NFA Self-Exam Checklist - Introducing Brokers (IBs Only)

2010

Introduction

Each NFA Member Firm must complete a yearly self-examination checklist and maintain the completed checklist as part of the firm's books and records. Mallon P.C. has prepared this guide to help managers complete the self-examination process as quickly and efficiently as possible.

Note: you should have already completed the general checklist for all NFA Member Firms.

Overview

This checklist covers the following categories:

- Supervision
- Due Diligence Prior to Trading
- Anti-Money Laundering
- Cash Flow
- Customer Trading
- Financial (Independent IBs only)
- Automatic Order Routing System

Instructions for completing this checklist can be found at http://www.hedgefundlawblog.com/nfa-self-examination-checklist-2010-fcms-ibs-cpos-and-ctas. If you have questions regarding your firm's compliance program or this self-exam checklist, please feel free to contact a compliance associate at Mallon P.C.

Mallon P.C.
One Ferry Building, Suite 255
San Francisco, CA 94111
415-868-5345.

Supervision		
Review	Notes	Initials
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		
Review	Notes	Initials
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		
Review	Notes	Initials
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.		
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 ▪ 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).		

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.		

Cash Flow		
Review	Notes	Initials
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		
Review	Notes	Initials
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)		
Review	Notes	Initials
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		
Review	Notes	Initials
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 ▪ 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.		

Additional Notes
Please use this area to describe any issues or potential issues which were identified through the self-examination.