RIA Compliance Consultants

RIA Compliance Connection Conference
August 24 & 25, 2022
Omaha, NE

SEC's Proposed Cybersecurity Risk Management Rule

Strategic Alliance Sponsor

Unitifi

Modern solution for financial professionals to fulfill their fiduciary responsibility to know and understand their client.

Presentation Disclosures

- Although the sponsor of this presentation, RIA Compliance Consultants, Inc. (“Sponsor”), is an affiliate of a law firm and Sponsor may have an individual on its staff that is also licensed as an attorney providing legal services in a completely separate capacity, Sponsor is **not** a law firm and does **not** provide legal services or legal advice. A consulting relationship with Sponsor does not provide the same protections as an attorney-client relationship.
- This presentation is offered for educational purposes only and should not be considered an engagement with Presenter or Sponsor. This presentation should not be considered a comprehensive review or analysis of the topics discussed today. These materials are not a substitute for consulting with an attorney or compliance consultant in a one-on-one context whereby all the facts of your situation can be considered in their entirety.
- Despite efforts to be accurate and current, this presentation may contain out-of-date information. Additionally, Presenter and Sponsor will not be under an obligation to advise you of any subsequent changes.
- Information provided during this presentation is provided "as is" without warranty of any kind, either express or implied, including, without limitation, warranties and merchantability, fitness for a particular purpose, or non-infringement. Presenter and Sponsor assume no liability or responsibility for any errors or omissions in the content of the presentation.

Presentation Disclosures

- Information provide during this presentation relates solely to the Investment Advisers Act of 1940 and the rules thereunder and, at times, we may reference similar state securities rules and regulations specific to registration as an investment adviser. Certain circumstances or arrangements you may have may warrant you to consider other regulations that may apply including, but not limited to: the Investment Company Act of 1940; the Securities Act of 1933; the Securities Exchange Act of 1934; ERISA and other Department of Labor regulations; federal or state laws and regulations and self-regulatory (e.g., FINRA) rules for broker-dealers and registered representatives/securities agents of broker-dealers; and state insurance rules and regulations. The Sponsor of this presentation does not provide any advice or consulting services outside the scope of the Investment Advisers Act of 1940 or similar investment adviser state securities rules and regulations. If you need advice regarding any other rules or regulations, the Sponsor recommends that you consult with an attorney or consultant that specializes in those specific rules or regulations.
- There is no guarantee or promise that concepts, opinions and/or recommendations discussed will be favorably received by any particular court, arbitration panel or securities regulator or result in a certain outcome.
- To the extent that you provide RCC with your email address, it will be added to RCC's electronic newsletter mailing list regarding compliance issues for investment advisers. You may opt out at any time by calling RCC at 877-345-4034 or clicking at any time the "unsubscribe" link on the electronic newsletter.
- Communication with today's webinar presenter is not protected by attorney-client privilege. Please keep questions during this seminar in a hypothetical form. This seminar session and/or the presentation materials may be recorded, copied and/or shared with third parties and/or posted to our public website.

Agenda

- *Regulatory Resources*
- *Background – Current Cybersecurity Regulation*
- *Proposed Rule 206(4)-9*
- *RCC Resources*

Regulatory Resources Related to SEC's Proposed Cybersecurity Risk Management Rule

Proposed Rule and Interpretative Release:

https://www.sec.gov/rules/proposed/2022/33-11028.pdf

Press Release & Fact Sheet:

https://www.sec.gov/files/33-11028-fact-sheet.pdf

Submitted Comments on Proposed Rule:

https://www.sec.gov/comments/s7-04-22/s70422.htm

Existing Regulatory Resources Related to Cybersecurity

Risk Alert: Cybersecurity: Safeguarding Client Accounts against Credential Compromise

https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf

Risk Alert: Cybersecurity: Ransomware Alert

https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf

Risk Alert: Safeguarding Customer Records and Information in Network Storage - Use of Third Party Security Features

https://www.sec.gov/ocie/announcement/risk-alert-network-storage

Regulation S-P Rule 30

https://www.law.cornell.edu/cfr/text/17/248.30

Regulation S-ID: Identity Theft Red Flags

https://www.law.cornell.edu/cfr/text/17/248.30

NASAA's Model Rule: Investment Adviser Information Security & Privacy Rule

https://www.nasaa.org/wp-content/uploads/2019/05/NASAA-IA-Information-Security-and-Data-Privacy-Model-Rule.pdf

