Cybersecurity Update

Member Regulatory Workshop

Session Objectives

Topics to be discussed:

- Cyber Interpretive Notice
- Common exam findings
- Cyber industry threats and breaches
- Member incidents and response

Cybersecurity

- Practice of protecting and prevention the loss of data: confidentiality (breach), integrity, availability.
- Safeguard from compromise of 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-party service providers (TPSP).

Interpretive Notice 9070 – ISSP

- Applies to all NFA membership categories – CPO, CTA, IB, FCM and SD
- 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: Exam Observations

Common Exam 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

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)

Cyber Industry Threats & Breaches

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)

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

Cyber Incidents

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

Cyber Incidents Reported to NFA

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

Responding to a Cyber Incident

- Execute a response and recovery plan
- Notify banks and/or engage counsel
- Consider hiring a third party to investigate
- Notify regulators, customers and counterparties, as applicable
- Reach out to law enforcement and information sharing agencies
- Notify insurance company

Q&A

Cybersecurity Update