back up essential electronic data (e.g., general ledger) and store off-site.
- Maintain a complete, up-to-date inventory of all information technology systems, including both hardware and software.
- Consider the impact of business interruptions encountered by third parties determined to be essential to the continuation of your business.
- Maintain a complete inventory of essential documents.
- Copy and store essential paper files off-site or include a plan for recreating required papers.
- Secure alternative remote office space or have provisions for key staff to work from home or an alternate site.
- Communicate transportation options and alternative routes to the backup facilities to employees.
- Contemplate the unavailability of key public utilities.
- Maintain current employee telephone lists and contact information.
- Duplicate critical staff competencies.
- Develop a communication plan to contact essential parties such as employees, board members, customers, carrying brokers, vendors, disaster recovery specialists and NFA.

## Account Opening

- Review the customer account documentation to ensure it complies with all applicable rules and regulations.
- Ensure safeguards are employed for the purpose of verifying that an electronic signature is that of the person purporting to use it.
- Ensure procedures are in place to safeguard the alteration of an electronic record after it has been signed.
- Require that all necessary information be on file before new accounts are allowed to commence trading.
- Require a partner, officer, director, branch office manager or supervisory employee to approve customer accounts and document this review.
- Provide adequate risk disclosure to customers prior to opening an account.
- Obtain the following information from customers: Name, address, occupation or business description, estimated annual income, estimated net worth, age and prior investment and futures trading experience.
- If the required information is not obtained, document that the customer declined to provide such information.
- Train individuals who are responsible for assessing and providing risk disclosure to customers as required by NFA Compliance Rule 2-30.
- Designate a supervisory individual to review the actions of the individuals providing risk disclosure to customers as required by NFA Compliance Rule 2-30.

## Privacy Rules

- Establish a written privacy policy pertaining to consumer financial information as required by CFTC Regulation 160. For further assistance in drafting these privacy procedures, see Appendix D on page 44.
- Provide the privacy notice to customers at the time the account is opened and annually thereafter.
- Provide and obtain customer “opt out” notices as required.

## Cash Flow

- Make all disbursements, except petty cash, by check.
- Require that a responsible individual approve all invoices in writing prior to payment.
- Review disbursements made by branch offices.
- Maintain documents authorizing use of qualifying bank accounts.
- Prepare a listing of all cash receipts.
- Make and keep copies of customer checks prior to depositing them.
- Restrictively endorse checks upon receipt.

- Review third-party checks received from customers to ensure the initial payee is not required to be an NFA Member.
- Prepare bank reconciliations on a timely basis.
- Ensure that blank checks are accessible only to authorized personnel.
- Ensure that all voided checks are mutilated to prevent reuse and kept on file.
- Limit access to signature plates used to sign checks.
- Review checks and wires received to ensure they are from owners of the account to which they are to be credited.
- Permit disbursements to a third party, only with specific written authorization from the account owner on file.

#### Promotional Material

- Establish written procedures to supervise the preparation and use of promotional material.
- Require an officer, general partner, sole proprietor, branch office manager or other supervisory employee other than the individual who prepared the material to approve promotional material before its use.
- Review and approve promotional material in writing.
- Maintain all promotional materials for a period of five years from the date last used.
- Maintain supporting documentation for all statements, claims and performance results.
- Include any material information so that the promotional material is not misleading.
- Include an equally prominent statement of the risk of loss if the material mentions the possibility of profit, including the presentation of past performance results.
- Calculate rates of return in a manner consistent with CFTC Part 4 Regulations.
- Ensure that the past performance of any actual accounts presented is representative of the actual performance of all reasonably comparable accounts for the same time period.
- Include a statement that past results are not necessarily indicative of future results when past performance is mentioned.
- Ensure that statements of opinion are identifiable as such and have a reasonable basis in fact. Maintain support for such statements.
- Ensure that there is no guarantee against loss.
- Identify the “limited-risk” and “no margin call” features of options as applying only to the purchase of options.

- Explain that the “limited-risk” feature of options includes the full amount of the premium and transaction costs including commissions.
- Explain fully ratings and results from outside sources, including the limitations of such ratings and results.
- Ensure that reprints of articles have been supplemented with the proper disclosures and disclaimers.
- Present hypothetical results only if there are less than three months of actual trading results for the offered program.
- Include the statement prescribed by NFA Compliance Rule 2-29(c) with hypothetical results.
- Include the actual results of all customer accounts directed by the Member for the past five years with any hypothetical results. If the Member has less than one year of experience directing accounts, include the results of any proprietary accounts for the past five years.
- Calculate hypothetical results in the same way as actual results.
- Ensure that hypothetical results and actual results are presented separately, clearly identified and given equal prominence.
- Explain all material assumptions made in preparing hypothetical results that includes at least the minimum investment amount, distribution or reinvestment of profits, commission charges, management and incentive fees, and the method used to determine the purchase and sale price for each trade.
- Ensure that paid promotional appearances are prominently identified as such prior to, during and subsequent to those appearances.
- Submit all radio or television advertisements that make any specific recommendations or refer to or describe the extent of any profit obtained in the past or that can be achieved in the future to NFA’s promotional material review team for its review and approval at least 10 days prior to first use.
- Prohibit the use of promotional material that contains the following:
  - Claims regarding seasonal trades;
  - Claims regarding historical price moves;
  - Claims regarding price movements that are characterized as conservative estimates when in fact such price movements would be dramatic;
  - Claims using certain pricing data for a product different from the one being marketed in the promotional material;
  - Claims containing profit projections;
  - Claims containing “cherry picked” trades; and
  - Claims regarding mathematical examples of leverage as a means of suggesting that prospective customers are likely to earn large profits from trading.
- Ensure employees and agents are not purchasing leads from non-Members required to be registered and/or using fraudulent advertising practices. Maintain a record of any advertisement used.

#### E-Mails

- Establish written procedures to review the use of futures-related e-mail by employees and agents that identifies by title or position the person responsible for conducting the review.
- Also, consider the following when establishing procedures:
  - How and with what frequency e-mails will be reviewed and how that review will be documented.
  - Categorize what type of e-mails will be pre-reviewed and post reviewed.
- Ensure e-mails are in compliance with NFA's promotional material content and review procedures.

#### Web Sites

- Establish written procedures to supervise the preparation and use of Web sites.
- Require prior review and approval of the Web site by an appropriate supervisor.
- Require documentation of review.
- Ensure Web site meets the standards of content established in Compliance Rule 2-29.
- Properly review personal Web sites of employees or agents used to attract business for the firm.
- Ensure paid hyperlinks to the firm's Web site do not contain deceptive information regarding futures or options trading.
- Monitor the general content of the Web site to which the Member links.