Background – Fiduciary Duty

Act in Client's Best Interest Which Includes

(i) Protecting Against Not Being Able to Serve Client and

(ii) Protecting Security of Client's Information

Background – Compliance Rule

Under SEC Rule 206(4)-7, An Investment Adviser Is Required to Consider Its Fiduciary Obligation and Formalize Policies & Procedures to Address Those Obligations

Background – Regulation S-P

- Requires Investment Advisers to Adopt Written Policies and Procedures to Protect Customer Information Including Security and Confidentiality
- Must be Reasonably Designed to Protect Against Any Anticipated Threats or Hazards, Unauthorized Access to or Use of Customer Records or Info

Background – Regulation S-ID

- Must Maintain Reasonable P&P to Identify and Detect Red Flags to Prevent and Mitigate Identity Theft
- Must Periodically Review, Train Employees and Oversee Third-Party Service Providers

Background – NASAA Model Rule

- NASAA Developed a Model Rule for State Securities Regulators
- Model Rule Requires (Similar to Reg S-P Rule 30) for a State Registered Investment Adviser to Protect Customer Information and Requires the Firm Maintain Written P&P to Identify Security Risks, Protect Systems and Information, Detect/Respond and Recover from a Cybsecurity Breach Incident
- Many States Have Adopt Even More Rigorous Requirements than NASAA Model Rule

Proposed 206(4)-9 – General Overview

Under the SEC's Initial Proposal (Before Comments) for a Cybersecurity Risk Management Rule, an Investment Adviser Would Be Required

- Implement Cybersecurity Policies and Procedures in Writing
- Disclose Cybersecurity Risks and Past Cybersecurity Incidents in Form ADV Part 2A
- Promptly Report Significant Cybersecurity Incidents to SEC

Cybersecurity Policies & Procedures

- Allowed to Tailor P&P to Fit Nature and Scope of Business and Address Individual Cybersecurity Risks
- Can Implement Using Internal or External Resources or a Third-Party's Cybersecurity Risk Management Services
- Policies Should Specify Which Position/Individual Is Responsible for Implementing and Administering P&P
    - Including specifying those responsible for communicating incidents internally and making decisions with respect to reporting to the SEC and disclosing to clients and investors certain incidents

Cybersecurity P&P – Risk Assessment

- Must (a) categorizes/prioritizes cybersecurity risks
- Should identifies vendors that receive, maintain or process client info and the associated cyber security risks
- Memorialized in writing
- Informs senior officers of investment adviser firm of specific risks
- Risk assessment used to develop cybersecurity P&P
- Periodically re-assess

Cybersecurity P&P – User Security & Access

- 2 Factor Authentication
- Password Expiration/Reset
- Limit Access & Information to Individuals on Need to Know/Use Basis
    - Portfolio Manager Should Access To Trade Entry Features & Compliance Should Access Only Review/Approval Features
- Secure Remote Access
- Regularly Monitor for Unauthorized Users (e.g., Removed from Project, Terminated Employee)
- Monitor for Unauthorized Login Attempts, Lock-Outs, and User ID/Password Changes

Cybersecurity P&P – Information Protection

- Monitor & Protect Systems and Information for Unauthorized Access/Use Based Upon Periodic Assessments Based Upon
  - Importance or Sensitivity of Information
  - Personal Information
  - How Information Is Accessed, Transmitted and Stored
  - Access Controls & Malware Protection
- Require Service Providers to Protect Adviser's Information

Cybersecurity P&P – Threat Vulnerability

- Specific Procedures for Ongoing Monitoring of Threats and Vulnerabilities
  - Conducting Review of Network and Application Vulnerabilities
  - Suggested Best Practices
    - Limiting Mobile Devices Approved for Remote Access
    - Monitoring All Files on End Point Like Mobile Phone
    - Scans of Networks for Threats
    - Patch & Updates Manager for All Computers/Devices
  - Monitoring New Threats from Industry and Government Sources
- Specific Procedures Handling Vulnerabilities Once Identified (e.g., Intake, Assignment, Escalation, Remediation, and Remediation Testing)

