January 9, 2019

The New Year Rings in New Requirements for NFA Member Asset Managers

Attorneys
Deborah A. Monson
Jeremy A. Liabo
Anne Fox
Erin M. Fredrick Conklin

In the final weeks of 2018, the National Futures Association ("NFA") issued new requirements applicable to asset managers who are members of the NFA that will take effect in 2019. First, the NFA amended its Interpretive Notice 9070, "NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs" (the "Cybersecurity Notice"). The amended Cybersecurity Notice adds an NFA notification obligation, employee training requirements, and specific approval procedures to the written information systems security program ("ISSP") required of each NFA member firm (a "firm") under the original Cybersecurity Notice issued in 2016. In addition, Interpretive Notice "NFA Compliance Rule 2-9: CPO Internal Controls System" (the "Internal Controls Notice") requires commodity pool operator ("CPO") members to establish a system of internal controls and provides guidance on designing and implementing such controls. The Cybersecurity Notice will become effective on April 1, 2019 and we expect the Internal Controls Notice to be effective on April 1 or soon thereafter.

Information Systems Security Programs

The original Cybersecurity Notice took effect in March 2016 and requires each NFA member firm to put in place an ISSP reasonably designed to address the risk of and response to unauthorized access to or attack of the firm's information technology systems. The amended Cybersecurity Notice (the "Amendments") requires, among other things:

- prompt notification to NFA of cybersecurity incidents related to a firm's commodity interest business that result in a loss of client or counterparty funds or a loss of the firm's capital, and notice to NFA if the firm notifies clients or counterparties of the incident pursuant to state or federal law,
- ongoing employee training upon hiring and at least annually thereafter, as well as written enumeration of specific training topics, and
- approval of the ISSP by a senior officer with primary responsibility for information security or another listed principal with the authority to supervise implementation of the ISSP, and if the firm is part of a holding company structure with a consolidated entity ISSP approved at the parent company level, then the firm's approval must indicate that the consolidated entity ISSP is appropriate for the firm.

These Amendments reflect requirements that NFA staff have required of members during routine on-site exams.

* * *

NFA Compliance Rules 2-9, 2-36 and 2-49 place continuing responsibilities on NFA member firms, including CPOs and commodity trading advisors, to diligently supervise employees and agents in all aspects of their commodity interest business. Pursuant to those rules, the Cybersecurity Notice sets forth general requirements for ISSPs, but allows each firm some flexibility to adopt and implement procedures tailored to its particular circumstances. To that end, the Cybersecurity Notice addresses a range of issues, including the contents and approval of a written ISSP, security and risk analysis practices, deployment of protective measures, incident response and recovery plans, employee training, procedures for internal review of a firm's ISSP, dealings with third-party service providers, and recordkeeping obligations.

Amendments to Written Program Requirements

The Amendments modify the NFA's guidance on how firms should incorporate the best practices of relevant professional associations into their written ISSPs. The NFA's original guidance suggested that, in the process of developing an appropriate ISSP, members should refer to the cybersecurity standards of certain professional organizations identified in the Cybersecurity Notice.

The Amendments remove references to specific professional and standard-setting organizations. Instead, firms are advised to consult the NFA's "Frequently Asked Questions on Cybersecurity", which will enable the NFA to provide additional resources and more timely updates to relevant information.

In addition, the original Cybersecurity Notice required an ISSP to be approved in writing by the firm's Chief Executive Officer ("CEO"), Chief Technology Officer ("CTO"), or other executive level official. The Amendments acknowledge that "executive level official" is not a universally used term among NFA members, and, to align with current practice in the industry, state that a firm's ISSP may approved by the CEO or other senior officer with primary responsibility for information system security (such as the CTO or Chief Information Security Officer ("CISO")), or by a senior official that is listed as a principal and has the authority to supervise ISSP implementation. If a firm has a committee that approves the ISSP, the committee must include one of these persons.

Where a firm relies on the ISSP of a parent company, the firm's CEO, CTO, CISO (or person with equivalent responsibility), or a senior official who is a listed principal of the firm must confirm in writing that the consolidated entity ISSP is appropriate for the firm's information security risks.

These Amendments are helpful in providing flexibility by acknowledging firm practices as well as business and governance structures.

Amendments to Incident Response and Recovery Requirements

The Amendments update the NFA's guidance on the parameters of an appropriate response to a cybersecurity event. The original Cybersecurity Notice suggested that incident response plans should address specific types of cybersecurity incidents, including unauthorized access, malicious code, denial of service, and inappropriate usage. The Amendments add data loss and ransomware attacks to the list of threats an ISSP should consider.

The Amendments further direct firms to familiarize themselves with notice requirements set forth in applicable U.S. and non-U.S. data security and privacy rules and regulations. The Amendments also suggest that firms should acquire the contact information of any regulatory bodies, self-regulatory organizations and law enforcement bodies prior to any incident.

Amendments to Employee Training Requirements

With respect to the frequency of employee cybersecurity training, the Amendments update the existing obligation from a "periodic" requirement to an annual requirement, with the caveat that more frequent trainings must occur if warranted. The Amendments continue to require that employees receive cybersecurity training upon hiring as well.

Additionally, the Amendments provide that an ISSP should identify the specific cybersecurity topics covered in the firm's employee training. The Amendments continue to highlight "social engineering tactics and other general threats posed for system compromise and data loss" as key topics to consider in employee trainings.