#### Security Futures Products

- Designate a security futures principal at each main or branch office.
- Check the Central Registration Depository (CRD) for information on prospective employees who will be involved in security futures activities. Obtain and review a copy of the individual's most recent Form 8-T or U-5.
- Require APs to complete appropriate security futures products training modules.
- Ensure that the firm's written procedures address the following:
  - Compliance with applicable securities laws, including Sections 9(a), 9(b), and 10(b) of the Securities Exchange Act of 1934.
  - The review and approval of customer accounts including:
    - Specific criteria and standards to be used in evaluating the suitability of a customer to engage in security futures transactions.
    - Specific procedures for approving accounts to engage in security futures transactions, including requiring written approval by a designated security futures principal.

- A requirement that the designated security futures principal explain, in writing, why he or she has approved an account that does not meet the specific criteria and standards set forth in the procedures.
  - Specific financial requirements for initial approval and maintenance of customer accounts that engage in security futures transactions.
- Check the Central Registration Depository (CRD) for any derogatory information on the IB, its principals and its employees who will be involved in security futures activities before entering into a guarantee agreement with an IB.
  - Provide the required risk disclosure statement prior to opening an account.
  - Obtain the following additional information for customers:
    - Identification that the customer account is speculative or hedge;
    - Employment status;
    - Estimated liquid net worth;
    - Marital status; and
    - Number of dependents.
  - Require that the customer account record include the name of the Associate, how the customer account information was obtained and the date the required risk disclosure statement was provided.
  - On an annual basis, ensure that customers are provided with written notice regarding NFA's Background Affiliation Status Information Center (BASIC) at [www.nfa.futures.org/basic](http://www.nfa.futures.org/basic).
  - Notify NFA within 10 business days of any required reportable events.
  - Submit a quarterly report to NFA regarding written customer complaints.
  - Ensure that promotional material meets the following requirements:
    - Prominently identifies the Member;
    - Includes the date that the material was first used;
    - Provides contact information for obtaining a copy of the disclosure statement for security futures products;
    - States that security futures products are not suitable for all customers;
    - Does not include any statement suggesting that security futures positions can be liquidated at any time;
    - Does not include any cautionary statement, caveat, or disclaimer that is not legible, that attempts to disclaim responsibility for the content of the promotional material or the opinions expressed in the material, that is misleading, or that is otherwise inconsistent with the content of the material;
    - Discloses the source of any statistical tables, charts, graphs or other illustrations from a source other than the Member, unless the source of the information is otherwise obvious;

- States that supporting documentation will be furnished upon request if it includes any claims, comparisons, recommendations, statistics or other technical data;
- If soliciting for a trading program that will be managed by an FCM or IB or Associate of an FCM or IB, it includes the cumulative performance history of the Member's customers or states that the trading program is unproven;
- Refers to past recommendations regarding security futures products, the underlying securities, or a derivative thereof only if it lists all similar recommendations made by the Member or Associate within the last year;
- Includes current recommendations regarding security futures products only if: (i) the Member has a reasonable basis for the recommendation; (ii) the material discloses all material conflicts of interest created by the Member's or Associate's activities in the underlying security; and (iii) the material contains contact information for obtaining a list of prior recommendations;
- Includes only a general description of the security futures products for which accounts, orders, trading authorization, or pool participations are being solicited; the name of the Member; and contact information for obtaining a copy of the current disclosure statement for security futures products; (unless the promotional material is accompanied or preceded by the disclosure statement for security futures products); and
- Has been submitted to NFA for review and approval at least ten days prior to first use if it reaches or is designed to reach a public audience through mass media.

## Supplemental Checklist for FCMs

---

### Financial

- Balance accounting records on a regular basis.
- Retain financial and compliance records for five years.
- Maintain a general ledger on an accrual basis.
- Prepare a trial balance on a regular basis.
- Require someone at an appropriate level of authority to approve journal entries.
- Prepare detailed support to convert the trial balance or general ledger to the financial statement format.
- Prepare monthly capital computations within 17 business days after the month end.
- Prepare required 1-FR or Focus statements including Supplementary Schedules and file them with NFA or the DSRO, and the CFTC, by the due dates.
- Prepare daily segregation and secured amount computations by noon of the following day.
- Ensure the preparer of financial statements is knowledgeable of all the requirements for financial statement preparation and have another knowledgeable individual available in the case of absence.
- Monitor intra-month capital compliance.
- Review positions in the firm's trading account to determine their effect on the firm's compliance with minimum capital requirements.
- Permit only authorized individuals access to accounting records.
- Reconcile positions and equities with carrying brokers in a timely manner.
- Maintain complete and detailed records of all securities held or owned by the firm.
- Safeguard all negotiable instruments.
- Reconcile securities held in safekeeping with the bank.
- Segregate and account for customer securities and property.
- Clearly designate all customer property as customer segregated.
- Reconcile the customer statements to the equity system.
- Review the equity run to ensure accounts of officers, directors, partners and employees are reflected separately from customers.
- Submit subordinated loan agreements to the DSRO for approval at least 10 days before the effective date. In addition, broker-dealers must file with NFA a copy of the firm's securities industry designated examining authority's approval immediately upon receipt.

### Supervision

- Provide adequate risk disclosure to customers purchasing deep out-of-the-money options.
- If affiliated persons are allowed to maintain accounts at other FCMs, provide the affiliated person with a written authorization from a person designated by the firm who has responsibility for surveillance of the affiliated person's account; and receive copies of statements and order tickets relating to the account of the affiliated person on a regular basis.
- Prohibit employees of exchanges and regulatory organizations from trading.
- Require corporate resolutions authorizing trading authority and account (strategy) limitations signed by the appropriate level of authority at the corporation.
- Identify which accounts are discretionary.
- Establish written procedures to supervise the trading of discretionary accounts.
- Prepare a written record of the review of discretionary accounts.
- Require power of attorney to be terminated in writing.
- Ensure that APs have been continuously registered for a minimum of two years prior to handling discretionary accounts.
- For accounts controlled by an outside party, obtain a copy of the account controller's written trading authorization, or a written acknowledgment from the customer that such authorization has been given.
- If fees and charges are not determined on a per-trade or round-turn basis, provide customers with a written explanation of the charges and reasonable examples on a per-trade or round-turn basis.
- For accounts of employees of other commodity firms, obtain written authorization from a person designated by such other FCM or IB with responsibility for surveillance over the employees' account and transmit regularly to the FCM or IB customer statements and order tickets for the account.
- Review the financial standing of omnibus accounts and commodity pools before the accounts are accepted.
- For accounts of investment companies or pension funds, comply with CFTC Interpretation #10.

### Due Diligence Prior to Trading

- Ensure that appropriate steps are taken to understand the risks associated with trading on different exchanges and clearing through different organizations.

