CYBERSECURITY UPDATE: NATIONAL FUTURES ASSOCIATION ADOPTS CYBERSECURITY GUIDANCE FOR MEMBER FIRM INFORMATION SYSTEMS SECURITY PROGRAMS

Date: 1 December 2015

Investment Management Alert

By: Mark C. Amorosi, Marguerite W. Laurent

The Commodity Futures Trading Commission (CFTC) recently approved the National Futures Association's Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49, entitled Information Systems Security Programs (the "Cybersecurity Guidance"). The Cybersecurity Guidance requires member firms to adopt and enforce written policies and procedures to secure customer data and access to their electronic systems. The Cybersecurity Guidance will become effective on **March 1, 2016**, and applies to all member categories -- commodity pool operators ("CPOs") (including CPOs for mutual funds and other investment companies registered under the Investment Company Act of 1940), commodity trading advisers ("CTAs"), futures commission merchants, swap dealers, major swap participants, introducing brokers ("IBs") and forex dealer members.

The Cybersecurity Guidance sets forth a detailed series of recommendations for NFA member firms. The Cybersecurity Guidance effectively will require firms to undertake substantial cybersecurity program reviews, including conducting risk assessments, reviewing compliance policies and procedures and incident-response protocols, and reviewing technical systems and safeguards and vendor relationships to seek to ensure NFA member firms' practices are consistent with the Cybersecurity Guidance. Firms should carefully review and consider the recommendations included in the Cybersecurity Guidance, as it is likely that they will be the basis for future NFA regulatory initiatives, including on-site examinations of member firms and, potentially, disciplinary matters. This is particularly true given regulators' increased interest in bringing "message cases" in the enforcement context involving, among other areas, cybersecurity, including the recent SEC enforcement action against a registered investment adviser for alleged violations of the "Safeguards Rule" under Regulation S-P.

BACKGROUND

The NFA is issuing the Cybersecurity Guidance under NFA Compliance Rules 2-9, 2-36, and 2-49, which generally impose obligations on NFA member firms to diligently supervise their businesses, employees, and agents in all aspects of their commodity interest activities.

The NFA's cybersecurity rules and interpretations traditionally have focused on the protection of personally identifiable information ("PII") of customers. The Cybersecurity Guidance, however, applies not only to the protection of PII, but also to operational security matters more generally. Furthermore, while the Cybersecurity Guidance is similar in substance to guidance provided by other regulators (*see*, *e.g.*, the SEC staff's IM Guidance

©2005-2026 K&L Gates LLP. All Rights Reserved.

Update on cybersecurity), it includes numerous, more detailed recommendations regarding cybersecurity compliance expectations.

CYBERSECURITY GUIDANCE

The major elements of the Cybersecurity Guidance are as follows:

Written Information Systems Security Program

The Cybersecurity Guidance states that each NFA member firm should establish and implement a written governance framework that supports informed decision-making and escalation within the firm to seek to identify and manage information security risks. In particular, the Cybersecurity Guidance states that:

- Each member must adopt and enforce a written information systems security program ("ISSP") reasonably designed to provide safeguards appropriate to the member's size, complexity, customers and counterparties, 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.
- Each member's ISSP should be approved, in writing, by the member's chief executive officer, chief technology officer, or other executive-level official.
- Member firms' senior management should provide periodic board reports (or reports to a similar governing body, committee, or delegate) to enable the board to monitor the member's information security efforts.
- Each member should monitor and conduct an annual review of the effectiveness of their ISSPs, which review may include penetration testing of the firm's systems, and make adjustments as appropriate.

In developing an ISSP, the Cybersecurity Guidance recommends, but does not require, that member firms use one of the many cybersecurity frameworks that have been published (*e.g.*, the National Institute for Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity). The Cybersecurity Guidance notes that ISSP policies and procedures may be documented in a single document or in documents maintained throughout various departments, so long as the ISSP can be made available to the NFA and the CFTC, upon appropriate request. Furthermore, the Cybersecurity Guidance recommends firms should define the terminology used in ISSPs to facilitate reviews of the ISSP.

Also, the Cybersecurity Guidance recognizes NFA member firms may be part of a larger holding company structure sharing common information systems security personnel, resources, systems, and infrastructure. 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 in these circumstances 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, the member firm can meet its supervisory responsibilities 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, the member firm will continue to have an obligation to ensure that all written policies and procedures relating to the

©2005-2026 K&L Gates LLP. All Rights Reserved.

program are appropriate to its information security risks, are maintained in a readable and accessible manner, and can be produced upon request to NFA and the CFTC.

