The SEC's Proposed Cybersecurity Risk Management Rule and The Proposed Outsourcing Rule:

What it is, how it may affect you, and what you can do to prepare

FAIRVIEW® FV

Today's Speakers

Frank Watson, Founder and Chairman

Frank founded Fairview in 2009 with the goal of providing streamlined compliance services to RIAs. Today, Fairview has grown to a mid-sized firm, which includes four distinct practice areas: Compliance Administration, Cyber Solutions, Investment Administration, and Performance Services. Frank has worked in the financial services industry since 1995.

Amber Allen, General Counsel and EVP; President of Fairview Cyber

Amber is General Counsel and EVP of Fairview and President of Fairview Cyber, which develops cyber and data security programs and advises its clients on regulatory requirements and industry best practices. Amber is licensed to practice law in North Carolina and is a Certified Information Privacy Professional. She is a member of the NSCP Board of Directors and serves as Co-Chair of NSCP Currents Publication Committee.

Jeremy McCamic, Director of Policy Management and Relationship Manager

Jeremy is Director of Policy Management and a Relationship Manager on our Compliance Administration team. Jeremy oversees a team responsible for monitoring regulatory changes and advising clients as they navigate those changes. This includes writing policies and procedures for use in compliance manuals and developing internal and external training on new regulations and best practices. He also partners with RIAs and CCOs to provide full compliance administration support.

Background

Cyberattacks in the Financial Services Industry

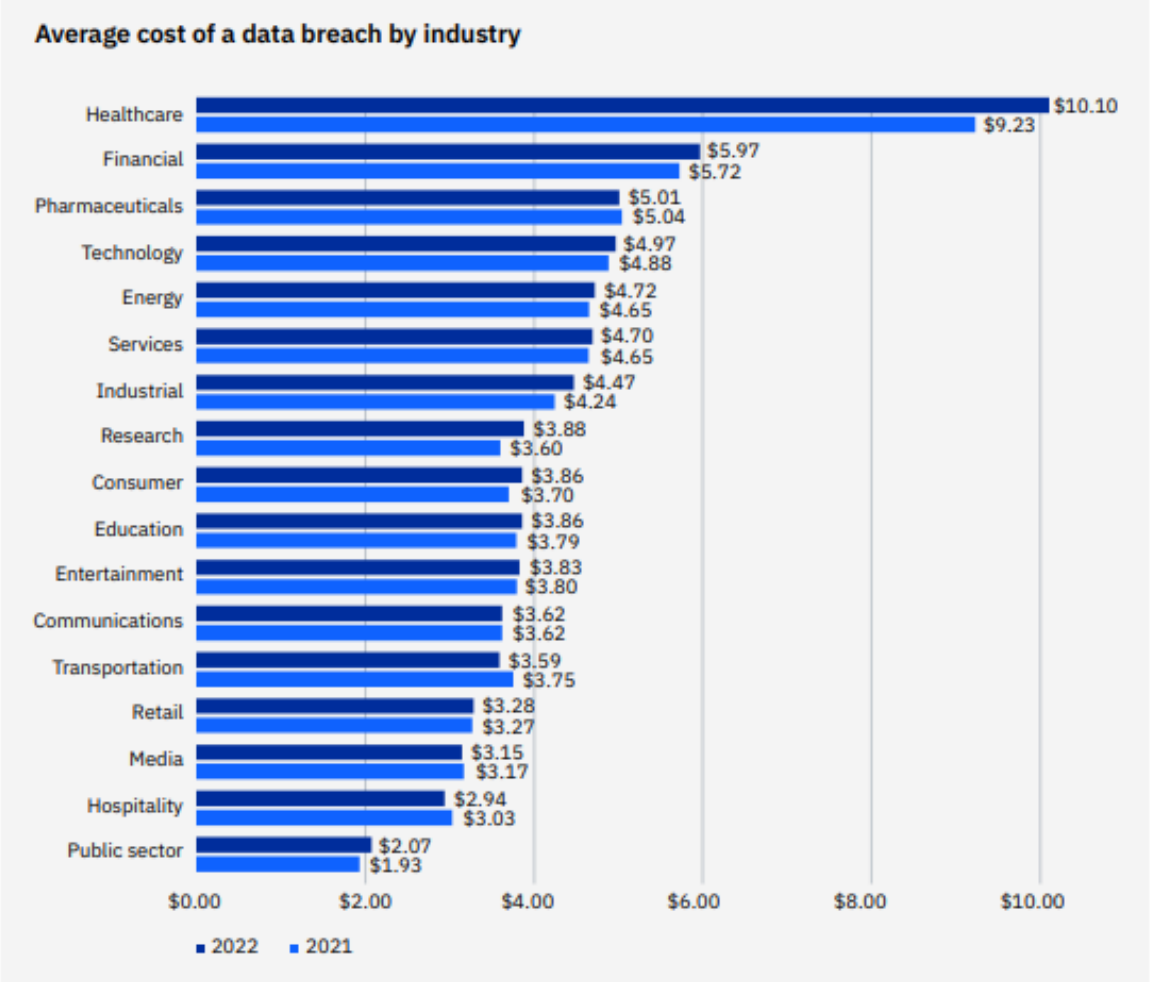
- Attacks against the financial sector increased **238% globally** from the beginning of February 2020 to the end of April, **with some 80% of financial institutions reporting an increase in cyberattacks.**[1]

