

Cybersecurity Update

London Member Workshop



MICHELLE CUNNINGHAM

Manager II

OTC Derivatives



TYLER KOVACH
Manager
Futures Compliance

Session Objectives



Topics to be discussed:

- Cyber interpretive notice;
- Common exam findings;
- Cyber industry threats and breaches; and
- Member incidents and response.

Cybersecurity

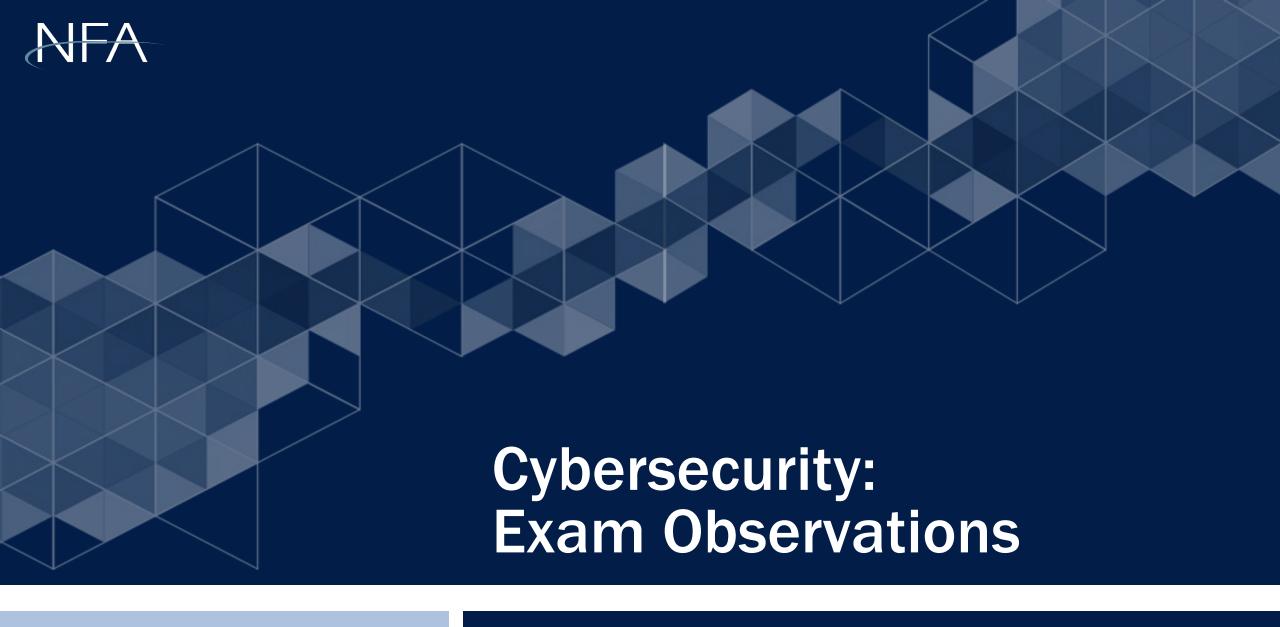


- Practice of protecting and prevention the loss of data: confidentiality (breach), integrity, availability.
- Safeguard from compromise of customer information, and PII(personally identifiable information) mandatory under the update May 15, 2024, SEC Proposed Rule Part 248 Reg S-P includes which governs the protection of consumer financial information held by brokerdealers, 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 CPOs, CTAs, IBs, FCMs and SDs.
- 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.



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 At A



- 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)



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 (A.I.)

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 – 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; and
 - Member providing notice to customers or counterparties under state or federal law.

Cyber Incidents Reported to NFA



- Ransomware
- Social engineeringg
 - 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



