June 15, 2018

Via Federal Express
Mr. Christopher J. Kirkpatrick
Secretary
Office of the Secretariat
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W.
Washington, DC 20581

Re: National Futures Association: Proposed Amendments to NFA Compliance Rule 2-9(c) and the Interpretive Notice: *Compliance Rule 2-9: FCM and IB Anti-Money Laundering Program*

Dear Mr. Kirkpatrick:

Pursuant to Section 17(j) of the Commodity Exchange Act ("CEA"), as amended, National Futures Association ("NFA") hereby submits to the Commodity Futures Trading Commission ("CFTC" or "Commission") the proposed amendments to NFA Compliance Rule 2-9(c) and the NFA Interpretive Notice entitled *Compliance Rule 2-9: FCM and IB Anti-Money Laundering Program*. NFA's Board of Directors ("Board") unanimously approved the proposals on May 17, 2018.

NFA is invoking the "ten-day" provision of Section 17(j) of the CEA and plans to make these proposals effective ten days after receipt of this submission by the Commission unless the Commission notifies NFA that the Commission has determined to review the proposals for approval.

PROPOSED AMENDMENTS
(additions are underscored and deletions are ~~stricken through~~)

COMPLIANCE RULES

* * *

RULE 2-9. SUPERVISION.

[Effective date of amendments: October 29, 1991; January 19, 1993; March 15, 1994; April 23, 2002; and November 1, 2007.]

* * *

(c) Each FCM and IB Member shall develop and implement a written anti-money laundering program approved in writing by senior management reasonably designed to achieve and monitor the Member's compliance with the applicable requirements of the Bank Secrecy Act (31 U.S.C. 5311, et. seq.), and the implementing regulations promulgated thereunder by the Department of the Treasury and, as applicable, the Commodity Futures Trading Commission. That anti-money laundering program shall, at a minimum,

(1) Establish and implement policies, procedures, and internal controls reasonably designed to prevent the financial institution from being used for money laundering or the financing of terrorist activities and to ~~assure~~ achieve compliance with the applicable provisions of the Bank Secrecy Act and the implementing regulations thereunder;

(2) Provide for independent testing for compliance to be conducted by Member personnel or by a qualified outside party;

(3) Designate an individual or individuals responsible for implementing and monitoring the day-to-day operations and internal controls of the program; ~~and~~

(4) Provide ongoing training for appropriate personnel~~.~~; and

(5) Include appropriate risk-based procedures for conducting ongoing customer due diligence, including, but not be limited to:

i) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and

ii) conducting ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, to maintain and update customer information, including the information regarding the beneficial owners of legal entity customers.

INTERPRETIVE NOTICES

* * *

9045 - NFA COMPLIANCE RULE 2-9: FCM AND IB ANTI-MONEY LAUNDERING PROGRAM

(Board of Directors, April 23, 2002; revised November 16, 2006; January 15, 2008; March 28, 2008; January 3, 2012; and August 27, 2013.)

INTERPRETIVE NOTICE

The *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001* ("Title III"),[1] which was signed into law on October 26, 2001, imposed significant

new anti-money laundering requirements on all "financial institutions," as so defined under the Bank Secrecy Act (BSA),[2] including FCMs.[3] In particular, Section 352 of Title III and NFA Compliance Rule 2-9(c) requires all financial institutions to establish anti-money laundering (AML) programs which, at a minimum, must include internal policies, procedures and controls; a designated compliance officer to oversee day-to-day operations of the program; an ongoing training program for employees; and an independent audit function to test the program. Additionally, regulations adopted by FinCEN under the BSA require an FCM's and IB's AML program to have appropriate risk-based procedures for conducting ongoing customer due diligence, including, but not limited to: i) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and ii) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, including information regarding the beneficial owners of legal entity customers.[4]

NFA's Board of Directors adopted NFA Compliance Rule 2-9(c) to impose these requirements on NFA Member FCMs and IBs.[5] [4] NFA recognizes, of course, that the exact form of program adopted by a Member will vary based on a Member's type of business, the size and complexity of its operations, the breadth and scope of its customer base, the number of firm employees, its risks and vulnerabilities to money-laundering and the firm's resources. Nevertheless, the Board believes that certain minimum standards must be a part of any adequate program. The purpose of this interpretive notice (Notice) is to highlight those minimum standards and provide Members with additional guidance on satisfying the requirements of Compliance Rule 2-9(c). Members must be aware, however, that the laws in this area are changing rapidly and that they need to conduct a regular review of their anti-money laundering program to ensure that the program is in compliance with any subsequent changes to the federal law or NFA Rules.

Many of the procedures discussed in the Notice are practices that firms may already employ in their businesses. In particular, bank or bank holding company-owned FCMs or IBs are already required to comply with certain components of the anti-money laundering programs of the banks. FCMs should also have procedures in place related to deposits of cash or cash-like instruments and procedures to obtain identifying information on customers. FCMs and IBs should use their existing programs and procedures as the building blocks for their anti-money laundering compliance programs. Moreover, FCMs and IBs that are registered as broker-dealers under the federal securities laws are subject to similar anti-money laundering requirements. In most cases, programs that comply with requirements applicable to the securities industry will comply with the requirements of this Notice.

Money laundering occurs when funds from an unlawful activity are moved through the financial system in such a way as to make it appear that the funds have come from legitimate sources. Money laundering usually follows three stages. First, cash or cash

equivalents are placed into the financial system. Second, the money is transferred or moved to other accounts (e.g. futures accounts) through a series of financial transactions designed to obscure the origin of the money (e.g. executing trades with little or no financial risk or transferring account balances to other accounts). Finally, the funds are reintroduced into the economy so that the funds appear to have come from legitimate sources (e.g. closing a futures account and transferring the funds to a bank account). Trading accounts that are carried by FCMs are one vehicle that can be used to launder illicit funds. In particular, a trading account could be used to execute financial transactions that help obscure the origin of the funds. FCMs and IBs need to be aware of potential money laundering abuses that could occur in a customer account and implement a compliance program to, among other things, deter, detect and report potentially suspicious activity.

DEVELOPING POLICIES, PROCEDURES AND INTERNAL CONTROLS

The starting point for an FCM and IB is to adopt a policy statement that clearly outlines the firm's policy against money laundering and its commitment to follow all applicable laws and regulations to ensure that its business is not used to facilitate money laundering or the financing of terrorist activities. The policy statement should also make clear that all employees of the firm have a responsibility to follow the firm's written anti-money laundering procedures and controls, and to abide by all applicable laws and regulations involving anti-money laundering programs. The policy statement also should discuss the consequences of not following these procedures. The firm's procedures and controls should enable appropriate personnel to form a reasonable belief that they know the true identity of each customer; recognize suspicious customers and transactions; and require personnel to report suspicious or unusual activity to appropriate supervisory personnel, including senior management, and to FinCEN when appropriate. The firm's procedures and controls should also ensure that the firm maintains an adequate audit trail to assist law enforcement agencies in any investigation. The key components of these policies, procedures and controls are discussed below.

