ALERTS

NFA Update: New Supervision and Cybersecurity Obligations for Private Fund Managers Registered with the National Futures Association

February 1, 2019

The National Futures Association issued two Interpretive Notices that will affect all private fund managers that are NFA members (i.e., managers with funds or accounts that trade commodity interests and that are not eligible for an exemption from registration with the Commodity Futures Trading Commission). While the Interpretive Notices address different areas of risk — one is focused on the need for more formal supervision of key financial functions, and the other is focused on addressing cybersecurity risks — they both require the attention of senior administrative personnel. Given that the obligations set forth in these notices will become effective on April 1, 2019, all affected managers should take steps to ensure timely compliance.

The Internal Control Systems Interpretive Notice

On Jan. 31, 2019, the NFA announced that it had adopted a new interpretive notice, "Compliance Rule 2-9: CPO Internal Control System" (the "Internal Controls Notice")[1], which is directed at commodity pool operators with control over customer funds.

As background, NFA Compliance Rule 2-9 imposes a general requirement for NFA members (including CFTC-registered private fund managers) to "diligently supervise" their personnel. The NFA interprets that general rule

as requiring a "strong control environment" with internal controls that are designed to deter fraud and errors in order to safeguard customer funds, to reliably produce accurate and timely financial reports, and to cause compliance with all regulations addressing the control of customer funds. The Internal Controls Notice is intended to supplement Compliance Rule 2-9 and provide CPOs with guidance on the design of an adequate financial controls system as well as to set forth certain "minimum components" of such a system.

A Strong Control Environment. Unsurprisingly, the Internal Controls Notice expressly requires the adoption and implementation of written compliance policies. However, compliance personnel should note that the Internal Controls Notice specifically requires the adoption of *two different sets* of written policies and procedures:

- Policies and procedures reasonably designed to ensure that a CPO's operations are in compliance with all applicable NFA rules and CFTC regulations; and
- Policies and procedures that fully explain a CPO's internal controls framework and describe the CPO's supervisory system, "which should be reasonably designed to ensure that [they] are diligently followed by all employees."

While the obligation to address *both* policy objectives is a fairly subtle point in the Internal Controls Notice, legal and compliance personnel should ensure that the design of their policies, as well as all periodic reviews of their effectiveness, expressly benchmark the firm's systems against both objectives.

The NFA also made clear in the Internal Controls Notice that the behavior of senior personnel is an integral element of a strong control environment. The notice states that "management must demonstrate its commitment to integrity and ethical values and emphasize the importance of establishing and following the internal controls" and that "no employee, including senior management, should inappropriately circumvent the firm's internal controls system." While these concepts are not new in the asset management industry, this express individual mandate for senior personnel (and not just for compliance personnel) is consistent with a broader regulatory shift.

The non-circumvention concept is also expressed in a requirement that the firm have an "escalation policy" that (1) provides a mechanism for reporting *attempts* to improperly override a firm's internal controls system "in any respect" and (2) addresses "whether and when a matter should be reported to the firm's regulator." Legal and compliance officers should consider these aspects of the Internal Controls Notice carefully, as they may differ in some details from many firms' current practices.

In a footnote, the NFA also set forth an additional element of an effective internal controls system, stating that the overall compliance program "should be supported by strong information technology controls operating within the firm's Information Systems Security Program." Compliance officers, when performing reviews and assessments, should take note of this and ensure that reviews of their information security systems and their cybersecurity measures are incorporated into their overall control system assessments.

Separation of Duties. The Internal Controls Notice also advises that, to the extent possible, persons who perform day-to-day functions in the following areas should be different from the persons who supervise those functions:

- Handling funds;
- Trade execution activities;
- Financial records; and
- Risk management.