We note that the NFA has been requiring firms to conduct cybersecurity training upon hiring and at least annually, rather than periodically, thereafter when it conducts routine on-site audits of its members. While the Amendments are helpful in that they put this requirement in writing and make it public, the requirement creates issues for firms that are part of a consolidated entity ISSP that does not call for annual training, in that they must now identify persons throughout the consolidated organization that need NFA-required training and specially conduct more frequent training for them. A trap

for the unwary is that the NFA generally considers "annually" to mean once in each 12-month period, rather than once each calendar year. We also remind firms to keep records of each training presentation and of each person's completion of such training.

Addition of Notice Requirement

The Amendments provide that ISSPs must include procedures to promptly notify the NFA of any cybersecurity incident relating to a firm's commodity interest business that results in (i) any loss of client or counterparty funds; (ii) any loss of the firm's own capital; or (iii) the triggering of a requirement under state or federal law whereby the firm must provide notice to its clients or counterparties.

The notice to the NFA must include a written summary of the cybersecurity event, including all relevant details. If the firm is required to provide notice of the cybersecurity event to clients or counterparties under state or federal law, a copy of such notice may be provided to the NFA instead of a separate written summary. Additionally, if state or federal law requires the distribution of "substantially identical notices" to multiple parties in respect of a single incident, the firm need only provide one example copy to the NFA. Prior to the April 1, 2019 effective date, the NFA will issue instructions for how firms are to provide notice to the NFA.

We recommend that firms seek legal advice prior to providing notice to the NFA to discuss and consider timing, content and the broad ramifications of making the filing.

As provided in the original Cybersecurity Notice, each firm should continue to monitor and regularly review its ISSP to gauge effectiveness and make adjustments as necessary. Such reviews should occur at least annually either by qualified in-house personnel or by an independent third-party specialist.

Internal Controls

The Internal Controls Notice will require CPO members to implement an internal controls system designed to safeguard customer funds, deter fraud, assure the reliability and accuracy of financial reports and ensure the CPO's operations comply with applicable NFA and CFTC rules and regulations.

In the Internal Controls Notice, the NFA acknowledges that what constitutes an effective system of internal controls will differ based on the size and complexity of the CPO. However, the NFA expects every system of internal controls to include certain key components.

1. **Internal Controls System:** A CPO must have a strong control environment that includes written policies and procedures reasonably designed to ensure the CPO's compliance with applicable rules and regulations and a management team that demonstrates a commitment to integrity and ethical values. Policies and procedures should include an escalation policy by which employees may report to senior management individuals who have attempted to circumvent the CPO's internal control systems. The NFA expects policies and procedures to be updated on an ongoing basis.

2. **Separation of Duties:** The internal controls system should include a separation of duties, when possible, to ensure that no single employee is in a position to carry out and conceal errors or fraud or have control over any two phases of a transaction or operation involving the CPO's commodity interest business. Specifically, the NFA expects, whenever possible:

    a. Duties to be assigned to different employees in a manner, or appropriate automated controls, that ensure regular cross-checking of work in material areas;

    b. Operational functions relating to the custody of pool assets to be separate from financial reporting functions, such as recordkeeping and accounting for the assets; and

c. With respect to pool funds (*e.g.*, subscriptions, transfers, and redemptions), no one person to be responsible for initiating a transaction, approving the transaction, recording the transaction, and reconciling the account to third-party documentation and information.

3. **Risk Assessment:** Each CPO should conduct a risk assessment of its business operations and establish controls to address each risk area. The NFA identifies in the Internal Controls Notice three risk areas that are generally applicable to CPOs and control activities that would form the basis of an adequate internal controls system.

   a. *Pool subscriptions, redemptions and transfers*: An effective internal control system should be reasonably designed to safeguard participant and pool assets. The controls should include (i) verification that pool investments are held in properly titled accounts and not commingled with other assets; (ii) regular reconciliation of transactions between the pool's general ledger and the records of third-party custodians; (iii) verification of redemption requests and the proper distribution of proceeds to pool participants; and (iv) verification that the CPO does not make a prohibited loan of pool assets.

   b. *Risk management and investment and valuation of pool funds*: Risk controls with respect to a CPO's investment activities should include (i) verification that each investment type is authorized and consistent with the pool's strategies; (ii) verification that investments are valued in accordance with the CPO's valuation policies; (iii) verification that counterparties and third-party depositories are subject to ongoing due diligence; (iv) ongoing monitoring of risks associated with investments held at third parties, including market and credit risk; and (v) ongoing monitoring of pool liquidity to ensure the pool is able to satisfy redemption requests, margin calls and other financial obligations.

   c. *Use of third-party administrators*: An adequate system of controls with respect to third-party administrators should include (i) initial and ongoing due diligence of administrators; (ii) obtaining evidence of a test of controls and security measures at the administrator conducted by an internal audit department or independent specialist; and (iii) a system for ensuring the CPO's records and financial statements are in agreement with those of the administrator.

4. **Recordkeeping:** A CPO must maintain records to support the implementation and effectiveness of its internal controls system.

The components of an adequate internal controls system discussed in the Internal Controls Notice are not exhaustive. Rather, each CPO member is expected to conduct its own review of its business and determine whether, based on its size, operations and activities, other areas should be included in its internal control systems.

The NFA notes that CPOs may have already developed controls and processes in response to similar requirements of other regulators and that such controls and processes may satisfy NFA Compliance Rule 2-9. Nevertheless, each CPO should carefully evaluate its existing internal controls system in light of the Internal Controls Notice to ensure that it is in compliance with all CFTC and NFA requirements.

Please contact Deborah A. Monson, Jeremy A. Liabo, Anne C. Fox, Erin M. Fredrick Conklin or the Ropes & Gray attorney who usually advises you for further information, or with any questions you may have.