A. Customer Identification Program

As part of its AML program, each FCM and IB Member must adopt a written customer identification program (CIP) that meets the requirements of the BSA.[6] [5] For purposes of the CIP requirements, a customer includes individuals or entities opening new accounts[7] [6] as of October 1, 2003. FCMs and IBs do not have to apply the CIP requirements to existing customers[8] [7] opening additional accounts provided the FCM or IB has a reasonable belief that it knows the true identity of the customer.[9] [8] FCMs and IBs should consider the following guidelines when determining whether it is required to apply its CIP requirements:

- For an omnibus account established by an intermediary, the FCM generally does not have to look through the intermediary to the underlying beneficiaries. *See*

FIN-2006-G004, *Frequently Asked Question Regarding Customer Identification Programs for Futures Commission Merchants and Introducing Brokers* (31 CFR 103.123), February 14, 2006.

- If an intermediary opens an account in the name of a collective investment vehicle such as a commodity pool, the FCM or IB is not required to apply its CIP to the pool's underlying participants.
- In a give-up arrangement, the clearing FCM, not an FCM acting solely as an executing broker, is required to apply its CIP to the customer. *See* FIN-2007-G001, *Application of the Customer Identification Program Rule to Futures Commission Merchants Operating as Executing and Clearing Brokers in Give-Up Arrangements*, April 20, 2007.

As discussed more fully below, the CIP must include the following elements:

- Required Identifying Information and Identity Verification Procedures
- Recordkeeping Procedures
- Comparison with Government List Procedures
- Customer Notice Procedures
- Reliance on Other Financial Institutions Procedures (if applicable)

Required Identifying Information and Identity Verification Procedures – These procedures should be designed to enable the FCM or IB to form a reasonable belief that it knows the true identity of each customer. In designing the procedures, the FCM or IB should consider the various types of accounts it maintains, the various account opening methods it uses, the various types of identifying information available and the firm's size, location and customer base.

Each CIP must specify the identifying information the FCM or IB will require from each customer. Although the type of identifying information a firm may require will vary based on, among other things, the nature of the firm's business and the type of customer, all firms must obtain certain minimum information prior to opening an account. For all customers, a firm must obtain the customer's name. For an individual, the firm must obtain the customer's date of birth and a residential or business address[10] [9] and for non-natural persons, the customer's principal place of business, local office or other physical location. For a U.S. person, a firm must obtain the customer's social security number or taxpayer identification number (TIN). For a non-U.S. person, the firm must obtain one or more of the following: a TIN, a 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. For a non-U.S., non-natural person, the firm must

obtain a government issued identification number.[11] [10] A firm may also choose to include procedures that provide for an exception for a person who has applied for a TIN. The CIP must include procedures to confirm that the application was filed before the customer opens the account and to obtain the TIN within a reasonable period of time after the account is opened.

The CIP must also include risk-based procedures to verify the identity of each customer to the extent reasonable and practicable. Verification may occur within a reasonable time before or after the customer's account is opened.[12] [11] Accounts may be verified using documentary methods, non-documentary methods or a combination of both. The CIP, however, must describe under what circumstances the firm will use each of these methods. In addition, the CIP must identify situations where the firm will require additional verification based on the FCM's or IB's risk assessment of the new account.

Each firm's CIP should identify the documents that will be used for documentary verification. These documents may vary from firm to firm based on the firm's own risk-based analysis of the types of documents that it believes will enable it to verify customer identity. A firm is encouraged, however, to obtain more than one type of documentary verification to ensure that it has a reasonable belief that it knows its customer's true identity. Documents that would be appropriate for verification include, for an individual, an unexpired government-issued identification that evidences nationality or residence and bears a photograph or similar safeguard (e. g. driver's license or passport); and for a non-individual (e.g. corporation, partnership or trust), documents that show the existence of the entity, such as certified articles of incorporation, a government issued business license, a partnership agreement or a trust instrument. In most instances, once an FCM or IB verifies the identity of a customer through documentary evidence, the FCM or IB does not have to determine whether the document is valid. However, if the document shows an obvious indication of fraud, then the FCM or IB must determine whether the document is sufficient for the firm to form a reasonable belief that it knows the customer's true identity.

In some situations, it may be appropriate to use non-documentary methods in addition to or in lieu of documentary methods. For example, a firm may want to use non-documentary methods in addition to documentary methods when a firm is not familiar with the documentary evidence provided. Non-documentary methods in lieu of documentary methods may be appropriate when the account is opened over the Internet or telephone. If a firm will rely on non-documentary methods, the firm's CIP must describe the non-documentary methods that will be used. These procedures must address situations where an individual is unable to present an unexpired government issued identification document that bears a photograph or similar safeguard; the FCM or IB is not familiar with the documents presented; the account is opened without obtaining documents; the customer opens the account without appearing in person; or where the FCM or IB is otherwise presented with circumstances that increase the risk that the FCM or IB will be unable to verify the identity of a customer through documents.

Appropriate non-documentary methods include contacting a customer; independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source; checking references with other financial institutions; or obtaining a financial statement. A firm may also want to examine whether there is a logical consistency between the customer's name, street address, ZIP code, telephone number, date of birth and social security number.

A firm's procedures should also include a mechanism to identify potentially high-risk accounts in the account opening process. Although attempts to launder money or finance terrorism can come from numerous sources, FCMs and IBs should be aware that certain types of entities or entities or individuals from certain geographic locations may pose a greater risk. FCMs and IBs should consult the Financial Action Task Force's (FATF) public statements of jurisdictions with strategic anti-money laundering and combating the financing of terrorism deficiencies (AML/CFT)[13] ~~[12]~~ to determine whether a customer is from one of those jurisdictions. If the customer is from one of the jurisdictions identified as having AML/CFT deficiencies, the FCM or IB should determine what, if any additional due diligence is necessary in deciding whether to open the account, and if the account is accepted, what if any additional monitoring of the account activity is appropriate.

Accounts opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by Treasury as a primary money laundering concern or has been designated as having AML/CFT deficiencies by FATF may pose additional risks. An FCM's and IB's CIP must also include additional procedures that address under what circumstances the firm will require, for a customer that is not an individual, information about individuals with authority or control over the account in order to verify the customer's identity. These procedures would be used only in situations where the FCM or IB is unable to adequately verify the customer's identity after using documentary and non-documentary methods.

Finally, there may be situations where an FCM or IB cannot form a reasonable belief that it knows the true identity of the customer. The firm's CIP must include procedures for handling this situation. At a minimum, these procedures should address: (1) when an account should not be opened; (2) the terms under which a customer may conduct transactions while the FCM or IB attempts to verify the customer's identity; (3) when an account should be closed after attempts to verify a customer's identity have failed; and (4) when the FCM or IB should file a Suspicious Activity Report (SAR) in accordance with applicable law and regulation.[14] ~~[13]~~

Recordkeeping Procedures – The firm's CIP must also describe the firm's recordkeeping policies regarding information and documents obtained during the identification and verification process. At a minimum, the CIP must require that a record be kept for: (1) all identifying information obtained from a customer (2) either a copy or a

description of any document that was relied on to verify identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date; (3) a description of the non-documentary verification methods or additional verification methods used and the results; and (4) a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. Although firms are required to keep a record of the identifying information, they do not have to maintain copies of the documents used to verify identity. However, if a firm elects to maintain copies of documents, then the copies themselves may serve as records of the identifying information that was relied upon to verify a customer's identity.

The CIP should also outline the firm's procedure for retaining records. FCMs and IBs must maintain a record of the identifying information collected from a customer for five years after the account is closed, and records of the description of the documents used to verify identity, description of the non-documentary methods or additional verification methods used and the results, and the resolution of any discrepancies for five years after the record is made.

