August 28, 2015

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: Information Systems Security Programs – Proposed Adoption of the Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs*

Dear Mr. Kirkpatrick:

Pursuant to Section 17(j) of the Commodity Exchange Act, as amended, National Futures Association ("NFA") hereby submits to the Commodity Futures Trading Commission ("CFTC" or "Commission") the proposed adoption of the Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs. NFA's Board approved the proposal on August 20, 2015, and NFA respectfully requests Commission review and approval of the proposal.

PROPOSED INTERPRETIVE NOTICE
(additions are underscored)

INTERPRETIVE NOTICES

*****

Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs[1]

NFA Compliance Rule 2-9 places a continuing responsibility on every Member futures commission merchant (FCM), commodity trading advisor (CTA), commodity pool operator (CPO), and introducing broker (IB) to diligently supervise its employees and agents in all aspects of their futures activities. Compliance Rule 2-36 places identical supervisory obligations on retail foreign exchange dealers (RFED) for their forex activities. Additionally, NFA Compliance Rule 2-49, which adopts by reference CFTC Regulation 23.602, places a continuing responsibility on every Member swap dealer (SD) and major swap participant (MSP) to diligently supervise its business. These rules are broadly written to provide Members with flexibility in developing procedures tailored to meet their particular needs. On certain issues, however, NFA issues Interpretive Notices to provide more specific guidance on acceptable standards for supervisory procedures.

Over the years, information technology has changed nearly every aspect of how Members conduct business. For example, Members may use electronic means to collect and maintain customer and counterparty information. This information may include personally identifying information (PII) for individuals such as social security numbers and confidential or sensitive information for institutional customers and counterparties, including corporate records and financial information. Additionally, Members may have websites that are available to customers and counterparties for opening accounts, trading, and accessing account information, and rely upon electronic means to enter customer, counterparty and proprietary orders. Moreover, Members either directly or indirectly connect electronically with other Members, exchanges, clearinghouses, third-party service providers, NFA and the CFTC. NFA's Board of Directors believes that Members should have supervisory practices in place reasonably designed to diligently supervise the risks of unauthorized access to or attack of their information technology systems, and to respond appropriately should unauthorized access or attack occur.

[1] Nothing in this Interpretive Notice is intended to relieve Members from or reduce the obligations to which Members are subject under other state or federal statutes or regulations related to data security and privacy.

NFA recognizes that, given the differences in the type, size and complexity of operations of Members' businesses including but not limited to their customers and counterparties, markets and products traded, and the access provided to trading venues and other industry participants, Members must have an appropriate degree of flexibility to determine how best to diligently supervise information security risks. Accordingly, this Interpretive Notice is designed to establish general requirements relating to Members' information systems security programs (ISSPs) but leave the exact form of an ISSP up to each Member thereby allowing the Member flexibility to design and implement security standards, procedures and practices that are appropriate for their circumstances. Given the rapidly changing nature of technology and threats to information systems, NFA's policy is not to establish specific technology requirements.

We also recognize that practices other than those described in this Interpretive Notice may comply with the general standards for supervisory responsibilities imposed by Compliance Rules 2-9, 2-36 and 2-49. For example, CFTC Regulations 160.30 and 162.21 require all FCMs, RFEDs, CTAs, CPOs, IBs, MSPs and SDs (Registrants) to adopt policies and procedures that address administrative, technical and physical safeguards to protect customer information. CFTC Regulation 162.30(d) requires some Registrants to develop and implement a written Identity Theft Prevention Program designed to detect, prevent and mitigate customer identity theft.[2] Moreover, CFTC Regulations 1.11 and 23.600 also require certain FCMs and SDs to adopt risk management policies and procedures addressing operational risks. The CFTC Division of Swap Dealer and Intermediary Oversight (DSIO) also issued guidance on what it considers to be best practices for privacy and security in connection with these rules.[3] Finally, almost all states have data protection laws that govern the loss of customers' PII.

[2] The CFTC's adopted rules are designed to be consistent with the regulations of other financial regulators, including the Office of the Comptroller of the Currency, the Department of Treasury, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration and the Federal Trade Commission.

[3] The guidance can currently be found at http://www.cftc.gov/ucm/groups/public/@lrlettergeneral/documents/letter/14-21.pdf

Further, NFA recognizes that Member firms may be part of a larger holding company structure that shares common information systems security personnel, resources, systems and infrastructure. In these circumstances, the top level company in the holding company structure may be in the best position to evaluate the risks associated with the use of information technology systems, as privacy and security safeguards are often adopted and implemented organization-wide. Therefore, to the extent a Member firm is part of a holding company that has adopted and implemented privacy and security safeguards organization-wide, then the Member firm can meet its supervisory responsibilities imposed by Compliance Rules 2-9, 2-36 and 2-49 to address the risks associated with information systems through its participation in a consolidated entity ISSP. If a Member firm is participating in a consolidated entity ISSP, then the Member firm still has an obligation to ensure that all written policies and procedures relating to the program are appropriate to its information security risks, are maintained in a readable and accessible manner and can be produced upon request to NFA[4] and the CFTC.