- Carefully examine a potential customer's creditworthiness, business reputation, market knowledge and anticipated trading patterns before authorizing a customer to commence trading.
- Establish margin requirements and risk guidelines or limits for each customer. These levels should be reviewed periodically and revised as necessary.
- Provide adequate risk disclosure about the markets appropriate to the particular customer and type of trading anticipated.
- Establish customer confidentiality procedures to prevent unauthorized use of customer information and trade data for the benefit of other customers.
- A firm that also trades one or more proprietary accounts, either on its own behalf or for an affiliate, should have clearly defined trading objectives and should establish and maintain loss limits or risk guidelines consistent with these objectives. Firms that have granted trading authority to an account manager or must rely on individuals to implement the entity's objectives should institute appropriate procedures to protect against unauthorized trading by employees or independent account managers.

#### Anti-Money Laundering

- Adopt a policy statement that clearly outlines the firm's policy against money laundering and terrorist financing, its commitment to follow all applicable laws to ensure that its business is not used to facilitate money laundering and the consequences to employees for not following the firm's procedures.
- Develop written anti-money laundering program with procedures that enable personnel to recognize suspicious customers and transactions, require them to report suspicious or unusual activity to appropriate supervisory personnel, and FinCen when required, and ensure that the firm maintains an adequate audit trail to assist law enforcement agencies in any investigations. For further assistance in drafting an anti-money laundering program, see Appendix A on page 35.
- Require senior management to approve the anti-money laundering program in writing.
- As part of the anti-money laundering program, establish a written customer identification program ("CIP") that includes procedures for requiring collection of identifying information and conducting identity verification, recordkeeping, comparison with government lists, customer notification and reliance on other financial institutions (if applicable).
- Designate an individual or individuals ("compliance officer") to be responsible for overseeing the day-to-day operations of the firm's anti-money laundering compliance program.
- Require the compliance officer be part of or report to senior management.
- Ensure the compliance officer is not responsible for any functional areas where money-laundering activity may occur.

- For all new customers, obtain the customer's name, date of birth (for individuals), address (residential or business address (for individuals) or principal place of business, local office or other physical location (for non-natural persons); and social security number or taxpayer identification number (for U.S. persons) or one or more of the following (for non-U.S. persons): a taxpayer identification number, passport number and country of issuance, an alien identification card number, or the number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.
- If the firm accepts accounts that are applying for a taxpayer identification number, develop procedures to confirm an application for a taxpayer identification number has been filed and obtain the taxpayer identification number within a reasonable period of time after the account opens.
- Adopt risk-based procedures to verify the identity of each new customer to the extent reasonable and practicable. Verify each new customer's identity within a reasonable time before or after the customer's account is opened, taking into consideration such factors as the type of account opened, whether the customer opens the account in person and the type of identifying information that is available.
- Develop documentary/non-documentary methods to verify a customer's identity and develop procedures that describe under what circumstances documentary/non-documentary methods will be used.
- Develop procedures that require non-documentary methods be used to verify a customer's identity in the following situations: no valid government identification (expired, etc.) is presented by customer; firm is not familiar with documents provided; account is opened without obtaining documents; customer opens account without appearing in person; or any other circumstances that increases risk that the firm will be unable to verify the identity of the customer through documents.
- Develop procedures that address under what circumstances the firm will require, for customers that are not individuals (e.g., corporate, partnership, trust, etc.), that the customer provide information on the account controller in order to verify a customer's identity. These procedures would be used only when the firm is unable to adequately verify the customer's identity after using documentary/non-documentary methods.
- For situations where the firm cannot form a reasonable belief on the customer's identity, develop procedures that address when an account should not be opened; parameters for customer transactions when the firm is still verifying the customer's identity; when an account should be closed after attempts to verify customer's identity have failed; and when a Suspicious Activity Report should be filed.
- Prior to relying on another financial institution to satisfy its CIP requirements, ensure that the other entity is subject to an AML compliance program requirement under the BSA, is regulated by a Federal functional regulator and enters into a contract 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 execute a written agreement with the other financial institution outlining the allocation of responsibilities.

- Develop procedures to provide customers with a notice that the firm is requesting information to verify their identity before account opening. Describe in the notice the identification requirements.
- Develop procedures that require that records be maintained of all identifying information obtained from a customer, either a copy or a description of any document that was relied on to verify identity, a description of the non-documentary verification methods or additional verification methods used and the results, and a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained.
- Maintain records of the identifying information collected from a customer for five years after the account is closed and verification documents and resolution of discrepancies for five years after the record is made.
- Adopt procedures to identify potentially high-risk accounts in the account opening process, including consulting FATF's list of uncooperative countries (NCCT list) to determine if customer is from one of those countries.
- Perform appropriate due diligence to determine whether to accept high risk accounts.
- Determine whether additional monitoring of account activity for a high risk account is necessary.
- Perform additional monitoring of account activity as necessary.
- Develop procedures for determining whether a customer appears on any list of known or suspected terrorist or terrorist organization issued by the Federal government and designated by Treasury and to follow all Federal directives issued in connection with the list.
- Review OFAC's list of Specially Designated Nationals and Blocked Persons (SDN Report) that identifies known or suspected terrorists and terrorist organizations to determine if customer appears on the list.
- For a potential match, immediately contact OFAC to verify if customer or prospective customer is a match to person on an OFAC SDN Report. If the customer is a match, obtain instructions from OFAC.
- Review OFAC's list of sanctioned countries to determine whether customer is located in sanctioned jurisdiction. If a customer is located in a sanctioned jurisdiction, review sanctioning document or contact OFAC for instructions on how to handle the situation.
- Maintain a written agreement outlining allocation of responsibilities between FCMs and IBs with respect to the division of any AML program responsibilities (if applicable).

- Comply with all information requests issued by FinCen and conduct expeditious searches of records and report back to FinCen any matches to named subjects listed in the requests.
- Maintain systems and procedures designed to detect and require reporting of suspicious activity (including the account opening process).
- Train appropriate staff to monitor trading activity to detect suspicious activity.
- Monitor wire transfer activity for unusual transfers, including those that involve an unexpected or extensive number of transfers by a particular account during a particular period and transfers involving certain countries identified as high risk of uncooperative.
- Provide employees with examples of activity that constitute “red flags.”
- Require employees to perform further investigation when red flags occur.
- Require employees to promptly notify appropriate firm personnel of potential suspicious activity.
- Require appropriate supervisory personnel to evaluate the activity and determine whether the firm is required to file a Suspicious Activity Report (i.e., SAR-SF) with FinCen.
- If applicable, develop procedures to comply with the currency transaction reporting and funds transfer recordkeeping requirements set forth in the Bank Secrecy Act.
- Develop procedures for special due diligence for private banking accounts maintained for a non-U.S. person and for enhanced scrutiny for accounts maintained by or on behalf of a senior political figure.
- Require individuals who staff areas that are susceptible to money laundering schemes to be trained on the firm’s AML program, and at least annually, provide follow-up training.
- Retain required records for five years, unless BSA Rules otherwise require.
- Require an annual testing of the adequacy of the firm’s anti-money laundering program by independent firm personnel or an experienced outside party.
- Require that the audit function test all affected areas to ensure that personnel understand and are complying with the anti-money laundering policies and procedures and that the policies and procedures are adequate.
- Provide senior management or audit committee with the results of the audit.
- Take corrective action on all deficiencies addressed in the report.

