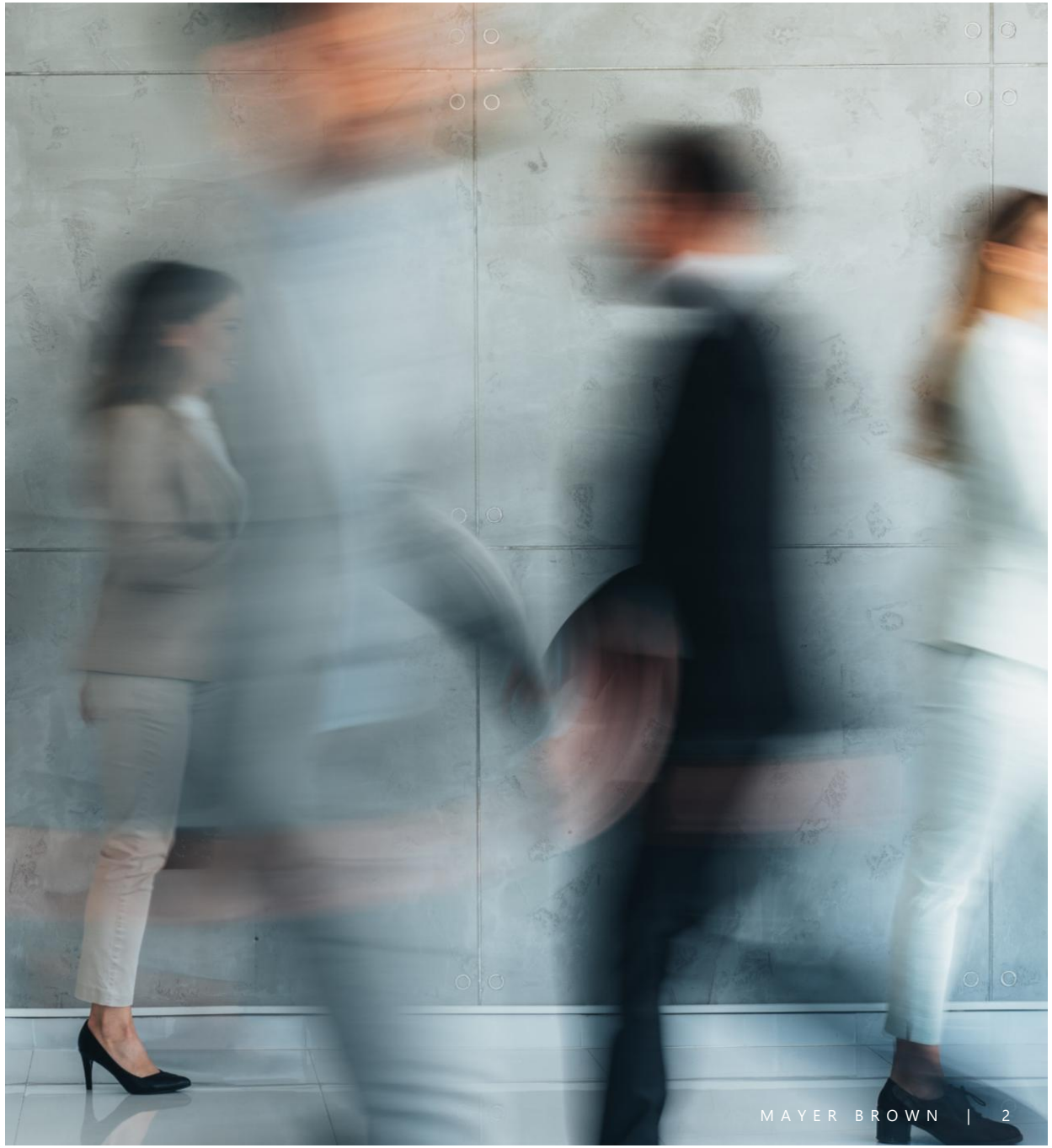
MAYER|BROWN

ENFORCEMENT LANDSCAPE
CYBERSECURITY SPOTLIGHT

ENFORCEMENT TRENDS

- Cybersecurity enforcement activity is up
- Most cybersecurity enforcement follows cyber incidents
  - Enforcement risk therefore tends to follow cyber risk
- Increased enforcement activity at the state level
- Mixed signs at the federal level but no broad pullback
- Focus on several areas, including:
  - Third-party cybersecurity risk
  - Data management/data retention
  - MFA and other access controls

