Interpretive Notices

Member Regulatory Workshop

Cybersecurity

The protection and prevention of damage of investor and firm information from compromise through the use—in whole or in part—of technology systems (e.g., computers, mobile devices or internet communication systems).

Cybersecurity

- “Compromise” refers to a loss of data: confidentiality (breach), integrity, availability
- Protection and prevention of damage to customer information, and PII (personally identifiable information) mandatory under the update May 15, 2024, SEC Proposed Rule Part 248 Reg S-P includes which governs the protection of consumer financial information held by broker-dealers, investment companies, registered investment advisers and now transfer agents (“S-P entities”)
- Protection and prevention of damage to firm’s confidential information (e.g., prop trading systems, trading strategies, proprietary softwarecode, merger information)
- Interpretive Notice 9070 – information systems security programs (ISSP)
- Interpretive Notice 9079 – Members’ use of third-partyservice providers (TPSP)

Cybersecurity

- Applies to all NFA membership categories.
- Requires Members to adopt and enforce an ISSP appropriate to their circumstances to secure both customer data and access to their electronic systems.
  - **Must be approved in writing**
  - **Must be appropriate to Member's security risk**
- Provides an overview and guidance regarding information security practices that Member firms should adopt and tailor to their business activities and risks and describes certain minimum ISSP requirements.
- Requires that cyber risks posed by critical third-party service providers be addressed in the Member's security risk assessment.

Cybersecurity

Common Findings:

- Lack of documented ISSP plans
  - Approved in writing
- Performing security and risk analysis
  - Applying data loss protective (DLP) measures
    - Encryption/Password Protection/MFA
- Non-enforced and minimal tracking cyber training
- Limited third-party assessments performed
- Insufficient incident response plan

Cybersecurity

Findings Safeguards and Controls Applied:

- Data loss prevention (DLP) rules
  - Consistent system monitoring
  - Blocking outbound emails with PII
- Authentication
  - Zero trust
  - MFA (challenge/response, token, SSO)
- Protecting PII
  - Encryption when sharing critical information
  - Sharing documents through secured portals (VPN)

Cybersecurity

Common Industry Breaches:

- Phishing, vishing and smishing
- Ransomware
- Distributed denial of service (DDoS)
- User account/password attacks(bank drops)
- Third-party attacks
    - Cloud base vendors
    - Artificial Intelligence (AI)

Cybersecurity

Industry Lessons Learned - Best Practices:

- Ongoing training and awareness
  - Simulated phishing exercise
  - Multi-factor authentication
    - Include mobile devices
- Third-party risk management
  - Cloud providers
- Security and event monitoring
- Data loss prevention (DLP) safeguards

Cybersecurity

Cyber Incidents – Notifying NFA:

- Required for a cybersecurity incident related to the Member's commodity interest business that results in:
  - Any loss of customer or counterparty funds
  - Any loss of a Member's own capital
  - Member providing notice to customers or counterparties under state or federal law

Cybersecurity

Cyber Incidents Reported to NFA:

- Ransomware
- Social engineering
  - Compromised email(s)
  - Phishing attacks
- Third-party vendor breach
- Wire transfers
- Username/password compromised

Third-Party Service Providers

NFA's Interpretive Notice 9079:

- All registration categories must have written procedures
- Effective for all third parties onboarded since September 2021
- Ongoing Due Diligence
- Recordkeeping includes documentation to evidence the process

Third-Party Service Providers

Common Findings:

- Failure to identify all third-party service providers used by the firm
- Written supervisory framework doesn't include all components required by the notice
- Failure to conduct initial risk assessment
- Failure to conduct ongoing monitoring at the frequency specified in written framework

Marketing Materials

NFA's Interpretative Notice 9077:

- Written supervisory program governing use of marketing material
- Review and approval of marketing materials
- Training of employees
- Recordkeeping

Marketing Materials

Common Findings:

- Inadequate policies and procedures, which do not include the following:
  - Identifying of personnel authorized to create, review, or approve of marketing materials
  - Requiring independence between creator, reviewer, and approver of marketing materials
  - Requiring marketing materials training prior to personnel being eligible to create, review or approve materials
  - Outlining requirements for record keeping of marketing materials and approvals
- Inadequate training materials:
  - Failure to cover applicable NFA and CFTC rules
  - Failure to cover what fair and balanced materials and violations would look like, as required
- Staff missing training prior to participating in contributing, creating or delivering of materials
- Missing approvals of materials prior to distribution as required by firm policies
- Inadequate supervision of tailored marketing materials to ensure said materials are only going to appropriate counterparties

Swap Valuation Disputes

- NFA's Interpretative Notice 9072 to NFA compliance 2-49
- SDs must submit to NFA disputes that have not been resolved within the time frames set forth in CFTC Regulation 23.502(c) for the following:
  - Initial Margin
  - Variation Margin
  - Transaction or portfolio valuations if the SD does not exchange collateral
- All reportable disputes of all SD Members must be submitted, regardless of any CFTC determination regarding the cross-border application of CFTC Regulation 23.502(c)

Risk Data Filings

- Notice I-17-10
- RDF metrics should be computed with the same methodology and systems used for the Firm's daily internal risk management calculations and therefore be subjected to the same controls.
- NFA expects each SD to implement controls to ensure the completeness and accuracy of each risk metric submitted to NFA as part of its monthly risk data reporting requirement, appropriate controls include:
  - Validation activities;
  - Back testing;
  - Reconciliations;
  - Price verification testing; and
  - Other ongoing monitoring activities.

Risk Margin Amount

- SD Members subject to CFTC minimum capital requirements in CFTC Regulation 23.101(a)(1) must maintain regulatory capital as defined under the bank holding company regulations.
- Minimum capital requirements include the uncleared swap margin amount (risk margin amount)

Risk Margin Amount

- CFTC letter 21-14: SD may use a model to compute the risk margin amount under 17 CFR 23.101(a)(1)(i)(C) without obtaining the approval of NFA or the CFTC
- SD Members using models in their internal risk management frameworks to comply with minimum capital requirements that are not required to be approved by NFA must subject these models to the SD's internal model risk management controls, such as SD's independent model validation, ongoing performance monitoring and audit processes.
- All the positions used in the RMA calculations must be adequately represented in the model ongoing performance monitoring.

Q&A

Interpretive Notices