#### Customer Trading

- Maintain any documents produced or obtained as a result of the order flow/trading process for a period of five years (i.e., customer order tickets, trade listing, equity run, customer statements, open position listing, day trade listing, P & S recap).

- For accounts of IBs, identify the FCM and IB on the account statements.
- Use pre-numbered customer order tickets or assign an internally generated order number to each order ticket immediately upon receipt of the order from the customer.
- Keep all customer order tickets (filled, unfilled, open, canceled).
- Record the following information on customer order tickets: date, commodity options/futures, account identification, quantity long/short, requested price and fill price. For customer option orders only, record put or call, strike price and premium.
- Ensure that sufficient information to identify the customer from entry through post-execution reporting is obtained. This can be accomplished by including a complete account identifier or a short code.
- Identify discretionary customer orders as discretionary.
- For discretionary accounts included in a bunched order, establish written procedures to allocate split fills and partial fills in a systematic and nonpreferential manner.
- For bunched orders placed by CTAs, ensure that required information is obtained prior to the end of the trading day concerning the number of contracts to be allocated to each account included in a bunched order along with instructions for the allocation of split and partial fills among accounts.
- Time-stamp futures order tickets immediately upon receipt of the order.
- Time-stamp options order tickets immediately upon receipt of the order from the customer and upon transmission of the order for execution.
- Immediately call the carrying broker or the floor directly upon receipt of a customer order during market hours.
- Transmit customer orders executable at or near the market to the floor before any orders in the same commodity for proprietary accounts or other accounts affiliated with the firm.
- Record the fill price when it is received.
- Promptly call the customer with the fill information.
- Prohibit the inclusion of discretionary and non-discretionary orders on a block order.
- Prohibit trades for proprietary and non-customer accounts to be combined with customer orders on block orders.
- Review accounts of foreign omnibus accounts for unusual trading or money flow patterns.
- Design and adopt procedures to identify and investigate in a timely manner unusual activity within or among accounts which may indicate illicit trading practices, including large or non-routine account transfers, account number changes and error accounts that appear to be used for trading purposes.

### Margins

- Make margin calls when an account is undermargined.
- Prepare a written daily listing of outstanding calls which indicates the number of days the call is outstanding.
- Make margin calls cumulative.
- Collect margin calls in a timely manner.
- Accept only immediately available funds from omnibus accounts.
- Set a pre-determined length of time allowed for the collection of outstanding margin calls.
- Refuse to allow customers to make withdrawals from accounts when the margin is less than the initial requirements, or when the withdrawals would impair the initial requirements.
- Aggregate related accounts as if they were one account when determining if excess margin is available for withdrawal.
- Make payouts to customers only after proper approval from the margin department or other appropriate level of authority.
- Margin domestic omnibus accounts on a gross basis.
- Utilize SPAN margin rates.
- Obtain current margin rates and SPAN risk parameters on a regular or daily basis.

### Account Statements

- Mail confirmation statements to customers no later than the business day after the customer transaction.
- Mail monthly statements to active customers promptly after every month end.
- Mail monthly statements to inactive customers at least every three months.
- Forward daily and monthly trade confirmations by means of electronic media to any customer who consents to delivery by that method, subject to certain conditions.
- Offset positions on a FIFO basis unless the customer gives other instructions.
- Absorb the losses and give the gains to the customer when errors arise between a requested customer order and the executed trade.
- Invoice NFA fees to all customers and non-customers in accordance with NFA Bylaw 1301.

### Cash Flow

- Ensure all requests for cash have been initiated by the account owner.
- For accounting purposes, ensure cash received is communicated and deposited in a timely manner.
- Control the receipt of cash through the use of pre-numbered receipts or the like.

- Verify wire transfer receipts before they are booked.
- Review cash accounts of branch offices and guaranteed IBs for unusual transactions.

#### Give-Up Transactions

- Know your rights and responsibilities for a give-up transaction.
- In absence of a written agreement, an executing broker should exercise due diligence prior to accepting an initial order for a customer to confirm that the carrying broker identified by the customer will accept the executed trade.
- Executing broker should notify the carrying broker promptly after an order has been executed if a customer has initiated trades that, in the circumstances, appear to deviate significantly from the customer's normal trading activities.
- Executing broker should provide all relevant trade information to the carrying broker as soon as practicable after a trade has been executed.
- Carrying brokers should keep a list of customers' executing brokers and adopt procedures to assure that the list is current. Carrying brokers should establish and communicate to an executing broker limits (e.g., order size, daily aggregate positions) on the trades that the executing broker can effect for each customer.

#### Automatic Order Routing System

- Establish written procedures to ensure that:
  - The order-routing process protects the integrity and confidentiality of orders and account information at all points during the process.
  - The delivery and reporting of customers orders is timely and efficient.
  - Customer complaints about order delivery and reporting are addressed expeditiously.
  - The system monitors trading and imposes controls on trading activity for each customer in order to prevent the customer from entering into trades that create undue financial risks for the firm or its other customers.
- Disclose pertinent information about the Automatic Order Routing System, including, but not limited to the following:
  - The time frame established for completion of transactions;
  - The time frame and process for informing customers of exceptions to normal processing of orders or requests;
  - Days and hours of operation;
  - Fees, commissions or costs associated with the transaction; and
  - Information to enable customers to file claims, ask questions, register complaints and obtain information on customer recourse.
- Establish security appropriate to protect internal systems from viruses and malicious code and to prevent unauthorized access.
- Monitor security procedures and update due to technology changes.

- Identify and authenticate authorized users and the protection of personally identifiable information. This should include limiting access to systems and data only to authorized employees based upon their assigned roles and responsibilities, using encryption or other equivalent security procedure to protect the transmission of information, and preventing customers from accessing others' information.
- Establish procedures to disclose to users any breaches or possible breaches to the system.
- Establish procedures to monitor availability and capacity compared to the disclosed commitments and provide for expected future requirements.
- Document, authorize, test and approve proposed system changes before implementation to protect the availability of the system.
- Provide for backup, offsite storage, restoration and disaster recovery processes sufficient to achieve the disclosed availability commitments.
- Ensure policies are current with disclosed business practices, laws and regulations.

