Cybersecurity Update

Member Regulatory Workshop

Session Objectives

Topics to be discussed:

- Interpretive Notices 9070 and 9079 and parallel themes
- Common exam findings
- Cyber threats and breaches
- Cyber incidents and response

Definition Of 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).

Definition Of Cybersecurity (cont.)

- “Compromise” refers to a loss of data: confidentiality (breach), integrity, availability
- Protection and prevention of damage to customer information, and PII (personally identifiable information) in particular (also mandatory under the recent SEC Proposed Rule Part 248 Reg S-P includes retail and institutional customers)
- Protection and prevention of damage to firm’s confidential information (e.g., prop trading systems, trading strategies, proprietary software code, merger information)
- Interpretive Notice 9070 – information systems security programs (ISSP)
- Interpretive Notice 9079 – Members’ use of third-party service providers (TPSP)

Interpretive Notice 9070 – Information Systems Security Programs

- 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 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

Interpretive Notice 9079 – Members Use of Third-Party Service Providers (TPSP)

- Applies to all NFA membership categories – CPO, CTA, IB, FCM, and SD
- NFA recognizes that a Member may use a TPSP to perform certain regulatory functions that would otherwise be undertaken by the Member itself
  - Requires a written supervisory framework addressing:
    - Initial risk assessment
    - Onboarding due diligence
    - Ongoing monitoring
    - Termination
    - Recordkeeping
  - Information security risks must be considered throughout the oversight process

TPSP - Cybersecurity Considerations

- **Risk assessment:** risk of outsourcing regulatory function to a TPSP, including cybersecurity risks
  - Regulatory and legal risks if provider fails to carry-out function
  - **Member is responsible for fulfilling regulatory responsibilities, even if function is outsourced**
- **Due diligence:** initial and ongoing with heightened scrutiny for critical TPSPs
  - Consider IT security and practices, history of events, and BCDR planning
  - Determine contingency plan to meet regulatory requirements
- **Written agreements:** scope of service and performance expectations
  - Address TPSP notifying of material failures
  - Consider including cyber expectations, escalation and communication of outages, and cyber issues

CFTC Proposed Rulemaking on Operational Resilience Framework for FCMs and SDs

- On December 13, 2023, the Commodity Futures Trading Commission (CFTC) approved a notice of proposed rulemaking (NPRM) seeking public comment on proposed requirements for SDs and FCMs to create an operational resilience framework (ORF) by amending existing Regulation 23.603 for SDs and adding Regulation 1.13 for FCMs
- Proposed areas include the following:
    - Information security
    - Third-party relationships
    - Business continuity and disaster recovery

NFA

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
- Non-enforced cyber training
- Limited third-party assessments performed
- Ad hoc incident response plan

Safeguarding Information

- 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)

NFA

Cyber Industry Threats & Breaches

Common Threats

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

Major Financial Industry Cyber Breaches

Industry

- UnitedHealth Group (ransomware)
- MOVEit attack - various firms (ransomware)
- Russia-Ukraine cyber attacks (various vectors)
- Industrial and Commercial Bank of China (ICBC) (Ransomware)
- Caesars and MGM casinos (ransomware)

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 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 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

Responding to a Cyber Incident

- Notify bank if funds are involved
- Notify insurance company
- File suspicious activity report (SAR) if appropriate
- Update ISSP to incorporate lessons learned

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