This Notice provides guidance regarding information systems security practices that Member firms should adopt and tailor to their particular business activities and risks.

Information Security Program

- Written Program

Each Member firm should establish and implement a governance framework that supports informed decision making and escalation within the firm to identify and manage information security risks. In implementing an ISSP, each Member must adopt and enforce a written ISSP reasonably designed to provide safeguards, appropriate to the Member's size, complexity of operations, type of customers and counterparties, the sensitivity of the data accessible within its systems, and its electronic interconnectivity with other entities, to protect against security threats or hazards to their technology systems[5]. The Member's ISSP should be approved, in writing, by the Member's Chief

[4] FCMs should be able to provide the ISSP to their DSRO.

[5] The ISSP's policies and procedures may be documented in a single document or in documents maintained throughout a Member's various departmental areas so long as the ISSP

Executive Officer, Chief Technology Officer, or other executive level official. Additionally, if applicable, the Member's senior management should periodically provide sufficient information about the Member's ISSP to the Member's board of directors or similar governing body, the board's or governing body's delegate or a committee of the board or body to enable it to monitor the Member's information security efforts.

In order to develop and adopt appropriate ISSPs, Members may consider several resources available appropriate to their size, sophistication and role in the financial industry. For example, in developing procedures, NFA suggests that Members review the cybersecurity best practices and standards promulgated by the SANS Institute (SANS) [6], and/or the Open Web Application Security Project (OWASP) [7], and/or ISACA's Control Objectives for Information and Related Technology (COBIT) 5 [8], and/or the National Institute of Standards and Technology (NIST)[9]. Additionally, NIST

can be made available upon appropriate requests by NFA and the CFTC. Additionally, a Member should consider including definitions of the terminology used in its ISSP in order to facilitate reviews of its ISSP.

[6] SANS is a cooperative research and education organization in which auditors, network administrators and chief information security officers share lessons they learn and jointly find solutions to challenges. The SANS Institute's Critical Security Controls for Effective Cyber Defense as well as Implementing an Effective IT Security Plan are currently available at www.sans.org.

[7] OWASP is a worldwide not-for-profit organization focused on improving the security of Web software applications. Its mission is to make software security visible so that individuals and organizations worldwide can make informed decisions about true software security risks. OWASP cybersecurity guidance is currently available at www.owasp.org.

[8] ISACA is an independent, nonprofit global association that engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. Information about the COBIT 5 framework is currently available at www.isaca.org.

[9] NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life. Information about the NIST security and privacy controls is available at http://www.nist.gov/itl/csd/soi/fisma.cfm.

developed a process for use in creating an ISSP, which is described in the Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework).[10] NIST developed the NIST Cybersecurity Framework in response to Executive Order 13636 that, in part, called for the development of industry standards and best practices.

NFA does not require a Member to utilize any of these resources in developing its ISSP, but each Member must formally adopt an ISSP appropriate for the Member's business.[11]

- Security and Risk Analysis

Each Member firm has a supervisory obligation to assess and prioritize the risks associated with the use of its information technology systems. In appropriate circumstances, personnel from a Member firm's business unit(s), information technology, back-office, risk management and internal audit, if applicable, may be included in performing this assessment.

Members should maintain an inventory of critical information technology hardware with network connectivity, data transmission or data storage capability and an inventory of critical software with applicable versions. Members should identify the significant internal and external threats and vulnerabilities to at-risk data that is collected, maintained and disseminated, including customer and counterparty PII, corporate records and financial information; assess the threats to and the vulnerability of their electronic infrastructure including any systems used to initiate, authorize, record, process and report transactions relating to customer funds, capital compliance, risk management and trading; assess the threats posed through any applicable third-party service providers or software; and know the devices connected to their network and network structure.

Generally speaking, threats include loss, destruction or theft of critical hardware containing at-risk data; insertion of viruses, spyware and other malware; and

[10] The NIST Cybersecurity Framework is currently available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[11] In developing their ISSPs, Members are permitted to use more than one of these resources and use relevant portions of each as appropriate to their business and risk.

interception and compromising of electronic transmissions (*e.g.,* email and payment processing systems). In assessing security risks, Members should estimate the severity of the potential threats, perform a vulnerability analysis, and decide how to manage the risks of these threats. A Member's assessment should address past internal and external security incidents at the firm and, to the extent applicable and within a reasonable time, consider known threats identified by the firm's critical third-party service providers, the industry or other organizations.