- The financial services industry consistently ranks second (behind healthcare) for the highest cost industry for data breaches.[2]

1. Allianz, Financial Services Risk Trends 2021

2. IBM Security, Cost of a Data Breach Report 2022

Data Breaches Cost Millions—and Continue to Rise



IBM Security, Cost of a Data Breach Report 2022

Current Regulatory Landscape

- **As fiduciaries, advisers must act in their client's best interest**
- **Regulation S-P**
    - Congress enacted the GLBA in November 1999
    - In response, the SEC Enacted Regulation S-P in June 2000
- **Regulation S-ID**
    - The Federal Trade Commission began enforcing the Red Flag Rule in January 2011
    - The SEC and CFTC were assigned responsibility for rulemaking and enforcement of identity theft red flags rules under Dodd-Frank
        - Issued Regulation S-ID (Reg S-ID) in 2013

Current Regulatory Landscape

- **Notable Guidance and Risk Alerts**
  - 2014 – 2023 Examination Priorities
  - 2014 Risk Alert
  - 2014 Cybersecurity Initiative
  - 2015 Risk Alert: Cybersecurity Examination Sweep Summary
  - 2017 Risk Alert: Observations from Cybersecurity Examinations
  - 2019 Risk Alert: Regulation S-P
  - 2019 Risk Alert: Safeguarding Customer Records and Information in Network Storage - Use of Third-Party Security Features
  - 2020 Risk Alert: Cybersecurity: Ransomware Alert
  - 2022 Risk Alert: Identity Theft and Reg S-ID

The SEC's Focus on Cybersecurity

"The financial sector remains a very real target of cyberattacks. What's more, it's become increasingly embedded within society's critical infrastructure…"

"More than two decades since Reg S-P was adopted—an eternity in the cybersecurity world—I think there may be opportunities to modernize and expand this rule."

- SEC Chair Gary Gensler, April 14, 2022

https://tax.thomsonreuters.com/news/chair-gensler-says-more-sec-cybersecurity-rule-proposals-in-the-works/

The SEC's Proposed Cybersecurity Risk Management Rule & The Proposed Outsourcing Rule

Proposed Rules

- **Cybersecurity Risk Management Proposal**
  - Proposed on February 9, 2022
  - Proposed Rule 206(4)-9 under the Advisers Act and Rule 38a-2 under the Investment Company Act
- **Outsourcing Key Service Provider Proposal**
  - Proposed on October 26, 2022
  - Proposed Rule 206(4)-11

Overview of the SEC's Proposed Cybersecurity Risk Management Rule

- Annual cybersecurity **risk assessment**
- Adopting cybersecurity **policies and procedures** including:
  - User security and access, information protection, threat and vulnerability management, cybersecurity incident response and recovery
- Conducting **testing** and documenting an annual Cybersecurity Review
- **Disclosures** and reporting
- Additional Considerations
  - Maintain certain **books and records**

A Closer Look at the SEC's Proposed Cybersecurity Risk Management Rule

- **Conduct an annual cybersecurity risk assessment**
  - **Step 1:** Internal or external reviews?
  - **Step 2:** Determine the framework
  - **Step 3:** Conduct the review
  - **Step 4:** Prioritize action items and assign responsibility
  - **Step 5:** Adjust policies and risk assessment as needed (and at least annually)