## Supplemental Checklist for IBs

---

### Supervision

- Provide adequate risk disclosure to customers purchasing deep out-of-the-money options.
- If affiliated persons are allowed to maintain accounts at other IBs, provide the affiliated person with a written authorization from a person designated by the firm who has responsibility for surveillance of the affiliated person's account; and receive copies of statements and order tickets relating to the account of the affiliated person on a regular basis.
- Prohibit employees of exchanges and regulatory organizations from trading.
- Require corporate resolutions authorizing trading authority and account (strategy) limitations signed by the appropriate level of authority at the corporation.
- Identify which accounts are discretionary.
- Establish written procedures to supervise the trading of discretionary accounts.
- Prepare a written record of the review of discretionary accounts.
- Require power of attorney to be terminated in writing.
- Ensure that APs have been continuously registered for a minimum of two years prior to handling discretionary accounts.
- For accounts controlled by an outside party, obtain a copy of the account controller's written trading authorization or a written acknowledgment from the customer that such authorization has been given.
- If fees and charges are not determined on a per-trade or round-turn basis, provide customers with a written explanation of the charges and reasonable examples on a per-trade or round-turn basis.
- For accounts of employees of other commodity firms, obtain written authorization from a person designated by such other FCM or IB with responsibility for surveillance over the employees' account and transmit regularly to the FCM or IB customer statements and order tickets for the account.
- Review the financial standing of omnibus accounts and commodity pools before the accounts are accepted.
- For accounts of investment companies or pension funds, comply with CFTC Interpretation #10.

### Due Diligence Prior to Trading

- Ensure that appropriate steps are taken to understand the risks associated with trading on different exchanges and clearing through different organizations.
- Carefully examine a potential customer's creditworthiness, business reputation, market knowledge and anticipated trading patterns before authorizing a customer to commence trading.

- Establish margin requirements and risk guidelines or limits for each customer. These levels should be reviewed periodically and revised as necessary.
- Provide adequate risk disclosure about the markets appropriate to the particular customer and type of trading anticipated.
- Establish customer confidentiality procedures to prevent unauthorized use of customer information and trade data for the benefit of other customers.
- A firm that also trades one or more proprietary accounts, either on its own behalf or for an affiliate, should have clearly defined trading objectives and should establish and maintain loss limits or risk guidelines consistent with these objectives. Firms that have granted trading authority to an account manager or must rely on individuals to implement the entity's objectives should institute appropriate procedures to protect against unauthorized trading by employees or independent account managers.

#### Anti-Money Laundering

- Adopt a policy statement that clearly outlines the firm's policy against money laundering and terrorist financing, its commitment to follow all applicable laws to ensure that its business is not used to facilitate money laundering and the consequences to employees for not following the firm's procedures.
- Develop written anti-money laundering program with procedures that enable personnel to recognize suspicious customers and transactions, require them to report suspicious or unusual activity to appropriate supervisory personnel, and FinCen when required, and ensure that the firm maintains an adequate audit trail to assist law enforcement agencies in any investigations. For further assistance in drafting an anti-money laundering program, see Appendix A on page 35.
- Require senior management to approve the anti-money laundering program in writing.
- As part of the anti-money laundering program, establish a written customer identification program ("CIP") that includes procedures for requiring collection of identifying information and conducting identity verification, recordkeeping, comparison with government lists, customer notification and reliance on other financial institutions (if applicable).
- Designate an individual or individuals ("compliance officer") to be responsible for overseeing the day-to-day operations of the firm's anti-money laundering compliance program.
- Require the compliance officer be part of or report to senior management.
- Ensure the compliance officer is not responsible for any functional areas where money-laundering activity may occur.
- For all new customers, obtain the customer's name, date of birth (for individuals), address (residential or business address (for individuals) or principal place of business, local office or other physical location (for non-natural

persons); and social security number or taxpayer identification number (for U.S. persons) or one or more of the following (for non-U.S. persons): a taxpayer identification number, passport number and country of issuance, an alien identification card number, or the number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

- If the firm accepts accounts that are applying for a taxpayer identification number, develop procedures to confirm an application for a taxpayer identification number has been filed and obtain the taxpayer identification number within a reasonable period of time after the account opens.
- Adopt risk-based procedures to verify the identity of each new customer to the extent reasonable and practicable. Verify each new customer's identity within a reasonable time before or after the customer's account is opened, taking into consideration such factors as the type of account opened, whether the customer opens the account in person and the type of identifying information that is available.
- Develop documentary/non-documentary methods to verify a customer's identity and develop procedures that describe under what circumstances documentary/non-documentary methods will be used.
- Develop procedures that require non-documentary methods be used to verify a customer's identity in the following situations: no valid government identification (expired, etc.) is presented by customer; firm is not familiar with documents provided; account is opened without obtaining documents; customer opens account without appearing in person; or any other circumstances that increases risk that the firm will be unable to verify the identity of the customer through documents.
- Develop procedures that address under what circumstances the firm will require, for customers that are not individuals (e.g., corporate, partnership, trust, etc.), that the customer provide information on the account controller in order to verify a customer's identity. These procedures would be used only when the firm is unable to adequately verify the customer's identity after using documentary/non-documentary methods.
- For situations where the firm cannot form a reasonable belief on the customer's identity, develop procedures that address when an account should not be opened; parameters for customer transactions when the firm is still verifying the customer's identity; when an account should be closed after attempts to verify customer's identity have failed; and when a Suspicious Activity Report should be filed.
- Prior to relying on another financial institution to satisfy its CIP requirements, ensure that the other entity is subject to an AML compliance program requirement under the BSA, and is regulated by a Federal functional regulator and enters into a contract 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 execute a written agreement with the other financial institution outlining the allocation of responsibilities.

- Develop procedures to provide customers with a notice that the firm is requesting information to verify their identity before account opening. Describe in the notice the identification requirements.
- Develop procedures that require that records be maintained of all identifying information obtained from a customer, either a copy or a description of any document that was relied on to verify identity, a description of the non-documentary verification methods or additional verification methods used and the results, and a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained.
- Maintain records of the identifying information collected from a customer for five years after the account is closed and verification documents and resolution of discrepancies for five years after the record is made.
- Adopt procedures to identify potentially high-risk accounts in the account opening process, including consulting FATF's list of uncooperative countries (NCCT list) to determine if customer is from one of those countries.
- Perform appropriate due diligence to determine whether to accept high risk accounts.
- Determine whether additional monitoring of account activity for a high risk account is necessary.
- Perform additional monitoring of account activity as necessary.
- Develop procedures for determining whether a customer appears on any list of known or suspected terrorist or terrorist organization issued by the Federal government and designated by Treasury and to follow all Federal directives issued in connection with the list.
- Review OFAC's list of Specially Designated Nationals and Blocked Persons (SDN Report) that identifies known or suspected terrorists and terrorist organizations to determine if customer appears on the list.
- For a potential match, immediately contact OFAC to verify if customer or prospective customer is a match to person on an OFAC SDN Report. If the customer is a match, obtain instructions from OFAC.
- Review OFAC's list of sanctioned countries to determine whether customer is located in sanctioned jurisdiction. If a customer is located in a sanctioned jurisdiction, review sanctioning document or contact OFAC for instructions on how to handle the situation.
- Maintain a written agreement outlining allocation of responsibilities between FCMs and IBs with respect to the division of any AML program responsibilities (if applicable).
- Maintain systems and procedures designed to detect and require reporting of suspicious activity (including the account opening process).
- Train appropriate staff to monitor trading activity to detect suspicious activity.

