NSCP
THE NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

MARCH 2017 SPECIAL REPRINT
NSCP Currents

Reminder to Commodity Pool Operators and Commodity Trading Advisors: NOW is the Time to Get Your Information Systems Security Programs in Place

By Christina Hill and Brian Walsh

Introduction

If you are a Commodity Pool Operator ("CPO") or Commodity Trading Advisor ("CTA") and you have not made strides to put an effective Information Systems Security Program ("ISSP") in place, doing so should be blinking red on your dashboard.

Both the Commodity Futures Trading Commission ("CFTC") and the National Futures Association's ("NFA") recently stepped-up regulation in the realm of cybersecurity, and the development that most impacts CPOs and CTAs is the NFA's Interpretive Notice 9070 "Information Systems Security Programs," approved by the CFTC in October 2015 (the "Notice").[1] The Notice, which became effective on March 1, 2016, provides interpretive guidance with respect to NFA Compliance Rules 2-9, 2-36, and 2-49[2] – specifically that NFA Member firms, including CPOs and CTAs, must "adopt and enforce written policies and procedures to secure customer data and access to their electronic systems" in order to meet acceptable standards for supervisory procedures.[3] The NFA terms these written policies and procedures "Information Systems Security Programs" or "ISSPs." NFA Notice to Members I-15-23, in announcing the Notice, indicated that the NFA will not look for a uniform, "one-size-fits-all" approach to compliance; rather, Member firms must "adopt and enforce [ISSPs] appropriate to [their] circumstances."[4]

The NFA expects Members to have ISSPs in place that are tailored to each firm's business. This article is a reminder to CPOs and CTAs that NOW is the time to get your ISSPs in place, and provides some insight into the NFA's potential approach to enforcement, as well as an overview of what the NFA expects the ISSPs to contain.

Thoughts on the NFA's Approach to Enforcement

The overarching concern for the NFA is that Members make a good faith effort to produce adequate ISSPs. NFA compliance staff have stated publicly that their intention is not to immediately refer cases of inadequate ISSPs to the business conduct committee for enforcement action. However, NFA audit staff will expect to see a well thought-out ISSP, which will include or show consideration of the elements included in the Notice. Because NFA examinations are risk-based, and cybersecurity is considered a high-level risk, Members should expect examination staff to inspect their ISSPs and ask questions related to the firm's cybersecurity practices. NFA staff have indicated that examiners will ask about: (1) employee training; (2) how the firm ensures its ISSPs stay current; and (3) any cybersecurity threats or incidents experienced by the firm. Though the NFA has not yet taken enforcement action related to inadequate ISSPs, recent FINRA actions indicate that regulators are taking cybersecurity enforcement seriously, and imposing significant fines for noncompliance.[5]

1. The Notice is available at http://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9.
2. NFA Compliance Rules 2-9, "Supervision" available at https://www.nfa.futures.org/nfaManual/NFAManual.aspx?RuleID=RULE%202-9&Section=4; 2-36 "Requirements for Forex Transactions" available at https://www.nfa.futures.org/nfaManual/NFAManual.aspx?RuleID=RULE%202-36&Section=4, and 2-49 "Swap Dealers and Major Swap Participants Regulations" available at https://www.nfa.futures.org/nfaManual/NFAManual.aspx?RuleID=RULE%202-49&Section=4.

About the Authors

Christina Hill is an officer resident in the Washington, D.C. office of Murphy & McGonigle, www.mmlawus.com. She can be reached at chill@mmlawus.com.

Brian Walsh is an associate resident in the Washington, D.C. office of Murphy & McGonigle, www.mmlawus.com. He can be reached at bwalsh@mmlawus.com.

This article was originally published in the March 2017 issue of *NSCP Currents*, a professional journal published by the National Society of Compliance Professionals. It is reprinted here with permission from the National Society of Compliance Professionals. This article may not be further re-published without permission from the National Society of Compliance Professionals.

3. NFA Compliance Rule 2-9 is the operative provision vis-à-vis CPO and CTA compliance with the Notice. It requires CPOs and CTAs (among other NFA Members) to diligently supervise their employees and agents in all aspects of their futures activities. In addition to meeting the requirements of the Notice, CPOs and CTAs must comply with CFTC Regulation 160.30, which requires the adoption of "policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information."
4. NFA Notice to Members I-15-23, available at https://www.nfa.futures.org/news/newsNotice.asp?ArticleID=4649.
5. FINRA announced on December 21, 2016 that it had fined 12 firms a combined $14.4

What does the NFA expect to be in the ISSP?