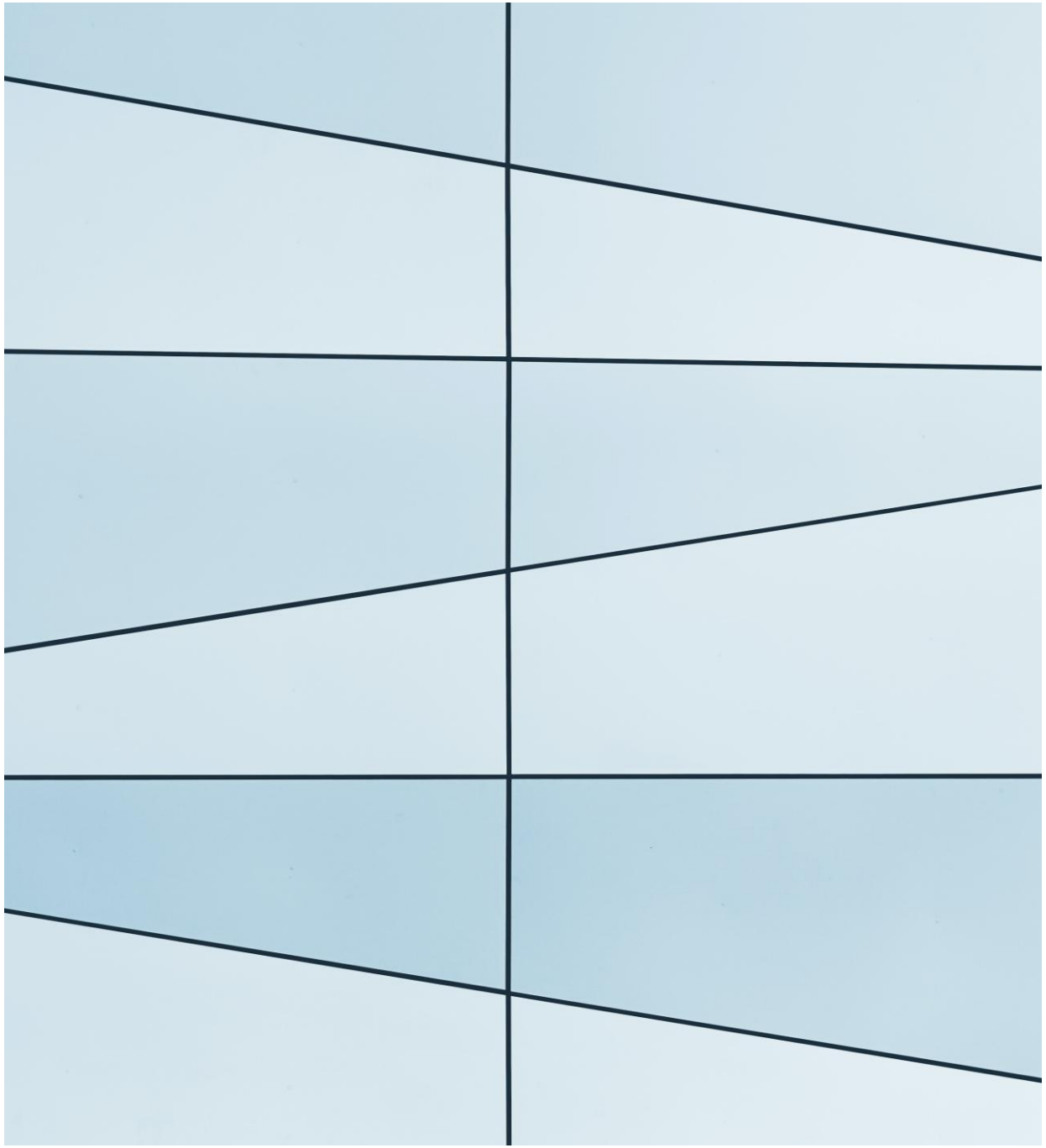


ENFORCEMENT TRENDS BY AGENCIES

- **Banking and insurance regulators**
  - Heightened scrutiny on cyber, including more regulations and more scrutiny during exams
- **Federal enforcement: SEC/FTC/DOJ**
  - SEC has continued to emphasize cyber enforcement
    - Has had 13 public cybersecurity actions since 2023, including three charged matters that are still pending
  - DOJ has continued to pursue cybersecurity FCA cases
  - FTC shift toward traditional enforcement (i.e., fraud, misrepresentation)
- **State regulators and AGs ramping up enforcement & "staffing up"**
  - More 50-state cyber enforcement actions