Comparison with Government Lists Procedures – The firm's CIP must also include procedures for determining whether a customer appears on any list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators. The firm's procedures must require the FCM or IB to make this determination within a reasonable period of time after the account is opened or earlier if required by another Federal law or regulation or Federal directive issued in connection with the applicable list. The CIP must also require the FCM or IB to follow all Federal directives issued in connection with such lists. No lists have yet been designated under the CIP rules.[15] ~~14~~

Customer Notice Procedures – An FCM's and IB's CIP must also include procedures that require the firm to provide customers with adequate notice that the firm is requesting information to verify their identity. An adequate notice describes the identification requirements of the final rule and provides notice in a manner reasonably designed to ensure that a customer is able to view the notice, or is otherwise given notice, before opening the account. For example, depending on how an account is opened, notice could be provided by the firm posting notice in its office lobby or on its website, including the notice on its account application or using other forms of oral or written notice.[16] ~~15~~

Reliance on Other Financial Institutions' Procedures – An FCM or IB may share a customer relationship with one or more financial institutions. For example, in the FCM/IB relationship, although the customer is a customer of both the FCM and IB, the IB often has primary contact with the customer. This type of relationship may give rise to circumstances where it would be appropriate for an FCM or IB to reasonably rely on the customer identification and verification procedures of another financial institution

that has an account or similar relationship with the customer. If an FCM or IB intends to reasonably rely on another financial institution, it must specify in its CIP when the firm will satisfy its obligations by relying upon another financial institution (including an affiliate).

An FCM or IB may rely on another financial institution if: (1) the reliance is reasonable under the circumstances; (2) the other financial institution is subject to an AML compliance program requirement under the BSA and is regulated by a Federal functional regulator;[17] ~~[16]~~ and (3) the other financial institution enters into a contract requiring it to certify annually to the FCM or IB that it has implemented an AML program and that it will perform the specified requirements of its own CIP. If the FCM or IB meets these requirements, it will not be held responsible for the failure of the other financial institution to adequately fulfill the FCM's or IB's CIP obligations.

An FCM or IB may also delegate some or all CIP implementation to a third party service provider or an agent. In those instances, the FCM or IB should have a written agreement with the other entity outlining the other entity's responsibilities. Under these circumstances, however, the FCM or IB remains solely responsible for assuring compliance with the CIP requirements. As a result, if an FCM or IB delegates any of its CIP responsibilities, it should actively monitor the delegation, assure that the procedures are being conducted in an effective manner and ensure that NFA and other appropriate regulatory bodies are able to obtain information and records relating to the CIP.

B. Identifying and Verifying Beneficial Owners

Each FCM's and IB's AML Program must include written procedures that are reasonably designed to identify and verify beneficial owners of legal entity customers[18] for which a new account[19] is opened on or after May 11, 2018. An individual is considered a beneficial owner if the individual meets the ownership prong test (i.e., directly or indirectly owning 25% or more of the equity interests of a legal entity customer) and/or the control prong test (i.e., having significant authority to control, manage or direct the legal entity customer).[20] Although the number of beneficial owners for each legal entity customer may vary, each FCM and IB is required to identify at least one beneficial owner under the control prong.

Required Identification and Verification Procedures – Each FCM's and IB's written procedures must require the firm to identify the beneficial owner(s) by obtaining certain required information from the natural person opening the account on behalf of the legal entity customer, along with the natural person's certification regarding the accuracy of the information provided.[21] The information required includes the name and title of the person opening the account and the name and address of the legal entity for which the account is being opened. Additionally, for each beneficial owner, the FCM or IB must obtain the person's name (and title for beneficial owners under the control prong), date

of birth, address and social security number (for U.S. persons) or passport number and country of issuance or other similar identification (for foreign persons).

An FCM or IB must also develop written risk-based procedures that allow it to verify the identity of the beneficial owner that, at a minimum, contain the same elements as it employs for verifying the identity of customers under its CIP procedures, including procedures that address situations in which the FCM or IB cannot form a reasonable belief that it knows the true identity of the beneficial owner. Unlike the CIP requirements, however, in the case of documentary verification, the firm may use photocopies or other reproductions of documents. An FCM and IB may rely on the information provided by the legal entity customer regarding its beneficial owners, provided the firm has no knowledge of facts that would reasonably call into question the reliability of that information.

Recordkeeping Procedures – FCMs and IBs must establish procedures for making and maintaining a record of all information obtained during the identification and verification of beneficial owners. At a minimum, these procedures must require that a record be kept for: (1) all identifying information obtained from a customer, including without limitation the certification (if obtained); (2) for verification, a description of any document relied on (noting the type, any identification number, place of issuance and expiration); (3) a description of the non-documentary verification methods or additional verification methods used and the results; and (4) a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. All records used for identification purposes must be maintained for five years after the date the account is closed and all records made for verification purposes must be maintained for five years after the record is made.

Reliance on Other Financial Institutions' Procedures – An FCM or IB may share a customer relationship with one or more financial institutions. For example, in the FCM/IB relationship, although the customer is a customer of both the FCM and IB, the IB often has primary contact with the customer. This type of relationship may give rise to circumstances where it would be appropriate for an FCM or IB to reasonably rely on the beneficial ownership procedures of another financial institution that has an account or similar relationship with the customer. If an FCM or IB intends to reasonably rely on another financial institution, it must specify in its beneficial ownership procedures when the firm will satisfy its obligations by relying upon another financial institution (including an affiliate).

An FCM or IB may rely on another financial institution to carry out its obligation to identify and verify beneficial owners of legal entity customers if: (1) the reliance is reasonable under the circumstances; (2) the other financial institution is subject to an AML compliance program requirement under the BSA and is regulated by a Federal functional regulator;[22] (3) the other financial institution enters into a contract requiring it to certify annually to the FCM or IB that it has implemented an AML program and that it will perform (or its agent will perform) the specified requirements of its obligation to

identify and verify the beneficial owner of legal entity customers. If the FCM or IB meets these requirements, it will not be held responsible for failure of the other financial institution to adequately fulfill the FCM's or IB's obligations.

~~B~~C. Ongoing CDD and Detection and Reporting of Suspicious Activity

Another essential component of an effective anti-money laundering compliance program is a set of systems and procedures designed to detect and report suspicious activity. As with most components of a firm's compliance program, the manner in which a firm monitors for suspicious activity will vary based on the firm's size and the nature of its business.

For some firms, appropriate manual monitoring of transactions in excess of a certain dollar amount may constitute acceptable review for suspicious transactions, while other firms may need to implement an automated monitoring process. Although in some instances the carrying FCM may be in the best position to monitor accounts for suspicious transactions, an FCM or IB that is involved in the account opening process or the order flow process should be alert to suspicious transactions and, where appropriate, refuse to open an account or accept a suspicious order and report such suspicious activity to the carrying FCM and FinCEN where required.

Examples of suspicious transactions are those that have no business or apparent lawful purpose, are unusual for the customer, or lack any reasonable explanation. As discussed above, recognizing suspicious transactions requires familiarity with the firm's customers, including the customer's business practices, trading activity and patterns. What constitutes a suspicious transaction will vary depending on factors such as the identity of the customer and the nature of the particular transaction.