- Monitor wire transfer activity for unusual transfers, including those that involve an unexpected or extensive number of transfers by a particular account during a particular period and transfers involving certain countries identified as high risk or uncooperative.
- Provide employees with examples of behavior or activity that constitute “red flags.”
- Require employees to perform further investigation when red flags occur.
- Require employees to promptly notify appropriate firm personnel of potential suspicious activity.
- Require appropriate supervisory personnel to evaluate the activity and determine whether the firm is required to file a Suspicious Activity Report (i.e., SAR-SF) with FinCen.
- If applicable, develop procedures to comply with the currency transaction reporting and funds transfer recordkeeping requirements set forth in the Bank Secrecy Act.
- Develop procedures for special due diligence for private banking accounts maintained for a non-U.S. person and for enhanced scrutiny for accounts maintained by or on behalf of a senior political figure.
- Require individuals who staff areas that are susceptible to money laundering schemes to be trained on the firm’s AML program and, at least annually, provide follow-up training.
- Retain required records for five years, unless BSA Rules otherwise require.
- Require an annual testing of the adequacy of the firm’s anti-money laundering program by independent firm personnel or an experienced outside party.
- Require that the audit function test all affected areas to ensure that personnel understand and are complying with the anti-money laundering policies and procedures and that the policies and procedures are adequate.
- Provide senior management or audit committee with the results of the audit.
- Take corrective action on all deficiencies addressed in the report.

#### Cash Flow

- Do not accept money, securities or property from customers except for checks made payable to the FCM.
- Deposit immediately, in a qualifying bank account, any check received from a customer which is made payable to the FCM or mail the check immediately to the FCM.

#### Customer Trading

- Establish written procedures to allocate split fills and partial fills in a systematic and nonpreferential manner.
- If a carrying broker allocates split fills and partial fills on behalf of the Member, require that the method used is systematic and non-preferential and ensure that it is followed.

- Provide the carrying broker with the account numbers at the time a trade is placed.
- Maintain any documents produced or obtained as a result of the order flow/trading process for a period of five years (i.e., customer order tickets, trade listing, equity run, customer statements, open position listing, day trade listing, P & S recap).
- Use pre-numbered customer order tickets or assign an internally generated order number to each order ticket immediately upon receipt of the order from the customer.
- Keep all customer order tickets (filled, unfilled, open, canceled).
- Record the following information on customer order tickets: date, commodity options/futures, account identification, quantity long/short, requested price and fill price. For customer option orders only, record put or call, strike price and premium.
- Ensure that sufficient information to identify the customer from entry through post-execution reporting is obtained. This can be accomplished by including a complete account identifier or a short code.
- Identify discretionary customer orders as discretionary.
- Time-stamp futures order tickets immediately upon receipt of the order.
- Time-stamp options order tickets immediately upon receipt of the order from the customer and upon transmission of the order for execution.
- Immediately call the carrying broker or the floor directly upon receipt of a customer order during market hours.
- Transmit customer orders executable at or near the market to the floor before any orders in the same commodity for proprietary accounts or other accounts affiliated with the firm.
- Record the fill price when it is received.
- Promptly call the customer with the fill information.
- Prohibit the inclusion of discretionary and non-discretionary orders on a block order.
- Prohibit trades for proprietary and non-customer accounts to be combined with customer orders on block orders.
- Review accounts of foreign omnibus accounts for unusual trading or money flow patterns.
- Design and adopt procedures to identify and investigate in a timely manner unusual activity within or among accounts which may indicate illicit trading practices, including large or non-routine account transfers, account number changes and error accounts that appear to be used for trading purposes.

#### Financial (Independent IBs only)

- Balance accounting records on a regular basis.
- Retain financial and compliance records for five years.
- Maintain a general ledger on an accrual basis.
- Prepare a trial balance on a regular basis.
- Require someone at an appropriate level of authority to approve journal entries.
- Prepare detailed support to convert the trial balance or general ledger to the financial statement format.
- Prepare monthly capital computations within 17 business days after the month end.
- Prepare required 1-FR or Focus statements including Supplementary Schedules and file them with NFA or the DSRO, and the CFTC, by the due dates.
- Ensure the preparer of financial statements is knowledgeable of all the requirements for financial statement preparation and have another knowledgeable individual available in the case of absence.
- Monitor intra-month capital compliance.
- Review positions in the firm's trading account to determine their effect on the firm's compliance with minimum capital requirements.
- Permit only authorized individuals access to accounting records.
- Reconcile positions and equities with carrying brokers in a timely manner.
- Maintain complete and detailed records of all securities held or owned by the firm.
- Safeguard all negotiable instruments.
- Reconcile securities held in safekeeping with the bank.
- Reconcile the customer statements to the equity system.
- Review the equity run to ensure accounts of officers, directors, partners and employees are reflected separately from customers.
- Submit subordinated loan agreements to the DSRO for approval at least 10 days before the effective date. Additionally, broker-dealers must file with NFA a copy of the firm's securities industry designated examining authority's approval immediately upon receipt.

#### Automatic Order Routing System

- Establish written procedures to ensure that:
  - The order-routing process protects the integrity and confidentiality of orders and account information at all points during the process.

- The delivery and reporting of customers orders is timely and efficient.
  - Customer complaints about order delivery and reporting are handled expeditiously.
  - The system monitors trading and imposes controls on trading activity for each customer in order to prevent the customer from entering into trades that create undue financial risks for the firm or its other customers.
- Disclose pertinent information about the Automatic Order Routing System, including, but not limited to the following:
    - The time frame established for completion of transactions;
    - The time frame and process for informing customers of exceptions to normal processing of orders or requests;
    - Days and hours of operation;
    - Fees, commissions or costs associated with the transaction; and
    - Information to enable customers to file claims, ask questions, register complaints and obtain information on customer recourse.
  - Establish security appropriate to protect internal systems from viruses and malicious code and to prevent unauthorized access.
  - Monitor security procedures and update due to technology changes.
  - Identify and authenticate authorized users and the protection of personally identifiable information. This should include limiting access to systems and data only to authorized employees based upon their assigned roles and responsibilities, using encryption or other equivalent security procedure to protect the transmission of information, and preventing customers from accessing others' information.
  - Establish procedures to disclose to users any breaches or possible breaches to the system.
  - Establish procedures to monitor availability and capacity compared to the disclosed commitments and provide for expected futures requirements.
  - Document, authorize, test and approve proposed system changes before implementation to protect the availability of the system.
  - Provide for backup, offsite storage, restoration and disastery recovery processes sufficient to achieve the disclosed availability commitments.
  - Ensure policies are current with disclosed business practices, laws and regulations.