COMMON TRIGGERS FOR ENFORCEMENT ACTIONS

- Regulatory Priorities
  - Example: NYDFS Guidance on MFA.
    - "MFA weaknesses are the **most common cybersecurity gap** exploited at financial services companies."
    - "MFA is therefore a **focus** of DFS's cybersecurity supervisory and **enforcement** work."
    - "DFS is also increasing its review of MFA **during examinations**, with a particular emphasis on probing for the common MFA failures discussed in this Guidance."
- Red Flags that lead to investigations and enforcement actions.
  - Incident timeline (discovery, containment, mitigation, notification)
  - Impact on consumers and economy
  - Control failures & program maturity
  - Patterns & frequent fliers

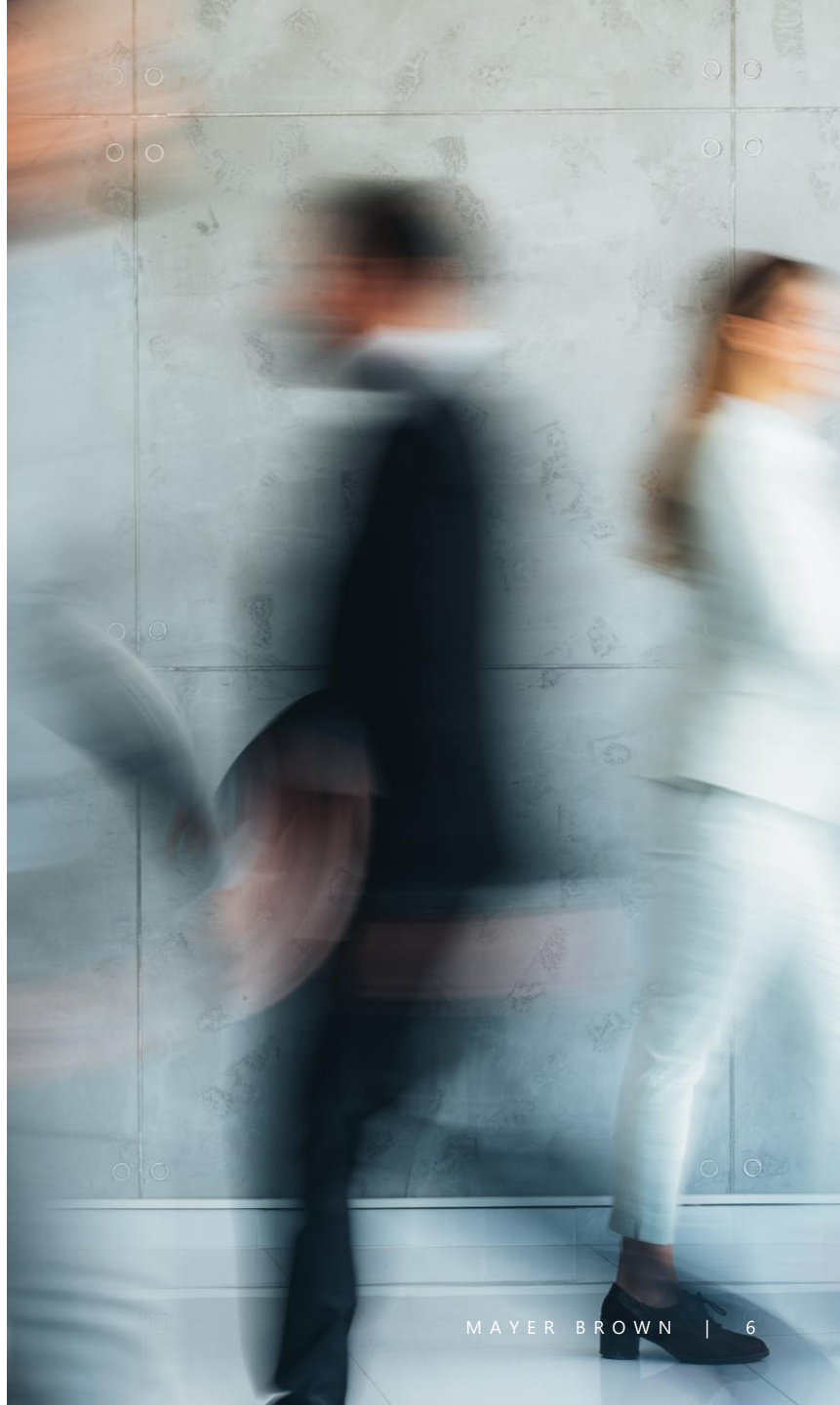


NYDFS CYBERSECURITY ENFORCEMENT BY THE NUMBERS

- There have been 17 public settlements of cybersecurity enforcement actions, totaling $144 million in fines
  - Many adverse cybersecurity actions are not public, such as private consent orders.
- Case origin: Incidents (10) and Examination (7)
- Most common charges
  - False/Incorrect Multi-factor Authentication (8)
  - Lack of Required Compliance Certification (8)
  - Lack of Required Policy (7)
  - Lack of (or inadequate) Risk Assessment (5)