Since suspicious transactions may occur at the time an account is opened or at any time throughout the life of an account, FCMs and IBs must train appropriate staff to identify suspicious behavior during the account opening process and monitor cash activity and trading activity in order to detect unusual transactions. Identifying suspicious activity may prove difficult and often requires subjective evaluation because the activity may be consistent with lawful transactions.

One area that firms should give heightened scrutiny is wire transfer activity. Monitoring of this area should include review of unusual wire transfers, including those that involve an unexpected or extensive number of transfers by a particular customer during a particular period and transfers involving certain countries identified as high risk or non-cooperative.[23] ~~17~~

Firms should provide employees with examples of behavior or activity that should raise a "red flag" and cause further inquiry. These "red flags" may alert employees to possible suspicious activity. Some examples of "red flags" that could cause further investigation include:[24] ~~18~~

- A customer exhibits an unusual level of concern for secrecy, particularly with regard to the customer's identity, type of business or source of assets;
- A corporate customer lacks general knowledge of its own industry;
- A customer is unconcerned with risks, commissions or other costs associated with trading;
- A customer appears to be acting as an agent for another entity or individual but is evasive about the identity of the other entity or individual (except situations involving the identity of ownership interests in a collective investment vehicle);
- A customer is from, or has accounts in a country identified as, a haven for bank secrecy, money laundering or narcotics production;
- A customer engages in extensive, sudden or unexplained wire activity (especially wire transfers involving countries with bank secrecy laws);[25] ~~19~~
- A customer engages in transactions involving more than $5,000 in currency or cash equivalents (in one transaction or a series of transactions in one or more days and in any number of accounts); and[26] ~~20~~
- A customer makes a funds deposit followed by a request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.

Monitoring accounts for suspicious activities is a fruitless activity without timely and effective follow-up and investigative procedures. Although the internal structure for reporting suspicious activities will vary from firm to firm, each firm's compliance program must require employees to promptly notify identified firm personnel of any potential suspicious activity. Appropriate supervisory personnel must evaluate the activity and decide whether the activity warrants reporting to FinCEN. In making this determination, an IB should consult with its carrying FCM.[27] ~~21~~

For transactions occurring after May 18, 2004, FCMs and IBs[28] ~~22~~ are required[29] ~~23~~ to file form SAR[30] ~~24~~ with FinCEN to report suspicious transactions that are conducted, or attempted by, at, or through an FCM or IB, involve an aggregate of at least $5,000 in funds or other assets (not limited to currency), and the FCM or IB knows, suspects or has reason to suspect that the transaction or pattern of transactions:

- Involves funds that come from illegal activity or are part of a transaction designed to conceal that the funds are from illegal activity;
- Is designed, such as through structuring, to evade the reporting requirements of the BSA;

- Does not appear to serve any business or apparent lawful purpose; or
- Involves the use of the FCM or IB to facilitate a criminal transaction.[31] ~~25~~

FCMs and IBs must file a SAR within 30 days after the firm becomes aware of the suspicious transaction. However, if the identity of the suspect involved is unknown on the date the firm first becomes aware of the suspicious transaction, the firm may delay filing up to an additional 30 days in order to identify the suspect. A copy of the SAR and all supporting documentation must be maintained for five years from the date the SAR was filed.

FCMs and IBs must develop risk-based ongoing CDD procedures that are designed to (1) understand the nature and purpose of customer relationships for purposes of developing a customer risk profile;[32] and (2) conduct ongoing monitoring to identify and report suspicious transactions, and on a risk basis, to maintain and update customer information, including information regarding the beneficial owner of a legal entity customer. An FCM or IB is not expected to update customer information on a continuous basis. Rather a firm should update customer information when it detects information relevant to assessing the risk of a customer relationship during the course of the firm's normal monitoring.

FCMs and IBs are prohibited from disclosing that a SAR was filed, or any information that would reveal the existence of a SAR to the person involved in the transaction, as well as any other persons except as specifically authorized by 31 CFR 1026.32. Firms should develop additional risk based measures to help ensure the confidentiality of SARs, including limiting access to a "need-to-know" basis, establishing restricted areas for reviewing SARs, maintaining a log of access to SARs, using cover sheets for SARS or supporting documentation that indicates the filing of a SAR, or using electronic notices that highlight confidentiality concerns before a person may access or disseminate the information. Firms should also consider including information on SAR confidentiality and the penalties associated with unauthorized disclosure in its ongoing training of employees.

FCMs and IBs are not required to file form SAR for activity related to a robbery or burglary, provided the activity is reported to the appropriate law enforcement agency. FCMs and IBs are also relieved of the filing requirement for a violation of the Commodity Exchange Act, CFTC Regulations, Exchange or NFA rules that is otherwise required to be reported under the Commodity Exchange Act, CFTC regulations, Exchange or NFA rules committed by the FCM/IB or any of its officers, directors, employees or associated persons, provided that the activity is properly reported to the appropriate regulatory authority. If this activity also involves a violation of the BSA, a firm must file the form SAR with FinCEN regardless of whether it has reported the activity to the CFTC or other appropriate regulator. If more than one FCM and/or IB is involved in a particular situation, firms may satisfy the filing requirement by filing one form, provided that the form contains all relevant information. The two firms involved in

the transaction may consult with each other and share information, including the SAR itself, to enable the firms to file a single report.[33] ~~[26]~~

Although the BSA and the implementing regulations prohibit an FCM or IB from sharing both the SAR itself or any information which would reveal the existence of a SAR,[34] ~~[27]~~ firms may share a SAR with parent entities, both domestic and foreign, for the purpose of the parent entity fulfilling its obligation to review compliance by its subsidiaries in meeting the legal requirements to identify and report suspicious activity. FCMs and IBs, however, must have written confidentiality agreements or other arrangements in place specifying that the parent entity (or entities) must protect the confidentiality of the SARs through appropriate internal controls. In addition, FCMs and IBs may also share a SAR, or any information that might reveal the existence of a SAR, with an affiliate, provided the affiliate is subject to a SAR regulation issued by FinCEN or another regulatory agency.[35] ~~[28]~~ However, the affiliate may not share the existence of that SAR, or any information that would reveal the existence of that SAR, with another affiliate, even if that affiliate is subject to a SAR rule. Futhermore, the FCM or IB, as part of its internal controls, must have policies and procedures in place which ensure that its affiliates protect the confidentiality of the SAR.

In the event an FCM or IB receives a request from an authorized law enforcement agency to keep an open account that has suspicious activity, FinCEN recommends that the firm ask for a written request from the law enforcement agency. This request should be issued by a supervisory agent or by an attorney within a United States Attorney's Office or another office of the Department of Justice. If the request is made by a state or local law enforcement agency, the request should be from a supervisor of the state or local law enforcement or from an attorney within a state or local prosecutor's office. The request should indicate that the agency requested that the financial institution maintain the account and the purpose of the request. The request should also indicate the duration of the request, not to exceed six months (law enforcement may issue a subsequent request for a longer duration). FinCEN also recommends that the FCM or IB maintain the request for five years after the request has expired.