## Supplemental Checklist for CPOs

---

- Establish pools as separate legal entities from the CPOs.
- Ensure that checks received from pool participants are payable to the pool.

### Account Statements

- Prepare account statements for each pool which include:
  - Statement of Income and Loss itemizing: realized commodity trading gain or loss, change in unrealized gain or loss, other gains and losses, management fees, advisory fees, brokerage commissions, other fees and other expenses.
  - Statement of Changes in NAV itemizing: beginning NAV, additions, withdrawals, net income/loss, ending NAV, NAV per unit or individual's interest in the pool, and oath or affirmation manually signed by the proper individual. In addition, the following must appear beneath the oath: the name of the individual signing the document, the capacity in which the individual is signing, the name of the commodity pool operator for which the individual is signing and the name of the commodity pool for which the document is being distributed.
- Use the account statement to disclose any changes or material information not previously disclosed in the disclosure document.

### Financial

- Engage an independent certified public accountant to do a certified audit of each pool operated during the past fiscal year, including those pools which have permanently ceased trading.
- Distribute copies of the certified reports to NFA and to each of the participants within 90 days of the fiscal year-end or within 90 days of when the pool funds were returned to participants.
- Include the following information for the preceding two year-ends in the certified audit for each pool: net asset value of the pool, net asset value per outstanding participation unit in the pool, total value of the participant's interest or share in the pool, statement of financial condition, statement of income and loss, changes in financial position, changes in ownership equity, appropriate footnote disclosure, and such further material information as may be necessary to ensure that the required statements are not misleading.
- Maintain the following documents for each pool: cash receipts and disbursements journal; security purchases and sales journal; adjusting journal entries; subsidiary ledger for each participant, including name, address, dates of deposits, withdrawals, etc., amount of deposits and withdrawals, etc., gains/losses accruing to participant, participant equity calculated on a quarterly/monthly basis, and the number of units owned; general ledger; copies of statements from any entity holding pool assets; copies of statements received from carrying brokers; bank statements and cancelled checks; dated copies of all reports and letters; balance sheets; income statements; account statements; and signed and dated acknowledgments of receipt of the disclosure document.

#### Disclosure Document

- Prepare the disclosure document in accordance with NFA Rules and CFTC Regulations.
- File disclosure document and any amendments with NFA either by mail or electronically at least 21 calendar days prior to the date you first intend to solicit clients with the document.
- File amendments or a new disclosure document when the existing document becomes materially incomplete or inaccurate.
- If disclosure document comment letters are received from NFA, promptly correct the document and submit your corrections to NFA.
- Provide prospective pool participants with a disclosure document, including any existing amendments, which is nine months old or less prior to accepting funds from the participant.
- Provide existing pool participants with all amendments to the disclosure document.
- Maintain signed and dated acknowledgments of receipt of disclosure documents from each pool participant.
- Calculate fees in accordance with the disclosure document.

## Supplemental Checklist for CTAs

---

### Disclosure Document

- File disclosure document and any amendments with NFA either by mail or electronically at least 21 calendar days prior to the date you first intend to solicit clients with the document.
- File amendments or a new disclosure document when the existing document becomes materially incomplete or inaccurate.
- Provide prospective clients with a disclosure document, including any existing amendments, which is nine months old or less prior to directing or guiding a client's account.
- Provide existing clients with all amendments to the disclosure document.
- If disclosure document comment letters are received from NFA, promptly correct the document and submit your corrections to NFA.
- Prepare the disclosure document in accordance with NFA Rules and CFTC Regulations.
- Maintain signed and dated acknowledgments of receipt of disclosure documents from each client.
- Calculate fees in accordance with the disclosure document.
- For fees collected directly from clients instead of from the carrying broker, reflect the amount in the performance record supporting worksheets as an addition and as a debit to net performance.

### Bunched Orders

- Maintain specific allocation procedures that are fair and equitable so that no account or group of accounts receives consistently favorable or unfavorable treatment.
- Ensure that all customer accounts have the correct allocation of contracts on each trade.
- Analyze each trading program at least once a quarter to ensure the allocation method has been fair and equitable. Maintain records of the review and any deficiencies that are discovered through the review.

### Post-Execution Allocation of Bunched Orders

- Make the following information available to customers upon request: (1) the general nature of the allocation methodology; (2) a summary of composite data sufficient for a customer to compare his results with those of other relevant customers and any account in which the account manager has an interest; and (3) an indication whether any account in which the account manager has an interest can be included with customer accounts in bunched orders.
- Prior to the end of the trading day, provide the clearing FCM with information concerning the number of contracts to be allocated to each account included in the bunched order along with instructions for the allocation of split and partial fills among accounts.
- If fill prices are allocated by an FCM, maintain a written agreement with the FCM that clearly describes that the FCM is responsible for the allocation.

## 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:

*NFA Rule 2-9. Supervision.*

*NFA Interpretive Notice “NFA Compliance Rule 2-9: FCM and IB Anti-Money Laundering Programs”.*

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 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?

## Appendix B - Business Continuity & Disaster Recovery Plan Questionnaire

---

Each National Futures Association (“NFA”) Member firm must adopt a written business continuity and disaster recovery plan tailored to its operations. NFA has developed the following questionnaire to assist firms in meeting that requirement.

The firm should maintain its business continuity and disaster recovery plan with other firm procedures. Having a written policy is not enough to meet your regulatory requirements, however. You must also implement and follow that policy and communicate it to your employees.

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

*NFA Rule 2-38. Business Continuity and Disaster Recovery Plan.*

*Interpretive Notice “NFA Compliance Rule 2-38: Business Continuity and Disaster Recovery Plan”.*

A Member firm’s written policy 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.

- Where are the firm’s backup facilities (including systems and personnel) located? Are the backup facilities located in separate geographical areas from the primary facility? Are the backup facilities on a different power grid than the primary facility? Do they utilize a different telecommunication vendor?
- What are the firm’s procedures for backing up or copying essential documents and data? How often is this done?
- Does the firm store the information in hard copy? In electronic format? Where is the backup information stored?
- What staff competencies or duties are critical to continuing your operations? How has your firm duplicated these competencies in order to minimize the effect on the firm’s operations if it loses primary staff?
- What specific steps will the firm take to minimize the impact of business interruptions encountered by the following third parties:
  - Banks?
  - Carrying brokers?
  - Order routers?
  - Data providers?
  - Other third parties that are critical to continuing your operation? Be specific.
- Describe the firm’s disaster-related communication plan. Specifically, how will the firm contact each of the following essential parties:

- Employees?
  - Customers?
  - Carrying brokers?
  - Vendors?
  - Other third parties that are essential to continuing your operation?  
Be specific.
- How often does management review the plan for needed updates? What evidence does the firm maintain as proof that a review was completed?
  - How often is the plan tested for effectiveness? Describe the testing process, including whether the firm plans to participate in any industry-wide disaster recovery testing. What evidence does the firm maintain as proof that a test was completed?
  - Where does the firm maintain copies of the plan? Is the plan kept at one or more off-site locations that are readily accessible to key employees? Be specific.
  - List the key employees that have received the plan. Has the plan been explained to these employees? What essential components have been discussed with all other employees? How often will the plan be communicated or distributed to employees?
  - What procedures are in place to ensure that any updated plan is distributed to key employees and that all other employees are notified of changes to essential components?
  - Has the firm provided NFA with emergency contact information for one or more individuals who NFA can contact in the event of an emergency?  
  