And, where a supervisor also handles day-to-day functions, a principal of the CPO (or other supervisory person) should periodically review the supervisor's work. In other words, whenever possible, the CPO's policies should require that:

- There is cross-checking of work in key areas, either by assigning duties to different employees or by implementing automated controls;
- Operational functions that involve handling or the custody of pool assets are separated from financial reporting functions; and
- No one person should be responsible for the full lifecycle of subscriptions, transfers and redemptions to or from a pool (or transactions that present similar risks).

The NFA believes that the separation of duties is "widely accepted as a key control activity." Therefore all CPOs should review their operational processes and financial controls to carefully consider the adequacy of their supervision framework in light of the NFA's advice on separation of duties.

Controls Over Investment Activity and Financial Transactions. The Internal Controls Notice also highlighted two common areas of risk (financial transactions between pools and their investors and investment decision-making) and suggested specific steps that would "form the basis of" adequate internal controls in these areas.

The Internal Controls Notice proposes that, to reduce the financial and operational risks associated with pool subscriptions, redemptions and transfers (and to protect participant and pool assets), a CPO should:

- Verify that pool investments are held in accounts properly titled with the pool's name and are not commingled with the assets of any other person;[2]
- Periodically reconcile transactions between the pool's general ledger, banks and other third-party depositories;
- Include authorization of redemptions as a process subject to explicit verification and confirmation checks (check that the request is made by a participant; that adequate funds are available; that the NAV calculation is correct; that funds are actually released and timely rendered to the correct party, etc.); and
- Verify that transactions involving pool funds do not violate NFA Compliance Rule 2-45, prohibiting direct or indirect loans from a pool to a member CPO or affiliates.

The NFA also regards investment activity and valuation process as common high-risk areas for CPOs and expects that a CPO will:

- Include approvals of investments within its control framework (for example, ensuring that each type of investment is authorized and consistent with the pool's strategy);
- Verify that investments are valued in accordance with its valuation policies;

- Perform ongoing due diligence of counterparties and other third-party depositories (including reviewing reputation, trading strategy, past performance and regulators' actions);

- Monitor risks associated with investments held at third parties on an ongoing basis, including market and credit risk; and

- Continually monitor pool liquidity to ensure its capacity to meet financial obligations such as redemption requests and margin calls.

When implementing such controls, the NFA advises that business and trading principals play a direct and primary role in monitoring and assessing risks within their areas of responsibility.

Use of Administrators. Third-party administrators that perform back office and other basic operational functions should be included within the internal controls system. A CPO should consider whether maintaining a set of "shadow books" is advisable and also:

- Perform both initial and ongoing due diligence on its administrator (including factors such as costs, reputation, expertise, timeliness, responsiveness, attention to detail, work history and cybersecurity); and

- Obtain evidence a test of the effectiveness of the administrator's own controls and security measures, conducted by an internal or independent auditor as appropriate.

Impact on CPOs. The Internal Controls Notice, at least in terms of the specificity of its requirements, in many ways breaks new ground for the NFA. While many managers, especially managers registered as investment advisers with the U.S. Securities and Exchange Commission, will have many of these practices in place, all CPOs will need to carefully review their compliance and operational policies and procedures to ensure that they are in compliance by April 1, 2019. The Internal Controls Notice also served to expressly remind all CPOs that they must maintain records sufficient to demonstrate the effectiveness of their programs.

Cybersecurity Amendments

On Jan. 7, 2019, the NFA announced that it had amended its 2016 Interpretive Notice, "Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs."[3] This amendment (the "Cybersecurity Notice Amendment")[4] underscores the importance of matters such as

training on cybersecurity topics and creates a new, "narrowly drawn," cybersecurity breach notification requirement for members (such as private fund managers registered with the CFTC).

Background. The NFA's 2016 cybersecurity interpretive notice prescribed that members create a written framework of supervisory practices to address unauthorized access risks and established general requirements relating to such programs, while leaving the exact form of the information systems security program up to each member.