~~C~~D. Section 314(a) Information Requests[36] ~~[29]~~

FCM Members are also required to develop procedures to access and respond to FinCEN's 314(a) subject lists that are published bi-weekly on FinCEN's secure web-site.[37] ~~[30]~~ These lists identify individuals, entities or organizations that are suspected by various law enforcement agencies of engaging in money laundering or terrorist financing. FCMs are required to access FinCEN's secure website to obtain the most recent lists and search their records for any current accounts and accounts maintained by a named subject during the preceding 12 months and for transactions not linked to an account conducted by a named subject during the preceding 6 months. FCMs must report any matches to FinCEN through the web based system within the required time-frames (generally within 14 days of the lists being posted on the secure web-site). For matches involving an introduced account, FCMs should inform FinCEN or the

appropriate law enforcement agency that the match involves an introduced account (and identify the IB) during any follow up conducted by FinCEN or the law enforcement agency. FCMs are not required to respond to FinCEN if no matches are found. FCMs must ensure that FinCEN's requests are kept confidential. FCMs and IBs are not expected to search beneficial ownership information when responding to a 3.14(a) information request.

FCMs should maintain the following records to verify that they are complying with 314(a) request requirements: a record of the date of the request, the tracking numbers within the request, and the date the request was searched; and for positive matches, the date the match was reported to FinCEN. FCMs should also maintain information concerning the identified accounts and transactions in a positive match in a manner that can be easily accessed when requested by law enforcement.

FCMs are required to designate a point of contact (POC) person(s) for matters involving 314(a) and provide NFA with that information. Any changes to POC information must be immediately reported to NFA.[38] ~~31~~

~~D~~E. Section 312 Foreign Private Banking and Correspondent Accounts

FCMs and IBs are also required to establish due diligence programs for correspondent accounts established or maintained for foreign financial institutions (correspondent account rule) and private banking accounts established or maintained for non-U.S. persons (private banking rule).[39] ~~32~~

Correspondent Account Rule – As part of its anti-money laundering program, FCMs and IBs must establish a due diligence program that includes appropriate, specific, risk based, and where necessary, enhanced policies, procedures and controls that are reasonably designed to enable the FCM/IB to detect and report, on an ongoing basis, any known or suspected money laundering activity conducted through or involving any correspondent account[40] ~~33~~ established, maintained, administered or managed by the FCM or IB in the United States for a foreign financial institution. However, an IB that only solicits or accepts orders for the purchase or sale of commodity futures contracts does not establish, maintain or administer a correspondent account for the foreign financial institution and therefore is not subject to the requirements of Section 312 (including the enhanced due diligence requirements for certain foreign banks described below) with respect to correspondent accounts. To the extent an IB performs additional services for the account, the IB may be administering or managing the correspondent account and would be subject to Section 312. Similarly, for give-up transactions involving correspondent accounts, the carrying FCM, and not the executing FCM, is subject to compliance with the due diligence provisions of the correspondent account rule.[41] ~~34~~

In assessing the risk presented by a correspondent account, FCM and IBs should consider a number of factors, as appropriate. These factors include: (1) the nature of the foreign financial institution's business and the markets it serves; (2) the type,

purpose and anticipated activity of the correspondent account; (3) the nature and duration of the FCM's or IB's relationship with the foreign financial institution; (4) the anti-money laundering and supervisory regime in which the foreign financial institution is chartered or licensed; and (5) information known or reasonably available to the FCM or IB about the foreign financial institution's anti-money laundering record.[42] ~~35~~ The due diligence program should also require the FCM or IB to conduct a periodic review of the activity in the correspondent account.

FCMs and IBs[43] ~~36~~ are required to apply enhanced due diligence measures to correspondent accounts maintained for a foreign bank operating under an offshore banking license, under a license issued by a country designated as being non-cooperative with international money laundering principles by FATF (and the U.S. concurs with the designation),[44] ~~37~~ or under a license issued by a country that has been designated by the Secretary of Treasury as a primary money laundering concern and as warranting special measures under Section 311. At a minimum, these measures must include taking reasonable steps to (1) conduct risk-based enhanced scrutiny of correspondent accounts established or maintained for this type of foreign bank to guard against money laundering and to identify and report suspicious activity, (2) determine whether any such foreign bank maintains correspondent accounts for other foreign banks that enable those other foreign banks to gain access to the foreign bank's correspondent account with the FCM or IB, and if so, to take reasonable steps to obtain information to assess and mitigate the money laundering risks associated with such accounts, and (3) identify the owners of the foreign bank if the bank's shares are not publicly traded, and the nature and extent of each owner's ownership interest.

Enhanced scrutiny should require the FCM or IB, (1) to obtain and consider information related to the anti-money laundering program of the foreign bank to assess the risk of money laundering presented by the bank's correspondent account in appropriate circumstances; (2) to monitor transactions to, from or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity; and (3) to obtain information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable-through account, and the sources and beneficial owner of the funds and other assets in the payable-through account.

An FCM/IB's due diligence program should include procedures for situations where the FCM/IB cannot perform the enhanced due diligence, including when the FCM/IB should refuse to open an account, suspend transaction activity, file a suspicious activity report or close the account.

Private Banking Rule – FCMs and IBs must also include in their AML program a due diligence program that includes policies, procedures and controls that are reasonably designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving any private banking account[45] ~~38~~ that is established, maintained, administered, or managed in the United States by the financial

institution for a non-U.S. person. The due diligence program should ensure that FCMs and IBs take reasonable steps to (1) ascertain the identity of all nominal and beneficial owners of a private banking account; (2) ascertain whether any owner of the account is a senior foreign political figure; (3) ascertain the source(s) of funds deposited into a private banking account and the purpose and expected use of the account; and (4) review the activity of the account to ensure that it is consistent with the information obtained about the client's source of funds and with the stated purpose and expected use of the account.[46] ~~39~~

An FCM's/IB's due diligence program must include procedures for enhanced scrutiny of a private banking account where a senior foreign political figure is a nominal or beneficial owner. This scrutiny must be reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.

An FCM's/IB's due diligence program should also include procedures for situations where the FCM/IB cannot perform appropriate due diligence with respect to a private banking account, including when the FCM/IB should refuse to open the account, suspend transaction activity, file a SAR or close the account.

~~E~~F. Ongoing Compliance Responsibilities

Office of Foreign Assets Control – FCMs and IBs, like other financial institutions, also have obligations under regulations issued by the Office of Foreign Assets Control (OFAC). FCMs and IBs are currently restricted from engaging in certain transactions with individuals or entities located in countries that are under a sanction program administered by OFAC. If the customer is located in one of these countries, the FCM or IB needs to review the sanctioning document or contact OFAC to determine the breadth of the restrictions.[47] ~~40~~ FCMs and IBs are also required to block funds from individuals or entities identified on OFAC's list of Specially Designated Nationals and Blocked Persons (SDN list).[48] ~~41~~ If the customer's name appears on this list, the firm should immediately notify OFAC.[49] ~~42~~ To avoid violating the economic sanctions laws administered by OFAC, FCMs and IBs need to check the OFAC lists for new customers and also recheck their existing customer base against the lists when the lists are updated and new countries or Specially Designated Nationals and Blocked Persons are added to the lists. Otherwise FCMs and IBs risk violating the laws by engaging in prohibited transactions with persons who were not subject to sanction when they became customers, but became subject to sanctions later. FCMs and IBs should use beneficial ownership information to help ensure that they do not open or maintain an account, or otherwise engage in prohibited transactions or dealings, involving individuals or entities subject to OFAC-administered sanctions.