The Notice provides that NFA Members' ISSPs must be written documents, tailored to the firm's business, designed to protect against security threats to the firm's technology systems.[6] The NFA notes that the Notice "adopts a principles-based risk approach to allow Member firms some degree of flexibility in determining what constitutes 'diligent supervision,' 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." The firm's ISSP must be approved in writing by an executive level official and senior management should periodically update the firm's board of directors or similar governing body regarding the ISSP.

Security and Risk Analysis

Member firms' ISSPs must provide for the assessment and prioritization of risks associated with the firm's information technology ("IT") systems. In furtherance of this assessment, members must: (1) maintain an inventory of critical IT hardware that can store or transmit data, and critical software, and be aware of devices connected to their networks; (2) assess the significant threats – internal and external – to sensitive data held or transmitted by the firm; (3) assess the threats to and vulnerabilities of the firm's electronic infrastructure; and (4) assess the threats to any third-party service providers utilized by the firm (including threats identified by the third-party as well as by the Member firm). Members' threat assessments should include an analysis of the severity of risks, a prioritization of risks, and a plan to manage the risks identified.

Deployment of Protective Measures Against the Identified Threats and Vulnerabilities

Member firms' ISSPs must detail the security safeguards – electronic and physical – used by the firm to address the risks and vulnerabilities identified through its assessment. The Notice provides Members a detailed list of examples of safeguards firms may employ. Additionally, ISSPs must discuss the firm's procedures for detecting potential threats.

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

Member firms' ISSPs must contain an incident response plan ("IRP") to establish procedures for managing security events. The NFA instructs that IRPs should provide how firms will analyze security events' impact and respond in a manner that will contain and mitigate the threat. The IRP should describe how the firm will respond to common types of threats, and detail how the threat will be communicated to others, including both internal escalation and to external parties, such as regulators and law enforcement. Firms' IRPs may include the involvement of an incident response team made up of firm employees tasked with responding to security events.

Employee Training

Member firms' ISSPs must provide for ongoing education and training of firm employees relating to information security. The Notice suggests that such training take place as part of the onboarding process as well as periodically.

Third-Party Service Providers

In addition to analyzing the risk posed by third-party service providers, Member firms should conduct a due diligence assessment of the provider's security practices prior to engaging the provider, and avoid using providers whose security standards are not compatible or substandard vis-à-vis the Member's. The Notice suggests that Members include provisions in their contractual arrangements with third-parties that protect customer and firm data. Additionally, the Notice suggests that Members place limits on third-party access to Member and customer data, and institute procedures to remove the third-party's access to the firm's information on a timely basis upon the conclusion of the service relationship.

Ongoing Evaluation of the ISSP and Recordkeeping

Member firms must monitor and regularly ensure that their ISSPs are effective, and amended as necessary to ensure effectiveness. ISSPs should be reviewed at least annually, and such review should include penetration testing. Member firms must keep records related to their adoption and implementation of ISSPs, as well as the Member's compliance with the Notice, pursuant to NFA Compliance Rule 2-10.

Conclusion

The NFA expects that Members are taking the Notice seriously, and making a diligent effort to put ISSPs into place. Accordingly, Members should be dedicating sufficient resources to ensure they have acceptable ISSPs as soon as possible, and certainly prior to their next NFA examination. ★

million for failing to ensure that customer records could not be altered, and that records were kept in "write once, read many" ("WORM") format. FINRA indicated that the cases reflect its focus on cybersecurity because unsecured data can be vulnerable in the case of cyberattacks. Additionally, certain settlements included sanctions for failing to obtain third-party vendor attestations and failing to implement adequate supervisory systems.

6. On February 29, 2016, the NFA released Notice I-16-10, which informed Members that the NFA added a cybersecurity section to the "Self-Examination Questionnaire", which can be used as a tool to assist Members to develop and implement adequate ISSPs. http://www.nfa.futures.org/news/newsNotice.asp?ArticleID=4701. Self-Examination Questionnaire is available at http://www.nfa.futures.org/NFA-compliance/publication-library/self-exam-questionnaire-general.pdf. See also "FAQs: NFA Cybersecurity Interpretive Notice", available at http://www.nfa.futures.org/NFA-compliance/NFA-general-compliance-issues/faqs-cybersecurity-interpretive-notice.pdf.