In particular, the 2016 Interpretive Notice required that covered entities create an incident response plan that addresses how the member will communicate externally with customers, counterparties, financial industry regulators, self-regulatory organizations and law enforcement in the event of a cybersecurity incident, but it did not explicitly require members to notify the NFA in connection with such an event.

New NFA Notification Requirement. The Cybersecurity Notice Amendment, however, contains a new requirement that a CPO must have procedures in place to promptly notify the NFA of a cybersecurity breach or similar incident that results in:

- Any loss of customer or counterparty funds;
- Any loss of a member's own capital; or
- The member providing notice to customers or counterparties under state or federal law.

When notifying the NFA, the member must provide a written summary of the incident, unless the member provides a notice to customers or counterparties (in which case it may provide a copy of the notice to NFA instead of a separate written summary).

ISSP Approval. In the Cybersecurity Notice Amendment, the NFA has also clarified that a CPO's ISSP must be approved by:

- The CEO;
- Another senior level official with primary responsibility for information technology security (such as a CTO or CISO); or
- A senior official who is listed as a principal and has authority to supervise the NFA member's execution of the ISSP.

There are different approval requirements for situations where committees approves an ISSP, or where there are approvals at different levels in a multi-entity organization, but all CPOs should confirm that the actual technicalities of the approval satisfy the new guidance.

Other Regulatory Regimes. The Cybersecurity Notice Amendment adds that a covered CPO should be familiar with notice requirements contained in applicable data security and privacy laws of the United States and other jurisdictions. The NFA encouraged members to obtain necessary contact information from regulators and law enforcement in advance of a breach. In addition, as an aid to the development of an appropriate ISSP, members are encouraged to review the practices and standards promulgated by various professional associations identified in the NFA's Frequently Asked Questions on Cybersecurity.[5]

Information Security Training. Under the NFA's prior release, members are required to provide training in information security to their employees both at hiring and "periodically" on an ongoing basis. The Cybersecurity Notice Amendment clarifies that such training should be provided both at hiring and at least annually thereafter, with more frequent training as circumstances warrant. A description of such training that identifies the topics covered in the training contents should be included in the firm's ISSP.

Action Items

Many of the NFA's recommendations for internal controls will be familiar to established private fund managers that are registered CPOs. While the NFA states that it recognizes that size and operational differences among CPOs require a degree of flexibility for self-determinations as to what constitutes an "adequate" control system, these Interpretative Notices contain a level of detail and prescription that is new.

All private fund managers should:

- Consider the adequacy of their current controls, including those established under the parallel requirements of other regulators, in light of the NFA's recommendations;
- Plan to conduct a review for any other member-specific factors that should be included in a control framework given the CPO's unique characteristics; and

- Roll out any new or amended policies in the next two months (i.e., before April 1).

More broadly, the two Interpretative Notices should encourage legal and compliance personnel to view their internal controls systems as living instruments that require constant engagement, reevaluation and renewal. NFA members should ensure that they are prepared to demonstrate to the NFA and other regulators that their control systems and cybersecurity policies and procedures are documented and in full effect.

Authored by Brian T. Daly and Joshua B. Wright.

---

[1] *See* NFA Interpretive Notice I-19-03, NFA adopts Interpretive Notice entitled NFA Compliance Rule 2-9: CPO Internal Controls System (Jan. 31, 2019), available here.

[2] Note that failure to properly segregate pool assets is also a violation of CFTC Rule 4.20(c) and often a predicate offense in CFTC enforcement actions.

[3] *See* NFA Interpretive Notice 9070, NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (effective March 1, 2016).

[4] *See* NFA Interpretive Notice I-19-01, NFA Amends Interpretive Notice Regarding Information Systems Security Programs—Cybersecurity (Jan. 7, 2019), available here.

[5] *See* NFA Cybersecurity FAQs, available here.

Practices

INVESTMENT MANAGEMENT

REGULATORY AND COMPLIANCE

CYBERSECURITY AND DATA PRIVACY

Attachments

Download Alert