Section 311 Special Measures – Section 311 of the USA Patriot Act gives the Secretary of the Treasury the authority to designate a foreign jurisdiction, institution(s), class(es) of transactions, or type(s) of account(s) as a "primary money laundering concern" and to impose certain "special measures" with respect to such jurisdiction, institution(s),

class(es) of transaction, or type(s) of account(s). FCMs and IBs should monitor FinCEN's website (www.fincen.gov) for information on foreign jurisdiction(s), institution(s), class(es) of transactions, or type(s) of account(s) that have been designated as a primary money laundering concern and any special measures that have been imposed.

Foreign Bank and Financial Accounts – FCMs and IBs are required to file a Report of Foreign Bank and Financial Accounts (FBAR) if they have a financial interest in, or signature authority over any financial accounts which exceed $10,000 in a foreign country at any time during the calendar year. This report must be filed with the Department of Treasury on or before June 30th of the following year.

International Transportation of Currency or Monetary Instruments – An FCM is required to file a Report of International Transportation of Currency or Monetary Instruments (CMIR) if the firm physically transports, mails or ships or causes to be physically transported, mailed or shipped an aggregate amount exceeding $10,000 at any one time from the United States to any place outside of the United States or any place into the United States from outside the United States. A CMIR must also be filed if the firm receives in the United States any currency or other monetary instrument in aggregate exceeding $10,000 at one time which has been transported, mailed or shipped from outside the United States. A CMIR does not need to be filed, however, if the FCM is a bank or broker-dealer, and the currency or other monetary instrument is mailed or shipped through the postal service or by a common carrier. CMIRs must be filed on or before the date of the shipment and must be filed within 15 days of the receipt of the currency/monetary instruments.

~~F~~G. Hiring Qualified Staff

It is also important for the firm to ensure that the individuals that staff areas that are susceptible to money-laundering schemes are trained to work in these areas. A firm may also want to conduct background checks on key employees to screen employees for criminal or disciplinary histories.

~~G~~H. Recordkeeping

An adequate compliance program for money laundering must also include written requirements on the types of records that should be maintained. The program also must specify where the records should be maintained and that, unless the BSA rules otherwise require, the records must be maintained in accordance with CFTC recordkeeping and record retention requirements under Regulation 1.31 (e.g., maintained for five years and be readily accessible for the first two years). The ultimate goal of the recordkeeping requirements is to provide an adequate audit trail for law enforcement officials investigating potential money laundering schemes.

DESIGNATION OF A COMPLIANCE OFFICER

NFA Compliance Rule 2-9(c) also requires that FCMs and IBs designate an individual or individuals to oversee the anti-money laundering program, including the firm's CIP. This person may be the compliance officer that is responsible for other compliance areas of the firm. Although the compliance officer need not be a designated principal or Associate Member, the person should ultimately report to the firm's senior management.

The firm must provide this compliance officer with sufficient authority and resources to effectively implement the firm's anti-money laundering program. Among other duties with respect to the firm's CIP and suspicious activity reporting, this person should:

- Receive reports of suspicious activity from firm personnel;
- Gather all relevant business information to evaluate and investigate suspicious activity; and
- Determine whether the activity warrants reporting to senior management, and, if authorized to do so, the firm's DSRO or FinCEN.

Obviously, the person responsible for overseeing the anti-money laundering procedures should not be the same employee responsible for the functional areas where money-laundering activity may occur.

EMPLOYEE TRAINING PROGRAM

Another important component of NFA Compliance Rule 2-9(c) is the requirement that FCM and IB Members provide ongoing education and training for all appropriate personnel. This training program should be conducted at least every 12 months and include training on the firm's policies and procedures, the relevant federal laws and NFA guidance issued in this area. Firms should also maintain records to evidence their compliance with this requirement.

INDEPENDENT AUDIT FUNCTION

NFA Compliance Rule 2-9(c) also requires that FCM and IB Members[50] ~~43~~ provide for independent testing of the adequacy of their anti-money laundering compliance programs. Most FCMs and IBs must conduct this independent testing at least every 12 months. FCMs and IBs that engage solely in proprietary trading or are inactive, however, may satisfy this requirement by conducting the independent test every two years. All firms, however, are required to test the adequacy of their AML program more frequently than the minimum requirements if circumstances warrant.

A firm may satisfy the independent testing requirement with its own personnel (such as an internal audit staff) or others who do not perform or oversee AML functions.[51] ~~44~~ In either circumstance, the audit function should test all affected areas to ensure that personnel understand and are complying with the anti-money laundering policies and

procedures and that these policies and procedures are adequate. The results of any audit should be documented and reported to the firm's senior management or an internal audit committee or department, and follow up should be done to ensure that any deficiencies in the firm's anti-money laundering program are addressed and corrected.

ALLOCATION OF COMPLIANCE PROGRAM RESPONSIBILITIES[52] [46]

NFA Compliance Rule 2-9(c) requires all FCMs and IBs to establish and implement anti-money laundering compliance programs. NFA recognizes, however, that given the inter-business relationships between and among some Members, the interests of business efficiency and anti-money laundering effectiveness may be best served if Members cooperate with each other in order to meet their respective obligations. Members may allocate between themselves elements of their anti-money laundering compliance programs. Any allocation agreement, however, must be clearly set forth in writing and any Member allocating anti-money laundering responsibilities to another Member must have a reasonable basis for believing that the other party is properly performing the required functions. Members should keep in mind, however, that Treasury takes the position that these allocation arrangements do not relieve an FCM or IB Member from its independent obligation to comply with anti-money laundering requirements.

CONCLUSION

Money-laundering schemes in the financial services industry lessen the public's faith in the integrity of the system. Therefore, NFA Members must ensure that they take adequate steps to identify and verify the identity of their customers (and the beneficial owners of legal entity customers) and to detect, deter and report suspicious transactions that could be part of a money-laundering scheme. The guidelines set forth in this Notice should provide FCMs and IBs with the tools needed to develop an effective anti-money laundering program. Member firms should keep in mind, however, that this is an evolving area and NFA expects to provide further guidance as additional requirements in this area are imposed.

---

[1] Pub. L. 107-56, 115 Stat. 296, 324 (2001). This Act is Title III of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001.

[2] 31 U.S.C. 5311 *et seq.* (2000). Title III amended the BSA, adding certain entities to the definition of financial institution. Regulations implementing the BSA can be found in Part 103 of Title 31 of the Code of Federal Regulations.

[3] Title III also defines CPOs and CTAs as "financial institutions" under the BSA; however, the Secretary of the Treasury (Treasury) temporarily deferred application of these requirements to

certain financial institutions, including CTAs and CPOs, pending further review and analysis of the money laundering risks posed by these entities. On September 26, 2002, Treasury issued a proposed regulation that would require certain unregistered investment companies to develop and implement a written anti-money laundering program. Commodity pools are included in the definition of unregistered investment companies. *See* 67 FR 60617 (September 26, 2002). A final rule has not been issued. In addition, on May 5, 2003, Treasury issued a proposed regulation concerning anti-money laundering programs for certain CTAs. *See* 68 FR 23640 (May 5, 2003). A final rule has not yet been issued. NFA will issue separate anti-money laundering program guidance for CPOs and CTAs, at such time as they become subject to the requirements of section 352.

[4] *See* 31 CFR 1010.230 for definitions legal entity customer and beneficial owner.