Cybersecurity P&P – Incident Response & Recovery

- Proposed Cybersecurity Risk Management Rule Requires Advisers to Have Measures to Detect, Respond and Recover from Cybersecurity Incident
- Cybersecurity Incident Response P&P Should Ensure Continued Operation of Investment Adviser, Protection of Investment Adviser's Systems and Information
- Internal & External Communication of Sharing Incident
- Reporting (via Form ADV-C) Significant Cybersecurity Incident to SEC within 48 Hours
- Document Each Incident Including Response and Recovery

Cybersecurity P&P – Annual Review

- Must Annually Review and Assess the Design & Effectiveness of Cybersecurity P&P and Prepare Written Report
- Should Be Prepared by Person Responsible for Investment Adviser's Cybersecurity P&P

Prompt Regulatory Reporting of Significant Cybersecurity Incidents to SEC

- Submit Form ADV-C promptly, but in no event more than 48 hours, after having a reasonable basis to conclude that a significant adviser cybersecurity incident occurred

Definition of Significant Cybersecurity Incident

The term “significant adviser cybersecurity incident” is an incident or set of incidents which significantly disrupts or degrades an investment adviser’s ability to maintain critical operations or leads to unauthorized access/use of adviser info which causes substantial harm to adviser or client.

Disclosure of Cybersecurity Risks – Form ADV Part 2A

- Adding Item 20 to Form ADV Part 2A
  - ✓ Describe cybersecurity risks that could materially affect the advisory services they offer and how they assess, prioritize, and address cybersecurity risks created by the nature and scope of their business
  - ✓ Describe any cybersecurity incidents that occurred within the last two fiscal years that have significantly disrupted or degraded the adviser's ability to maintain critical operations, or that have led to the unauthorized access or use of adviser information, resulting in substantial harm to the adviser or its clients
  - ✓ **Interim Amendment Due to Cybersecurity Incident Requires Delivery to Clients**

Final Comments

- Only a Proposed Rule – There Will Most Likely Be Some Changes to the Final Rule
- Proposed Rule Is Based Upon Section 206 of IAA'40 (Anti-Fraud) Which Increases Penalties for Violations
- Through These More Detailed Requirements for Cybersecurity P&P, Cybersecurity Risk Disclosures and Cybersecurity Reporting to a Regulator, the SEC Is Raising the Baseline

Recordkeeping

- Must Maintain for 5 Years
  - ✓Cybersecurity P&P
  - ✓Annual Review of Cybersecurity P&P
  - ✓A Copy of Form ADV – C
  - ✓Records Documenting Cybersecurity Incident and Response/Recovery
  - ✓Risk Assessment

Resources

Sample Forms Available in Online Store and Knowledge Base

- Cybersecurity – Best Practices Checklist (22 plus pages)
- Cybersecurity – Employee Acknowledgement
- Cybersecurity – Phishing Email – Letter Notifying Client
- Cybersecurity – Website Security Checklist for Investment Adviser
- Cybersecurity – Best Practices for Avoiding and Responding to Phishing Attacks
- Cybersecurity – Best Practices for RIA Collecting Devices for Digital Forensic Expert
- Cybersecurity – Conducting Due Diligence of Cloud Computing Service Providers
- Cybersecurity – Training to Avoid Phishing
- Cybersecurity - 12 Steps for an RIA to Improve Security of Client Information
- Cybersecurity - GDPR Best Practices Checklist for Website
- Cybersecurity – Cleaning Company Acknowledgement – Background Checks

Strategic Alliance Sponsor

Unitifi

Modern solution for financial professionals to fulfill their fiduciary responsibility to know and understand their client.

Connect With Us

www.ria-compliance-consultants.com

www.Facebook.com/riacompliance

www.YouTube.com/riacompliance

www.linkedin.com/company/ria-compliance-consultants-inc.