

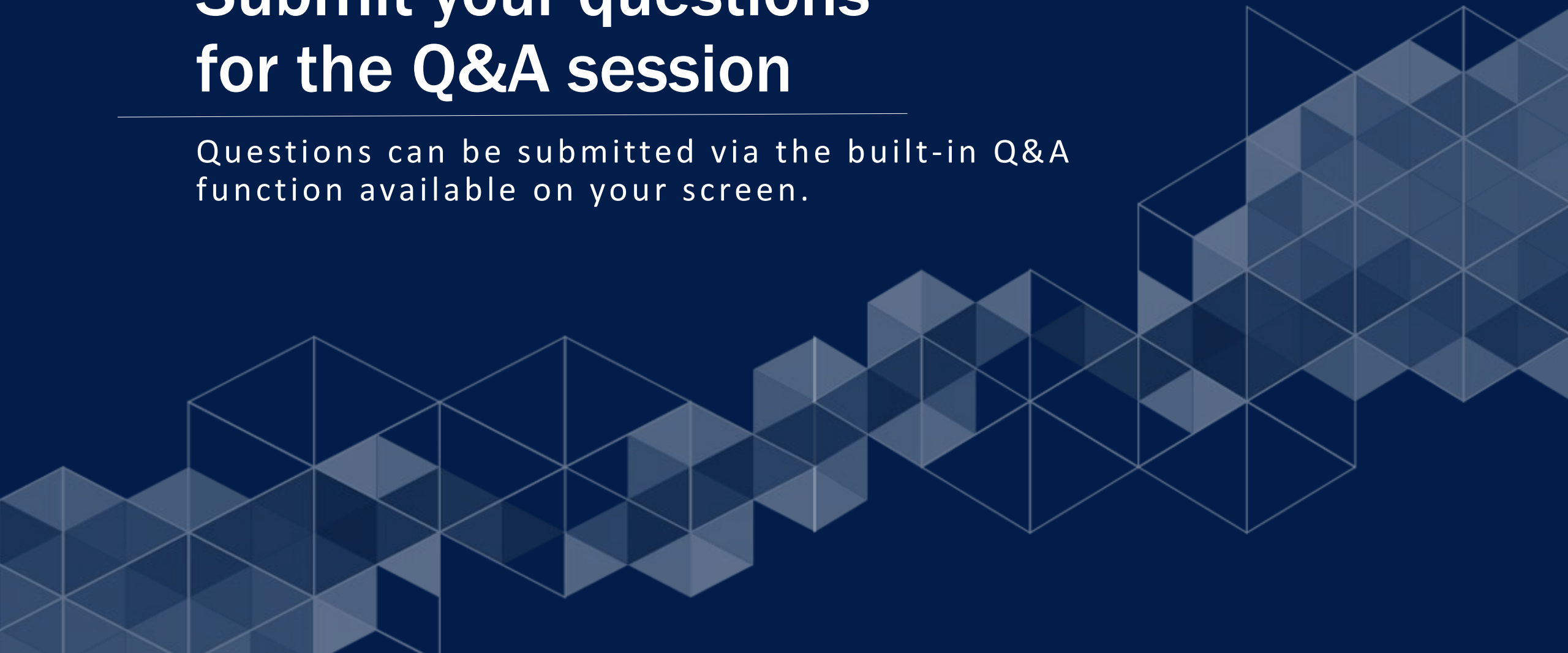
Cybersecurity

June 2, 2022




Submit your questions for the Q&A session

Questions can be submitted via the built-in Q&A function available on your screen.



Cybersecurity

An archived version of today's session, along with all other sessions for the Member Regulatory Workshop, will be available on NFA's website in the coming weeks.

A decorative background pattern of overlapping, semi-transparent hexagons in various shades of blue, creating a 3D effect. The pattern is most prominent on the right side and bottom of the slide.

Cybersecurity

Member Regulatory Workshop 2022



Session Objectives



Topics to be discussed:

- Expectations from our Members of meeting NFA's Interpretive Notices 9070 and 9079
- Key industry cyber risks and the common threats related to them
- Examples of data loss prevention techniques and safeguards and processes
- Requirements for notifying us of significant breaches

Definition Of Cybersecurity



**The protection 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 of 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 of firm confidential information (ex: prop trading systems, trading strategies, proprietary software code, merger information)
- Interpretive Notice 9070 - NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs;
- Interpretive Notice 9079 – Members’ Use of Third-Party Service Providers

NFA Interpretive Notice 9070



- Applies to all NFA membership categories – CPO, CPA, IB, FCM
- 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 Members 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

Information Systems Security Program



- Tailor ISSP to Member's operations
- ISSP approval
- Annual review
- Assessment of threats and vulnerabilities



Information Systems Security Program (cont.)



- Written program
- Security and risk analysis
- Deployment of protective measures
- Incident response plan/cyber incident notification to NFA
- Third party risk management
- Member staff training

The background of the slide features a complex geometric pattern of overlapping, semi-transparent cubes and hexagons in various shades of blue, creating a 3D effect. The pattern is most prominent on the left side and fades towards the right.