[5] [4] Although IBs are not explicitly defined as "financial institutions" under the BSA, Treasury has clarified that IBs fall within the BSA's "financial institution" definition, which includes "a broker or dealer in securities or commodities." *See* 68 FR 25149 n.3 (May 9, 2003).

[6] [5] *See* 31 U.S.C. 5318(l) and the implementing regulation jointly promulgated by Treasury and the CFTC at 31 CFR 1026.00.

[7] [6] *See* 31 CFR 1026.100(a) for a definition of what does and does not constitute an account.

[8] [7] For purposes of these requirements, a customer with an existing securities account with a dually registered securities broker-dealer and FCM who elects to open a futures account with the dually registered firm may be treated as an existing customer of the firm.

[9] [8] *See* 31 CFR 1026.100(d) for the complete definition of who is and who is not a customer. The rule specifically excludes (1) financial institutions regulated by a Federal functional regulator; (2) banks regulated by a state bank regulator; and (3) persons described in 31 CFR 1026.220 (entities such as governmental agencies and instrumentalities and the domestic operations of a publicly traded company).

[10] [9] For an individual that does not have a residential or business street address, an Army Post Office or Fleet Post Office box number, or the residential or business street address of a next of kin or another contact individual should be obtained.

[11] [10] In situations where a foreign business or enterprise does not have an identification number, an FCM or IB must request alternative government issued documentation certifying the existence of the business or enterprise.

[12] [11] A reasonable amount of time may depend on various factors such as the type of account opened, whether the customer opens the account in person, and the type of identifying information that is available. A firm may choose to place limits on an account, such as restricting the number of transactions or the dollar value of transactions, until a customer's identity is verified. *See Customer Identification Program for Futures Commission Merchants and Introducing Brokers*, 67 FR 48328, 48333 (July 23, 2002). A firm should also keep in mind the regulations of Treasury's Office of Foreign Assets Control (OFAC) (*see* 31 CFR Part 500 *et.*

seq.) prohibiting transactions involving designated foreign countries, their nationals, and other specially designated persons. *See Customer Identification Programs for Futures Commission Merchants and Introducing Brokers*, 68 FR 25149, 25154 (May 9, 2003).

13 ~~12~~ FATF is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering. Since 2007, FATF's International Co- operation Review Group analyzes high risk jurisdictions and recommends specific action to address these jurisdictions' money laundering and financial terrorism risks. These public statements can be found at http://www.fatf-gafi.org. This process replaces FATF's previous procedure of publishing a list of non-cooperative countries/territories in the fight against money laundering.

14 ~~13~~ *See* Section C ~~B~~ of this Notice for details regarding SARs.

15 ~~14~~ Firms are required to comply with OFAC's list of blocked persons, restricted countries and specially designated nationals, for example, which can be found at www.ustreas.gov/ofac. Firms should also establish policies and procedures for consulting such lists and other publicly available information as part of their anti-money laundering programs. *See, e.g.,* In the Matter of the Federal Branch of Arab Bank PLC, No. 2005-2 at 5,7, available at www.fincen.gov/sites/default/files/enforcement_action/arab081705.pdf. However, firms do not have an affirmative duty to seek out the lists of known or suspected terrorists or terrorist organizations issued by the Federal government under the CIP rules. Firms will receive notification by separate guidance regarding the lists they must consult for CIP purposes.

16 ~~15~~ If appropriate, an FCM or IB may use the following sample language to provide notice to its customers:

> **Important Information About Procedures For Opening a New Account**
>
> To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify and record information that identifies each person who opens an account.
>
> What this means for you: When you open an account, we will ask you for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

17 ~~16~~ Currently, these financial institutions include banks, broker-dealers, FCMs and IBs. FCMs and IBs may rely upon these financial institutions to carry out the CIP provided that the other reliance requirements noted above are satisfied. (*See* CFTC No Action Letter 05-50 (March 14, 2005)).

18 *See* 31 CFR 1010.230(e) which defines a legal entity customer and provides the list of all entities excluded from the definition of a legal entity customer. Among others, the definition excludes registered FCMs, IBs, CPOs, CTAs, retail foreign exchange dealers, swaps dealers, major swap participants and pooled investment vehicles operated or advised by these entities.

Therefore, FCMs and IBs are not required to obtain beneficial ownership information from accounts opened for commodity pools advised or operated by registered CPOs or CTAs.

[19] Account is defined under 31 CFR 1026.100(a) and has the same meaning as it does for CIP purposes. New Account, however, means each account opened at an FCM or IB by a legal entity customer on or after May 11, 2018. Therefore, if an existing legal entity customer opens a new account, the FCM or IB must identify and verify the beneficial owners.

[20] Examples of the types of positions that could qualify as controlling include chief executive officer, chief financial officer, chief operating officer, managing member, general partner, president, vice president, treasurer, or any person who regularly performs similar functions.

[21] Firms may comply with this requirement by obtaining a completed FinCEN certification form (*See* 31 CFR 1010.230 Appendix A) from the natural person opening the account on behalf of the legal entity customer or by obtaining the information required by FinCEN's certification form, along with the required certification as to the accuracy of the information.

[22] Currently, these financial institutions include banks, broker-dealers, FCMs and IBs. FCMs and IBs may rely upon these financial institutions to carry out beneficial ownership obligations provided that the other reliance requirements noted above are satisfied.

[23] ~~[17]~~ *See supra* note ~~12~~13.

[24] ~~[18]~~ Each firm should determine whether it needs to develop additional "red flags" based on the nature of its customers and its business.

[25] ~~[19]~~ Although alternative means of funding an account, such as credit cards and non-bank online remittance systems, e.g. PayPal, are not common in the futures industry, firms that accept such forms of payment should determine if their use by a customer, like suspicious wire activity, raises a "red flag" that should cause further inquiry.

[26] ~~[20]~~ FinCEN has added FCMs and IBs to the "financial institution" definition in the rules under the BSA, thereby making them subject to the requirement to file currency transaction reports in lieu of Form 8300, *See* 68 FR 65392 (November 20, 2003). FCMs and IBs are also required to comply with BSA recordkeeping and reporting requirements set forth in 31 CFR 1010.410, including the requirements regarding requests by customers for transfers and transmittals of funds in the amount of $3,000 or more.

[27] ~~[21]~~ FCMs and IBs that comply with 31 CFR 1010.540, which includes an annual notice filing and verification requirement, are immune from civil liability for sharing information for the purpose of detecting, identifying, or reporting activities involving possible money laundering or terrorist activities. This notice can be accessed at www.fincen.gov/resources/advisories/fincen-advisory-issue-5.

[28] ~~[22]~~ Broker dealers that are notice registered for purposes of offering security futures products are required to comply with the broker-dealer reporting requirements in the securities industry.

Dually registered broker- dealers may comply with the SAR requirements in the futures industry or the securities industry's requirements. *See* 68 FR 65392 (November 20, 2003).

29 ~~23~~ Firms are encouraged to file form SAR for suspicious activity that is not required to be reported (e.g. a transaction falling below the $5,000 threshold).

30 ~~24~~ A copy of form SAR and the filing instructions are available at www.fincen.gov.

31 ~~25~~ *See* 31 CFR 1026.320 for a copy of the final regulation.