- Deployment of Protective Measures Against the Identified Threats and Vulnerabilities

Members should document and describe in their ISSPs the safeguards deployed in light of the identified and prioritized threats and vulnerabilities. Adopted safeguards will be highly dependent upon a Member's size, business, technology, electronic interconnectivity with other entities and the potential threats identified in its risk assessment. Examples of these safeguards may include:

- protecting the Member's physical facility against unauthorized intrusion by imposing appropriate restrictions on access to the facility and protections against the theft of equipment;
- establishing appropriate identity and access controls to a Member's systems and data, including media upon which information is stored;
- using complex passwords and changing them periodically;
- using and maintaining up-to-date firewall and anti-virus and anti-malware software to protect against threats posed by hackers;
- using supported and trusted software or, alternatively, implement appropriate controls regarding the use of unsupported software;
- prevent the use of unauthorized software through the use of application whitelists;
- using automatic software updating functionality or, alternatively, manually monitoring the availability of available software updates and installing updates, and spot check to ensure that updates are applied when necessary;
- using supported and current operating systems or, alternatively, implement appropriate controls regarding the use of unsupported operating systems;

- regularly backing up systems and data as part of a sustainable disaster recovery and business continuity plan;
- deploying encryption software to protect the data on equipment in the event of theft or loss of the equipment;
- using network segmentation and network access controls;
- using secure software development practices if the Member develops its own software;
- using web filtering technology to block access to inappropriate or malicious websites;
- encrypting data in motion, (*e.g.,* encrypting email attachments containing customer information or other sensitive information), to reduce the risk of unauthorized interception; and
- ensuring that mobile devices are subject to similar applicable safeguards.

Members should also document and implement reasonable procedures to detect potential threats. These steps may include utilizing network monitoring software, watching for the presence on the Member's physical premises of unauthorized users and becoming members of threat/data sharing organizations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) [12] or establishing procedures designed to identify unauthorized connections by employees to the Member's network.

- Response and Recovery from Events that Threaten the Security of the Electronic Systems

Members should create an incident response plan to provide a framework to manage detected security events or incidents, analyze their potential impact and take appropriate measures to contain and mitigate their threat. Members should consider in appropriate circumstances forming an incident response team responsible for investigating an incident, assessing its damage and coordinating the internal and external response. A Member should consider including in its incident response plan a description of how the Member will address common types of potential incidents (*e.g.,* unauthorized access, malicious code, denial of service and inappropriate usage),

[12] Through contributions from firms across the financial services sector, information sharing organizations like FS-ISAC can help mitigate the effects of cyber attacks by analyzing incoming threat information and promptly notifying participants of potential attacks.

including how it will communicate internally with an appropriate escalation procedure and externally with customers/counterparties, regulators and law enforcement. In addition, Members should consider providing details of any detected threats to an industry-specific information sharing platform such as FS-ISAC.

Finally, the ISSP should contain a Member's procedures to restore compromised systems and data, communicate with appropriate stakeholders and regulatory authorities and incorporate lessons learned into the ISSP.

- Employee Training

A Member's ISSP should contain a description of the Member's ongoing education and training relating to information security for all appropriate personnel. This training program should be conducted for employees upon hiring and periodically during their employment and be appropriate to the security risks the Member faces as well as the composition of its workforce. Members should consider including as training topics social engineering tactics and other general threats posed for system compromise and data loss.

Review of Information Security Programs

Members should monitor and regularly review the effectiveness of their ISSPs, including the efficacy of the safeguards deployed, and make adjustments as appropriate. A Member should perform a regular review of its ISSP at least once every twelve months using either in-house staff with appropriate knowledge or by engaging an independent third-party information security specialist. Under appropriate circumstances, a Member's review may include penetration testing of the firm's systems, the scope and timing of which is highly dependent upon the Member's size, business, technology, its electronic interconnectivity with other entities and the potential threats identified in its risk assessment.

Third-Party Service Providers

A Member's ISSP should address in its security risk assessment the risks posed by critical third-party service providers that have access to a Member's systems, operate outsourced systems for the Member or provide cloud-based services such as data storage or application software to the Member. A Member should consider using a risk based approach to manage the information security risks posed by these providers. NFA recognizes that a Member's ability to manage the security risks posed by third-party service providers may be limited by the information these service providers elect to provide to the Member. Generally, a Member should perform due diligence on a critical service provider's security practices and avoid using third parties whose security standards are not comparable to the Member's standards in a particular area or activity. Members should consider including in their arrangements with critical third-party service providers appropriate measures that are designed to protect customer and firm confidential data. Members should also consider adopting procedures to place appropriate access controls to their information systems and data upon third-party service providers, and procedures to restrict or remove, on a timely basis, a third-party service provider's access to their information systems once the service provider is no longer providing services.[13]

Recordkeeping

All records relating to a Member's adoption and implementation of an ISSP and that document a Member's compliance with this Interpretive Notice must be maintained pursuant to NFA Compliance Rule 2-10.

