September 22, 2022

Via Email (secretary@cftc.gov)
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's Interpretive Notice 9045—*NFA Compliance Rule 2-9: FCM and IB Anti-Money Laundering*

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's Interpretive Notice entitled *NFA Compliance Rule 2-9: FCM and IB Anti-Money Laundering.* NFA's Board of Directors ("Board") unanimously approved the proposal on February 18, 2021.

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

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

NATIONAL FUTURES ASSOCIATION

* * *

NFA INTERPRETIVE NOTICES

* * *

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

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 (May 11, 2016 regulation), 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~~. For purposes of the May 11, 2016 regulation, customer information includes 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] 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.

* * *

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 and terrorist financing. 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) [6] that meets the requirements of the BSA[7]. For purposes of the CIP requirements, a customer includes individuals or entities opening new accounts[8] as of October 1, 2003. FCMs and IBs do not have to apply the CIP requirements to existing customers[9] opening additional accounts provided the FCM or IB has a reasonable belief that it knows the true identity of the customer.[10] 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.~~ where an intermediary is the account holder, the FCM should treat the intermediary as the customer and the FCM does not have to apply its CIP requirements 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~~ identify and verify 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.

* * *

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;[18]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 (or its agent will perform) the specified requirements of the FCM's or IB's ~~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.

* * *

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[19] for which a new account[20] 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 a significant authority to control, manage or direct the legal entity customer.~~ A beneficial owner means: (1) each individual, if any, who directly or indirectly, through any contract, arrangement, understanding, relationship, or

otherwise, owns 25% or more of the equity interests of a legal entity customer; and (2) a single individual with significant responsibility to control, manage or direct a legal entity customer, including an executive officer or senior manager or any other individual who regularly performs similar functions.[21] 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. An FCM or IB is not precluded from identifying additional individuals as part of its customer due diligence.

* * *

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) for identification, all identifying information obtained from a customer, including without limitation the certification (if obtained); (2) for verification, (i) a description of any document relied on (noting the type, any identification number, place of issuance and expiration); (ii) ~~(3)~~ a description of any non-documentary verification methods or additional verification methods used and the results of any measures undertaken; and ~~(4)~~ (iii) 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.

* * *

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~~ having AML/CFT deficiencies.[24]

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:[25]

- 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);[26]
- 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[27]
- 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.[28]

For transactions occurring after May 18, 2004, FCMs and IBs[29] are required[30] to file form SAR[31] 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 is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as ~~are~~ part of a plan to ~~transaction designed to conceal that the funds are from illegal activity~~ violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;
- Is designed, whether ~~such as~~ through structuring or any other means, to evade any ~~the reporting~~ requirements of 31 CFR Chapter X or any other regulations under the BSA;
- Has no ~~Does not appear to serve any~~ business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the FCM or IB knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or
- Involves the use of the FCM or IB to facilitate a criminal ~~transaction~~ activity.[32]

FCMs and IBs must file a SAR within 30 days after the date of the initial detection by the firm of facts that may constitute the basis for reporting ~~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 initial detection ~~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 appropriate risk-based CDD procedures ~~that are designed~~ for conducting ongoing CDD to include, but not limited to: (1) understanding the nature and purpose of customer relationships for purposes of developing a customer risk profile;[33] and (2) 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 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~~0~~. 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.[34]

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,[35] 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.~~ <u>oversight responsibilities with respect to enterprise-wide risk management and compliance with applicable laws and regulations.</u> 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.[36] 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. Furthermore, 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 open an 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 agency 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.

In guidance issued in this area, note that, ultimately, the decision to maintain or close an account should be made by a financial institution in accordance with its own standards and guidelines. Although there is no requirement that a financial institution maintain a particular account relationship, financial institutions should be mindful that complying with such a request may further law enforcement efforts to combat money laundering, terrorist financing, and other crimes.

D. Section 314(a) Information Requests[37]

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~~ Secure Information Sharing System website.[38] 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 Information Sharing System ~~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. FinCEN sends notification to designated contacts within financial institutions across the country once every 2 weeks informing them new information has been made available. 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.[39]

E. Section 312 ~~Foreign~~ Private Banking and Foreign 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).[38] [40]

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[39] [41] 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.[40] [42]

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 (and any of its affiliates); (4) the anti-money laundering and supervisory regime of the jurisdiction in

which the foreign financial institution is chartered or licensed and, to the extent reasonably available, of the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered; (5) information known or reasonably available to the FCM or IB about the foreign financial institution's anti-money laundering record.[41] [43] 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[42] [44] 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),[43] [45] 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[44] [46] that is established, maintained, administered, or managed in the United States by the financial institution for ~~a~~ one or more non-U.S. person[s]. 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.[45] ~~47~~

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.