32 A customer risk profile for purposes of suspicious activity monitoring refers to information gathered about a customer to develop the baseline against which customer activity is assessed for suspicious activity reporting. Depending on the facts and circumstances, relevant information could include basic information such as a customer's annual income, net worth, domicile, or principal occupation or business, as well as, in the case of longstanding customers, the customer's history of trading activity.

33 ~~26~~ Firms jointly filing a single SAR are immune from liability with respect to such filing as provided at 31 CFR 1026.320(f).

34 ~~27~~ As noted earlier, FCMs and IBs are not prohibited from sharing or disclosing the existence of a SAR to appropriate law enforcement agencies or regulatory agencies, including the CFTC, that examine them for compliance with the BSA; or to NFA and other self-regulatory organizations that examine them for compliance with SAR requirements, upon the request of the CFTC. In addition, when requested by one of these agencies, FCMs and IBs are required to provide these agencies with any supporting documentation to a SAR. (*See* FIN-2007-G003, *Suspicious Activity Report Supporting Documentation*, June 13, 2007.) Firms should create procedures to verify that any requests for SARs or supporting documentation comes from a representative of FinCEN or an appropriate law enforcement or supervisory agency.

35 ~~28~~ Other regulatory agencies include the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision and the Securities and Exchange Commission.

36 ~~29~~ Although Section 314(a) applies to IBs, FinCEN currently does not routinely require IBs to conduct 314(a) searches. FinCEN has the authority to require IBs to comply with Section 314(a) in whole or with respect to a particular request. If FinCEN requests IBs to begin conducting 314(a) searches or to comply with a particular request, IBs would be required to conduct the search or searches.

37 ~~30~~ If a firm does not have electronic access to FinCEN's secure web-site, FinCEN faxes the subject lists to the firm on a bi-weekly basis. This firm is required to conduct the same searches and report any matches to FinCEN via fax.

38 ~~31~~ FCMs are directed to follow the detailed instructions and frequently asked questions concerning these information requests that have been issued directly to them by FinCEN.

39 ~~32~~ *See* 71 Fed. Reg. 496 (January 4, 2006). *See also* FIN-2006-G009 - *Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to Securities and Futures Industries*, May 10, 2006.

40 ~~33~~ Correspondent accounts include accounts for foreign financial institutions to engage in futures or commodity options transactions, funds transfers, or other financial transactions, whether for the financial institution or principal or for its customers. An account includes any formal relationship established by an FCM to provide regular services, including but not limited to, those established to effect transactions in contracts of sale of a commodity for future delivery, options on a commodity or options on futures. 31 CFR 1010.650(c).

41 ~~34~~ *See* FIN-2206-G011, *Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to Certain Introduced Accounts and Give-Up Arrangements in the Futures Industries*, June 7, 2006.

42 ~~35~~ *See* 31 CFR 1010.610(a).

43 ~~36~~ As previously noted, as a general rule, the FCM establishing and maintaining the account is subject to the enhanced due diligence requirements of Section 312. An IB that only solicits or accepts orders for the purchase or sale of commodity futures contracts is not subject to the enhanced due diligence requirements of Section 312.

44 ~~37~~ The final rule refers to being designated by an intergovernmental group or organization of which the United States is a member. Currently, FATF is the only such group.

45 ~~38~~ A private banking account is an account (or any combination of accounts) that (1) requires a minimum aggregate deposit of funds or other assets of not less than $1,000,000; (2) is established on behalf of one or more individuals who have a direct or beneficial ownership interest in the account; and (3) is assigned to, or is administered or managed by, in whole or in part, an officer, employee, or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account.

46 ~~39~~ *See* 31 CFR 1010.620(b).

47 ~~40~~ OFAC administers sanction programs against a number of foreign countries. A list of these countries and the sanctioning documents can be found at http://www.ustreas.gov/offices/enforcement/ofac.

48 ~~41~~ OFAC's SDN list identifies individuals and entities owned or controlled by, or acting for or on behalf of targeted countries, or known or suspected terrorists or terrorist organizations. This list and information on how to handle matches can be found at http://www.ustreas.gov/offices/enforcement/ofac.

49 ~~42~~ In addition, if a customer attempts to wire transfer money to or receive money from a country under a sanction program or an entity or individual on the SDN list, the firm should contact OFAC immediately.

50 ~~43~~ Although guarantor FCMs may conduct this audit for any of their guaranteed IBs, the IB's senior management must review the scope of the audit and its findings and take corrective action where necessary.

51 ~~44~~ For small firms with limited staff, the audit function can be accomplished by a staff person who is not involved in the anti-money laundering program.

52 ~~45~~ This discussion does not apply to reliance arrangements that meet the requirements discussed under the customer identification program section of this interpretive notice.

* * *

EXPLANATION OF PROPOSED AMENDMENTS

NFA Compliance Rule 2-9(c), as well as the related Interpretive Notice, require FCMs and IBs to develop and implement an AML program reasonably designed to achieve and monitor a Member's compliance with the requirements of the Bank Secrecy Act (BSA) and the implementing regulations promulgated thereunder. On May 11, 2016, the Financial Crimes Enforcement Network (FinCEN) issued new regulations that require financial institutions to identify and verify the identity of beneficial owners of legal entity (LE) customers and amended the AML program requirements to require appropriate risk-based procedures to conduct ongoing customer due diligence (collectively, CDD Rule). FCMs and IBs were required to comply with the CDD Rule on or before May 11, 2018.

On August 12, 2016, NFA notified FCM and IB Members of these new requirements and instructed them to begin considering modifications to their AML programs in order to comply with these new requirements. The Notice also indicated that NFA would be updating Compliance Rule 2-9 and the related Interpretive Notice to reflect these changes.

NFA is amending NFA Compliance Rule 2-9(c) and the Interpretive Notice to incorporate the requirements of FinCEN's beneficial ownership rule. The amendments closely track the language in FinCEN's rule and include some language from the preambles of the proposed rule and the final rule that NFA believes will provide useful guidance to FCM and IB Members.

The proposed amendments include the following substantive changes:

- Amend Compliance Rule 2-9(c) to modify the language in prong (1) of the AML Compliance Program Requirements and add prong (5) to specifically require appropriate risk based procedures for conducting ongoing customer due diligence;

- Amend the Interpretive Notice to add a separate section on Identifying and Verifying Beneficial Owners pursuant to FinCEN's requirements;

- Amend the Suspicious Activity Reporting section of the Interpretive Notice to add a requirement that FCMs and IBs develop risk-based ongoing CDD procedures in accordance with FinCEN's requirements; and

- Amend the Ongoing Compliance Responsibilities – Office of Foreign Asset Control section of the Interpretive Notice to clarify that FCMs and IBs should use the beneficial ownership information to help ensure that they are in compliance with OFAC regulations.

NFA's FCM and IB Advisory Committees fully support the proposed amendments to NFA Compliance Rule 2-9(c) and the related Interpretive Notice.

As mentioned earlier, NFA is invoking the "ten-day" provision of Section 17(j) of the CEA. NFA intends to make the proposed amendments to NFA's Compliance Rule 2-9(c) and the related Interpretive Notice entitled *Compliance Rule 2-9: FCM and IB Anti-Money Laundering Program* effective ten days after receipt of this submission by the Commission, unless the Commission notifies NFA that the Commission has determined to review the proposals for approval.

Respectfully submitted,

Carol A. Wooding
Vice President and General Counsel