Security and Risk Assessment

The Cybersecurity Guidance also states that NFA member firms have supervisory obligations requiring them to assess and prioritize the risks associated with their use of information technology. According to the Cybersecurity Guidance, the following topics should be addressed within the assessment:

- Developing and maintaining 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;
- Identifying the significant internal and external threats and vulnerabilities to at-risk data that is collected, maintained, and disseminated (e.g., customer and counterparty PII, corporate records, and financial information);
- Assessing the threats to, and the vulnerability of, electronic infrastructure, including any systems used to initiate, authorize, record, process, and report transactions relating to customer funds, capital compliance, risk management, and trading;
- Assessing the threats posed through any applicable third-party service providers or software; and
- Identifying the devices connected to the firm's network and network structure.

Deployment of Protective Measures Against Identified Threats and Vulnerabilities

The Cybersecurity Guidance further states that NFA member firms should document and describe the safeguards they deploy in light of identified and prioritized threats and vulnerabilities in their ISSPs. The Cybersecurity Guidance provides a list of example safeguards, including physical safeguards, access controls, firewalls and anti-virus and anti-malware software, software and operating system updates, software whitelists, regular backups, business continuity and disaster recovery capabilities, encryption, network segmentation, web filtering, and mobile device safeguards.

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

The Cybersecurity Guidance also makes clear that NFA member firms should create an incident response plan to provide a framework to manage detected security events or incidents, analyze their potential effect, and take appropriate measures to contain and mitigate such threats. The Cybersecurity Guidance specifically suggests that member firms should consider the following in developing an incident response plan:

- Under the appropriate circumstances, forming an incident response team responsible for investigating an incident, assessing its damage, and coordinating an internal and external response.
- Including in its incident response plan a description of how the member firm will address common types of potential incidents (*e.g.*, unauthorized access, malicious code, denial of service, and inappropriate

©2005-2026 K&L Gates LLP. All Rights Reserved.

usage), including how it will communicate internally with an appropriate escalation procedure, and externally with customers/counterparties, regulators, and law enforcement. In addition, member firms should consider providing details of any detected threats to an industry-specific information-sharing platform, such as FS-ISAC (https://www.fsisac.com/).

- Member firms should include procedures to restore compromised systems and data, communicate with appropriate stakeholders and regulatory authorities, and incorporate lessons learned into the ISSP.

Other Components of an ISSP

The Cybersecurity Guidance also includes the following that the NFA indicates should be part of a member firm's ISSP:

- *Employee Training*. ISSPs should contain, among other things, a description of the member firm's ongoing education and training relating to information security for all appropriate personnel.
- *Third-Party Service Providers*. ISSPs should address, as part of the security risk assessment, the risks posed by critical third-party service providers that have access to a member firm's systems; operate outsourced systems for the member; or provide cloud-based services, such as data storage or application software, to the member. The NFA recommends that member firms employ various techniques to limit the cyber risks of using third-party service providers, including performing due diligence on critical service providers' security practices; avoiding use of third parties whose security standards are not comparable to the member's standards, including in their arrangements with critical third-party service providers appropriate measures that are designed to protect customer and firm confidential data; implementing access controls on third-party service providers; and restricting or removing, on a timely basis, a third party's access to information systems once the service provider is no longer providing services.
- *Recordkeeping*. All records relating to a member firm's adoption and implementation of an ISSP and that document a member's compliance with the Cybersecurity Guidance must be maintained pursuant to NFA Compliance Rule 2-10.

Conclusion

The CFTC and NFA each stated earlier this year that cybersecurity would be a significant regulatory priority for each organization going forward. The Cybersecurity Guidance is a significant element of the NFA's initiatives in this area, and the content of the guidance could be the basis for future regulatory, inspection, and enforcement actions by the NFA related to cybersecurity failures. The March 1, 2016 compliance date is relatively soon, and therefore it is important for NFA member firms to review their cybersecurity programs to seek to ensure they are consistent with the Cybersecurity Guidance.

©2005-2026 K&L Gates LLP. All Rights Reserved.

KEY CONTACTS



MARK C. AMOROSI
CO-LEAD PRACTICE AREA LEADER - ASSET MANAGEMENT AND INVESTMENT FUNDS

WASHINGTON, DC
+1.202.778.9351
MARK.AMOROSI@KLGATES.COM



MARGUERITE W. LAURENT
PARTNER

WASHINGTON, DC
+1.202.778.9403
MARGUERITE.LAURENT@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.