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.[46] ~~48~~ 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).[47] ~~49~~ If the customer's name appears on this list, the firm should immediately notify OFAC.[48] ~~50~~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.

* * *

INDEPENDENT AUDIT FUNCTION

NFA Compliance Rule 2-9(c) also requires that FCM and IB Members[49] [51] 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.[50] [52] 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 [51] [53]

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 and terrorist financing 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.

* * *

[14] 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, terrorist financing, and proliferation financing. 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.

* * *

[16] 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.~~us~~treasury.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~~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.~~

* * *

[30] 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). 31 U.S.C. 5318(g)(3) provides a safe harbor from liability in situations where a firm makes a voluntary SAR filing.

* * *

~~[37] 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.~~

~~[38] 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.~~

[37] ~~39~~ 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.

[38] ~~40~~ *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.

[39] ~~41~~ 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 1010.605(c).

[40] ~~42~~ *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.

[41] ~~43~~ *See* 31 CFR 1010.610(a).

[42] ~~44~~ 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.

[43] ~~45~~ 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.

[44] ~~46~~ 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~~ non-U.S. persons 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.

[45] ~~47~~ *See* 31 CFR 1010.620(b).

[46] ~~48~~ OFAC administers sanction programs against a number of foreign countries. Further information is available at https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx. ~~A list of these countries and the sanctioning documents can be found at http://www.ustreas.gov/offices/enforcement/ofac.~~

47 ~~49~~ As part of its enforcement efforts, OFAC's ~~s~~ publishes a SDN list ~~identifies~~ of individuals and companies ~~entities~~ owned or controlled by, or acting for or on behalf of targeted countries.~~,~~ It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and U.S. persons are generally prohibited from dealing with them. View more information at: https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information. ~~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.~~

48 ~~50~~ 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 file the reports as required by 31 CFR 501.603 and 501.604 ~~contact OFAC immediately~~.

49 ~~51~~ 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.

50 ~~52~~ 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.

51 ~~53~~ 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) and its related Interpretive Notice entitled *NFA Compliance Rule 2-9: FCM and IB Anti-Money Laundering Program* (Interpretive Notice) require each FCM and IB Member to develop and implement an AML Compliance Program that is reasonably designed to ensure that the FCM or IB is in compliance with the applicable requirements of the Bank Secrecy Act (BSA) and its implementing regulations. In May 2018, NFA's Board approved several amendments to the Interpretive Notice to incorporate the Financial Crimes Enforcement Network's (FinCEN) Customer Due Diligence Requirements (CDD Requirements). After submitting those particular amendments to the Commission and upon the Commission's determination that its review of the proposed rule change was not necessary, NFA made those amendments to the Interpretive Notice effective as of July 30, 2018.

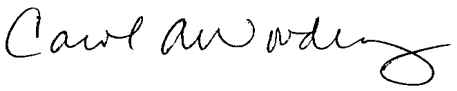
NFA is a national securities association for the limited purpose of regulating the activities of Members who are registered as brokers or dealers in

securities futures products under Section 15(b)(11) of the Securities Exchange Act (Exchange Act), and any amendments to the Interpretive Notice also apply to the activities of Members that are registered as brokers or dealers in securities futures products under the Exchange Act. Therefore, NFA is also required to submit such amendments to the Securities and Exchange Commission (SEC) for approval. SEC staff requested that NFA wait to formally submit the proposed rule amendments to the Interpretive Notice until both the SEC and FinCEN had an opportunity to review the proposed amendments to ensure that it corresponded with current SEC and FinCEN requirements.

During several virtual meetings during the months of August and September 2020, NFA staff met with CFTC and SEC staff to discuss the SEC's proposed amendments to the Interpretive Notice. In 2021, the SEC and FinCEN provided NFA staff with a copy of proposed changes to the Interpretive Notice, which included several proposed technical revisions related to the CDD Requirements and other portions of the Interpretive Notice. These proposed amendments are all non-substantive and primarily intended to more closely align NFA's Interpretive Notice with the exact language included in the BSA and its implementing regulations. Additionally, the proposed amendments do not require NFA Members to alter the manner in which they discharge their AML obligations. The proposed amendments also include the deletion of two footnotes that are no longer applicable as well as amendments to other footnotes that include outdated language and website links that are no longer operable.

As mentioned earlier, NFA is invoking the “ten-day” provision of Section 17(j) of the CEA and NFA intends to make the amendments to the Interpretive Notice to NFA Compliance Rule 2-9 regarding an FCM's and IB's 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 proposal for approval.

Respectfully submitted,



Carol A. Wooding
Senior Vice President and
General Counsel