Investment Management Alert

Akin Gump
STRAUSS HAUER & FELD LLP

NFA Issues Interpretive Notices for CPOs Regarding Internal Controls Systems and Cybersecurity

January 15, 2019

Contact

Jan-Paul Bruynes
jpbruynes@akingump.com
+1 212.872.7457
New York

Jason M. Daniel
jdaniel@akingump.com
+1 214.969.4209
Dallas

Mereen Miran
Director of Business Development
mmiran@akingump.com
+1 212.407.3050
New York

Key Points

- The NFA has determined that registered CPOs must implement an internal controls system and highlighted best practices for such a framework.
- In response to certain frequently asked questions, the NFA has also updated its guidance on how NFA members, including CPOs, can comply with cybersecurity requirements.

Internal Controls System

The National Futures Association (NFA) adopted an Interpretive Notice[1] providing that, effective April 1, 2019, registered commodity pool operators (CPOs) must implement an internal controls system that is designed to deter fraudulent activity by employees (including management) and third parties in order to protect customer funds, provide reasonable assurances that the books and records of the CPOs' commodity pools are reliable, and that the CPOs are in compliance with all Commodity Futures Trading Commission (CFTC) and NFA requirements. While acknowledging that there can be no "one-size-fits-all" approach for CPOs due to differences in size and complexity of operations, the NFA highlighted the following guidance when designing an internal system of controls:

Written Policies and Procedures. CPOs must adopt written policies and procedures that (i) are designed to ensure that they comply with all CFTC and NFA requirements, (ii) demonstrate the CPOs' commitment to integrity and ethical values, (iii) explain the internal controls framework and supervisory system, and (iv) provide for escalation procedures to senior management of potential violations of internal controls (and whether and when reporting to regulators should occur).

Separation of Duties. CPOs should require that duties are assigned to different employees to ensure that no single employee is in a position to carry out and conceal errors or fraud or have control over two phases of a transaction or operation. The NFA,

in particular, stated that different employees should be involved in the areas of handling customer funds, trade execution, financial records and risk management such that regular cross-checking of work occurs; operational and financial reporting functions are completely segregated; and no one person handles each stage of a pool's subscription, transfer or redemption processes.

Risk Assessment. While CPOs should conduct ongoing internal risk assessments to determine specific areas of the firm's operations in need of controls, at a minimum, each CPO's internal controls system must address pool subscriptions, redemptions and transfers, risk management and investment and valuation of pool funds, and use of administrators.

Recordkeeping. CPOs must maintain records that support the implementation and effectiveness of their internal controls systems.

Monitoring. CPOs should monitor the effectiveness of their controls to ensure that they are functioning properly and make adjustments where appropriate.

Cybersecurity

In March 2016, the NFA adopted an Interpretive Notice requiring all NFA members ("Members"), including CPOs, to adopt a written information systems security program (ISSP) to address the risk of unauthorized access to, or attack of, their information technology systems and to respond appropriately should any breach occur. The NFA adopted amendments to this notice that go into effect April 1, 2019, to clarify certain frequently asked compliance questions that have been posed since the Interpretive Notice was first issued:[2]

Training. The NFA clarified that Members must train employees regarding the firm's ISSP upon hiring, at least annually thereafter and more frequently if information security risks warrant such extra training. Members must also identify specific topical areas covered by the training program.

Approval of the ISSP. Instead of referring to an "executive level officer," the NFA has clarified that any "senior level officer with primary responsibility for information security or other senior official who is a listed principal and has the authority to supervise the Member's execution of its ISSP" may initially approve the Member's ISSP (e.g., Chief Executive Officer, Chief Technology Officer or Chief Information Security Officer). If a Member participates in a consolidated entity ISSP that has been approved at the parent company level, then one of the foregoing individuals still must certify in writing that the ISSP is appropriate for the Member's cybersecurity risks.

Notification to the NFA. The NFA clarified that, as part of the existing requirement to notify external parties of cybersecurity incidents, Members must notify the NFA itself when the cybersecurity incident results in the loss of customer or counterparty funds or the Member's own capital, or the Member otherwise notifies its customers or counterparties pursuant to state or federal law.

---

[1] See NFA Compliance Rule 2-9: CPO Internal Controls System, available at https://www.nfa.futures.org/news/PDF/CFTC/Interp-Notc-CR-2-9-CPO-Internal-Controls-System.pdf.

[2] See NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs, available at https://www.nfa.futures.org/news/PDF/CFTC/Interp-Notc-NFA-CR-2-9-2-36-and-2-49-Information-Systems-Security-Programs.pdf.