*If not, this information can be updated in the firm's annual questionnaire. Go to NFA's Web site home page under the "Annual Update" heading. Then click on "Annual Questionnaire." Members will need an ORS sign-on ID and password to gain access.*
  - The components listed in Steps 1 through 12 are the minimum areas that the plan should address. Please include additional information on any other areas that are essential to your operations.

## Appendix C - Ethics Training Policy Questionnaire

---

Each National Futures Association (“NFA”) Member firm must adopt a written ethics training policy tailored to its operations. NFA has developed the following questionnaire to assist firms in meeting that requirement.

The firm should maintain its ethics training policy with other firm procedures. Having a written policy is not enough to meet your regulatory requirements, however. You must also implement and follow that policy.

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

*NFA Rule 2-9. Supervision.*

*Interpretive Notice “NFA Compliance Rule 2-9: Ethics Training Requirements”*

A Member firm’s written policy should answer all of the following questions as completely as possible.

- Who conducts the ethics training? If the firm conducts training in-house, who are the training personnel (by name or title)? If the firm utilizes an outside provider, what is the provider’s name?
- What are the training personnel’s or provider’s qualifications? What proof does the firm maintain that the training personnel or provider are qualified to conduct ethics training?
- What type of medium (e.g., Internet, audiotapes, computer software, video tapes, in-person courses) does the firm utilize for the ethics training course?
- How frequently are employees required to complete the training? Specifically, how soon and how often are new registrants required to complete ethics training? How often are other registrants required to complete ethics training?
- How long is the ethics training program for new registrants? For existing registrants?
- List the topics the ethics training program addresses.
- What type of written materials are distributed during training? How does the firm ensure that it maintains copies of those materials?
- What type of documentation or records does the firm maintain as proof that its employees have completed the ethics training?
- How often does management review the firm’s ethics training policy?

## Appendix D - Privacy Policy Questionnaire

---

National Futures Association (“NFA”) has developed the following questionnaire to assist firms in meeting their obligations under the CFTC’s privacy rules.

Many elements of the firm’s privacy policy must be described in the privacy notice given to customers. The firm’s policy and procedures for protecting customer records and information (see third bullet below) must be in writing separate from the privacy notice and should be maintained with the rest of the firm’s written procedures. Although the firm is not technically required to have a separate document describing every aspect of its privacy policy and procedures, a comprehensive written policy is the best way to ensure that firm personnel know what the firm’s policy is. This is important because just having a policy is not enough to meet your regulatory requirements. You must also implement and follow that policy.

The questions listed below are very general and do not cover every aspect of the privacy rules. You should consult the following CFTC Regulations when designing your privacy policy:

### *CFTC Regulation 160 – Privacy of Consumer Financial Information*

A firm’s privacy policy 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.

- Does the firm solicit, accept, or have any clients or customers who are individuals and who use the firm’s products or services primarily for personal, family or household purposes?  
  
[NOTE: If the answer to this question is “NO,” the firm is not required to have a privacy policy and does not need to answer the remaining questions.]
- What types of nonpublic personal information does the firm collect from clients or customers? Be specific. (NOTE: Nonpublic personal information includes account numbers, trading history, account balances, social security numbers and all financial information obtained from the customer. It also includes names and addresses when that information is included in a list derived in whole or in part from nonpublic personal information, such as a list of the firm’s customers.)
- What does the firm do – administratively, technically and physically – to maintain the confidentiality and security of customer information?
  - How does the firm safeguard paper documents?
  - How does the firm safeguard electronic information?
  - Who has access to nonpublic personal information?
  - How does the firm protect against unauthorized access, disclosure or use of the information?

- Does the firm disclose information to nonaffiliated third parties? If so, what categories of nonaffiliated third parties does the firm disclose customer information to? For each category, what information does the firm disclose and under what circumstances does the firm disclose it? Be specific.
- What types of information are included in the firm's written privacy notice? (If the firm has written privacy procedures, you should attach a copy of the privacy notice to those procedures.)
- When does the firm provide new customers with the firm's privacy policy? How often does the firm provide its privacy policy to existing customers?
- Under what circumstances does the firm provide its privacy policy to consumers who do not become customers?
- How does the firm distribute its privacy policy to customers (e.g., electronically or mailed, included with account statements)?
- Does the firm give customers an opt-out notice? (If the firm has written privacy procedures, you should attach a copy of the opt-out notice to those procedures.) [NOTE: Your firm does not have to give customers an opt-out notice if it does not share nonpublic personal information with nonaffiliated third parties.]
- When does the firm provide customers with amended privacy and opt-out notices?

## Sources of Additional Information

---

Your attorney and accountant

American Institute of Certified Public Accountants  
1211 Avenue of the Americas  
New York, NY 10036  
(212) 596-6200  
[www.aicpa.org](http://www.aicpa.org)

Commodity Futures Trading Commission  
Three Lafayette Centre  
1155 21<sup>st</sup> Street, N.W.  
Washington, D.C. 20581  
(202) 418-5000  
[www.cftc.gov](http://www.cftc.gov)

Futures Industry Association/Institute for Financial Markets  
2001 Pennsylvania Avenue, N.W.  
Suite 600  
Washington, D.C. 20006  
(202) 466-5460  
(202) 223-1528  
[www.futuresindustry.org](http://www.futuresindustry.org)  
[www.theifm.org](http://www.theifm.org)

Managed Funds Association  
2025 M Street, N.W.  
Suite 800  
Washington D.C. 20036-3309  
(202) 367-1140  
[www.mfainfo.org](http://www.mfainfo.org)

Financial Industry Regulatory Authority  
9509 Key West Avenue  
Rockville, MD 20850  
(301) 590-6500  
[www.finra.org](http://www.finra.org)

National Futures Association  
300 South Riverside Plaza  
Suite 1800  
Chicago, IL 60606-6615  
(312) 781-1410  
[www.nfa.futures.org](http://www.nfa.futures.org)

National Introducing Brokers Association  
c/o Melinda Schramm  
55 West Monroe Street  
Suite 3330  
Chicago, IL 60603  
(312) 977-0598  
[www.theniba.com](http://www.theniba.com)

U.S. Securities and Exchange Commission  
450 Fifth Street, N.W.  
Washington, D.C. 20549  
(202) 942-7040  
[www.sec.gov](http://www.sec.gov)