Proskauer

NFA Issues Guidance on Information Systems Security Programs and CPO Internal Controls Systems

March 5, 2019

The NFA has amended its existing guidance to its members on Information Systems Security Programs (ISSPs), and has adopted a new Interpretive Notice related to commodity pool operator internal controls systems. Both will become effective on April 1, 2019.

ISSPs

The new ISSP guidance, which applies to all NFA members, provides additional clarity on training requirements and the level of management at which an ISSP must be approved.

Specifically, NFA members are required to identify the topics covered during ISSP training and are required to train employees when hired, at least annually thereafter, and more frequently if circumstances warrant.

ISSPs must now be approved by each member's CEO or another senior level officer with primary responsibility for information systems security (*e.g.*, the Chief Technology Officer (CTO) or Chief Information Security Officer (CISO)). The amendment further clarifies that, although an NFA member firm can participate in a consolidated group ISSP, each member still has an independent obligation to ensure that all written policies and procedures relating to the ISSP are appropriate to its information security risks, and can be produced upon request to the NFA and the CFTC.

Also included in the amended ISSP guidance is a new requirement that NFA members notify the NFA of cybersecurity incidents related to their commodity interest business that result in a loss of customer or counterparty funds or loss of a member firm's capital, or where a member notifies its customers or counterparties of an incident pursuant to state or federal law.

CPO Internal Controls System

The NFA has adopted an Interpretive Notice which requires CPOs to develop an internal controls system designed to deter errors and fraudulent activity, protect customer funds, and produce financial reports that are timely, accurate and reliable.

The Interpretive Notice specifically focuses on the creation of a strong controls environment and management's commitment to integrity and ethical values. At a minimum, this means that a CPO must adopt and implement:

- written policies and procedures reasonably designed to ensure that the CPO's operations are in compliance with applicable NFA rules and CFTC regulations; and
- written policies and procedures that fully explain the CPO's internal controls framework.

While the Notice acknowledges that internal controls systems will vary based on a CPO's size and the complexity of its operations, it states that every CPO should conduct a risk assessment to identify its most critical risks and develop and implement controls to address those risks. The Notice highlights the importance of adequate controls with respect to subscriptions, redemptions and transfers, risk management, and investment and valuation of pool assets. The Notice also stresses that there should be a separation of duties, when possible, to ensure that no single employee is in a position to carry out or conceal errors or fraud or have control over any two phases of a transaction or operation.

https://www.nfa.futures.org/rulebook/rules.aspx?Section=9&RuleID=9070

https://www.nfa.futures.org/rulebook/rules.aspx?Section=9&RuleID=9074