A Closer Look at the SEC's Proposed Cybersecurity Risk Management Rule

Goal: Inform senior officers of threats that could lead to breach

Content:

- Categorize and prioritize cyber risks based on an inventory of systems used and data contained therein
- Identify service providers that have access to client information
  - Type of data
  - Risk associated with service provider

Consider:

- Remote work and traveling employees
- Breach of service provider
- Internal operations and insider threats

A Closer Look at the SEC's Proposed Cybersecurity Risk Management Rule

Implement cyber and data security policies and procedures

User Security and Access

- Acceptable use policy
- Account authentication
- Password Policy
- Access Management
- Secure remote access

Information Protection

- Data classification
- PII tracking
- Data access, storage, transmission, and monitoring
- Access controls and malware protection
- Cyber incident assessment, including business continuity

A Closer Look at the SEC's Proposed Cybersecurity Risk Management Rule

Implement cyber and data security policies and procedures

Threat and vulnerability management

- Detect, mitigate and remediate cyber threats and vulnerabilities
- Network, system, and application vulnerability management
- Industry and government threat source monitoring

Cybersecurity Incident Response and Recovery

- IRP and BCP
- Protection of information
- Notification obligations
- Tabletop exercises
- Relevant vendors

A Closer Look at the SEC's Proposed Cybersecurity Risk Management Rule

- **Conducting and documenting an annual Cybersecurity Review**
  - **Review policies at least annually**
  - **Prepare a written report, including:**
    - Description of annual review
    - Assessment of program, including any testing performed and the results
    - Documentation of any cyber incidents
    - Description of any material changes to policies

A Closer Look at the SEC's Proposed Cybersecurity Risk Management Rule

- **Maintain certain books and records**
- **Rule 204-2 Books and Records Rule Amendment**
  - Cyber policies and procedures adopted pursuant to Rule 206(4)-9
  - Annual Cybersecurity Review
  - Risk assessment
  - Form ADV-C filings, if any
  - Documentation of any cyber incident

A Closer Look at the SEC's Proposed Cybersecurity Risk Management Rule

- **Provide cyber disclosures:**
  - Form ADV Part 2A, Item 20 Cybersecurity Risks and Incidents
  - Form ADV-C
    - Within 48-hours of having a reasonable basis to conclude a significant cyber incident occurred or is occurring
    - Promptly amend within 48 hours if
      - Information previously disclosed becomes inaccurate
      - New information is discovered
      - Incident is closed or resolved

Outsourced Service Provider Rule

- **Rule 206(4)-11**
- **Scope of Rule:**
- **Requirements:**
  - Conduct due diligence on service provider **before** retaining a service provider for a covered function
  - Periodic monitoring and due diligence
  - Report census-type information about these service providers on Form ADV
- **Amendments to Books & Records Rule & Form ADV**

How RIAs Can Prepare for Compliance

How You Can Prepare

- **Get ahead of rule's adoption.**
  - All RIAs should already have a cybersecurity program in place—but that will just be a starting place
  - Use proposed rule as a guide to determine additional cybersecurity-related needs and disclosures

- **Don't panic.**
  - Remember that there is still time—even when the rule is finalized, there will be an implementation period. Use this time to start planning.

How You Can Prepare

- **Don't know where to start? Start with the risk assessment.**
- **Then, make sure you have policies and procedures in place to use as a starting point:**
  - Cyber and risk management policies
    - User Security and Access
      - Access management and review
    - Information Protection
      - Data mapping
      - Vendor access
    - Threat and vulnerability management
      - Patching
      - Vulnerability scans
    - Cybersecurity Incident Response and Recovery
      - IRP, BCP, DRP

How You Can Prepare

- **Vendor Management takes time to implement, so start sooner rather than later**
  - Identify key vendors
  - Adopt policy
  - Centralize responsibility
  - Conduct initial due diligence before engaging vendors
  - Conduct periodic vendor reviews based on risk

Q&A

Additional questions?
Contact Amber Allen at
Amber.Allen@FairviewInvest.com
or visit www.FairviewInvest.com

FAIRVIEW® FV