CYBERSECURITY – EXAM OBSERVATIONS

Major Cyber Industry Breaches



- Recent Events
 - Colonial Pipeline (ransomware)
 - Microsoft (stolen passwords/system vulnerabilities)
 - Log4J (inherent Java program vulnerability)
 - Crypto.com (lack of 2FA - accounts compromised)
 - CNA Financial (ransomware)



Common Threats

- Phishing, vishing and smishing
 - Spear phishing
 - Whaling attacks
- Ransomware
 - Ransomware as a service
- DDoS
- Password attacks
- Third party

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
 - Sharing documents through secured portals (VPN)



Identity Access Management (IAM)



- Approving access permissions
- Periodic access reviews
- Procedures for vendors and consultant access
- Off-boarding/transfers
- Inactive users
- Administrative access



Testing & Monitoring



- Penetration testing
- Internal audit
- Security information and event management
- Behavioral analysis



Third Party Risk Management

- Initial risk assessment
- Onboarding due diligence
- Ongoing monitoring
- Termination
- Recordkeeping
- Interpretive Notice 9079 – Members' Use of Third-Party Service Providers

Training



- Inadequate education and training program
- Employees not trained upon hiring and annually thereafter
- Increased training and awareness to employees at home
- Simulated phishing exercises



Remote Working – Best Practices



- Ongoing training and awareness
- Securing all devices
- Protecting PII



CYBER INCIDENTS

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 (cont.)



- Notify bank if funds are involved
- Notify insurance company
- File Suspicious Activity Report (SAR) if appropriate
- Update ISSP to incorporate lessons learned



Cyber Incidents Reported to NFA



- Compromised email(s)
- Phishing attacks
- Third party vendor breached
- Ransomware
- Credential stuffing
- Username/password compromised



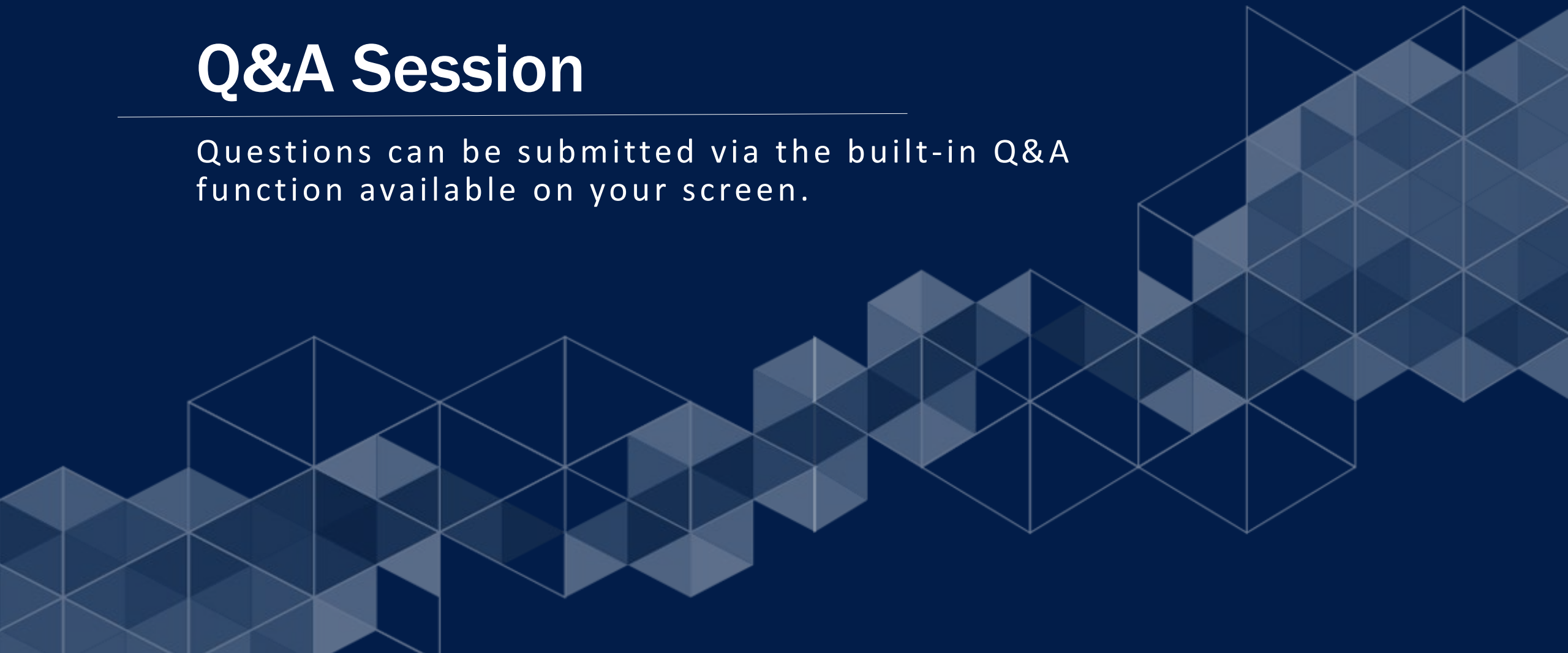
Cyber Incidents – Notifying NFA



- 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
 - The Member providing notice to customers or counterparties under state or federal law


Q&A Session

Questions can be submitted via the built-in Q&A function available on your screen.



Cybersecurity

An archived version of today's session, along with all other sessions for the Member Regulatory Workshop, will be available on NFA's website in the coming weeks.

A decorative background pattern of overlapping, semi-transparent hexagons in various shades of blue, creating a 3D effect.

Member Regulatory Workshop – Next Session

Swap Dealer Capital Updates will begin at 11:00 a.m. CT/12:00 p.m. ET.