NFA Compliance Rules 2-9, 2-36 and 2-49, as applicable, require NFA Members to develop, maintain and implement an appropriate ISSP in light of the importance of protecting the integrity of their technology systems. NFA recognizes that the particulars of a Member's ISSP will vary based on the Member's size, complexity of operations, type of customers and counterparties, and its electronic interconnectivity with other entities. There is no one-size-fits-all ISSP, and resources and processes that differ from those described above can be used to develop an appropriate ISSP.

EXPLANATION OF PROPOSED INTEPRETIVE NOTICE

The proposed Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49 requires Member firms to adopt and enforce written procedures to secure

[13] Additionally, Members whose data resides in third-party service provider systems should consider including procedures to respond to notices from a service provider that it has experienced a data breach as state laws may require the Member to notify its customers of the breach.

customer data and access to their electronic systems (Interpretive Notice). NFA believes that in light of the almost daily news about information systems security breaches at U.S. businesses, including financial institutions, and the significant threat and damage these breaches could cause to NFA's Member firms, customers, and the U.S. futures industry, it is appropriate for NFA to issue guidance to its Member firms.

In developing the Interpretive Notice, NFA reviewed guidance issued by other financial regulators including FINRA's February 2015 *Report on Cybersecurity Practices* that presents an approach to cybersecurity for broker-dealers grounded in risk management and the *Guidance Update* issued in April 2015 by the SEC's Division of Investment Management that discusses cybersecurity measures for investment companies and investment advisers. NFA also reviewed SIFMA's July 2014 *Small Firms' Cybersecurity Guidance* and the U.S. Department of Justice's April 2015 *Best Practices for Victim Response and Reporting of Cyber Incidents*. NFA's Interpretive Notice is consistent with the prior guidance issued by the other financial regulators. NFA will continue to monitor any forthcoming guidance from other regulators.

NFA believes that the proposed Interpretive Notice provides appropriate guidance to Member firms to address the supervision of information security. The Interpretive Notice adopts a principles-based risk approach and recognizes that, given the differences in Members' size and complexity of operations, the make-up of customers and counterparties serviced by Members, and the extent of Members' interconnectedness there must be some degree of flexibility in determining what constitutes "diligent supervision" in this area for each firm. The Interpretive Notice recognizes that a one-size-fits-all approach will not work for the application of these requirements. Nonetheless, the Interpretive Notice requires every Member to adopt and enforce an information systems security program (ISSP).

In order to develop and adopt an appropriate ISSP, the Interpretive Notice provides several possible resources for Members to consider, including the process described in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework). NIST developed the NIST Cybersecurity Framework in response to Executive Order 13636, which among other things, called for the development of industry standards and best practices. NFA does not require Members to utilize any of the resources listed in the Interpretive Notice in developing their ISSPs, but NFA expects each Member to use a formal process to develop an ISSP appropriate for the Member's business.

NFA's proposed Interpretive Notice requires an ISSP to cover several key areas, which are comparable to the areas addressed in the guidance issued by other regulators. Written ISSPs must be approved within Member firms by an executive level official and contain a security and risk analysis, a description of the safeguards deployed against identified threats and vulnerabilities, and the process used to evaluate the nature of a detected security event, understand its potential impact and take appropriate measures to contain and mitigate the breach. Additionally, the ISSP should describe the Member's ongoing education and training related to information systems security for all appropriate personnel. Lastly, the Interpretive Notice requires a Member to monitor and regularly review (i.e., at least every twelve months) the effectiveness of its ISSP, including the efficacy of the safeguards the Member has deployed, and make adjustments as appropriate, and requires Members' ISSPs to address the risks posed by critical third-party service providers.

NFA recognizes that some Members will already have ISSPs while others will need to devote a significant amount of time and resources to meet their obligations. Therefore, NFA believes that it may need to provide additional, more detailed guidance to Members including smaller IBs, CPOs and CTAs so that these firms may satisfy their obligations pursuant to the Interpretive Notice. Given that this framework is a significant new requirement for Members, NFA intends to develop an incremental, risk-based examination approach regarding the Interpretive Notice's requirements and we will initially work with Member firms to assist them in developing their ISSPs.

NFA's IB, CPO/CTA, FCM and Swap Dealer Advisory Committees have all reviewed the Interpretive Notice and expressed their support for its content. They also agreed with NFA's suggestion of a measured approach to implementation. Finally, each emphasized that additional education and guidance, especially for less technologically sophisticated Members, will be critical components of the implementation process.

NFA respectfully requests that the Commission review and approve the proposed adoption of the Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs.

Respectfully submitted,

Thomas W. Sexton

Thomas W. Sexton
Senior Vice President and
General Counsel

*The proposed adoption of the Interpretive Notice became effective March 1, 2016.