  - Failure to Report a Cybersecurity Incident (5)
- Four cases combined Cybersecurity & AML charges.

NYDFS CASE STUDY: FIRST UNUM/PAUL REVERE AND FIRST AMERICAN

- **May 13, 2021:** NYDFS found that First Unum and Paul Revere violated the DFS Cybersecurity Regulation by failing to implement MFA and falsely certifying compliance with the Cybersecurity Regulation for the calendar year 2018.
  - The companies had been the subject of two phishing attacks in 2018 and 2019 that succeeded, in part, because the accounts were not protected by **MFA for remote access**.
  - As part of the settlement, the companies agreed to pay a $1.8 million penalty and implement remediation.
- **November 28, 2023:** NYDFS's investigation found that First American failed to maintain and implement effective governance and classification, access controls and identity management, and risk assessment policies and procedures.
  - In May 2019, a vulnerability in an application permitted any individual in possession of the link used to access customer data without authentication. NYDFS alleged significant deficiencies in the **vulnerability management program**.
  - First American agreed to pay a $1 million penalty and implement remediation.



NYDFS CASE STUDY: GEICO AND TRAVELERS

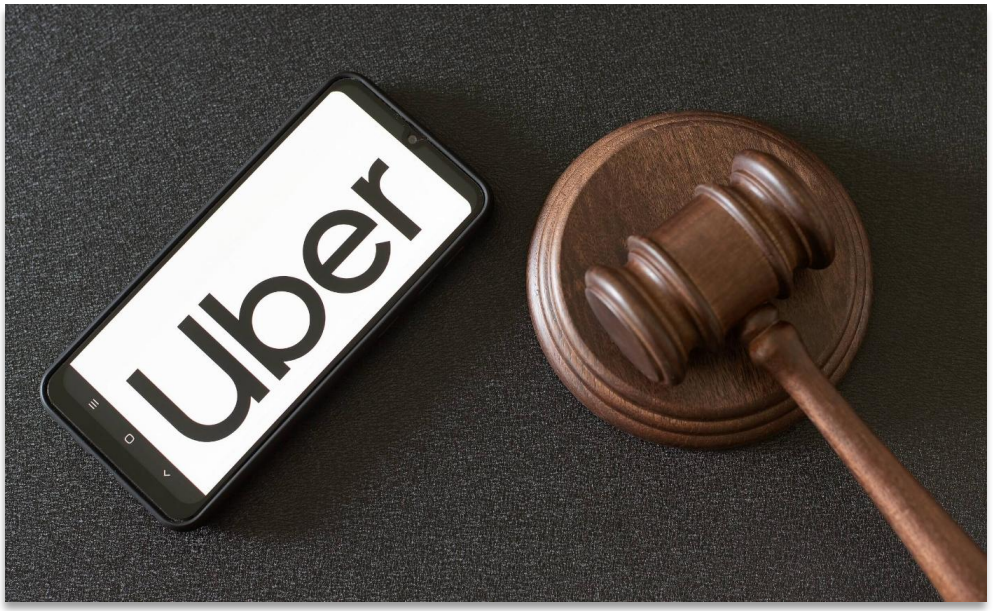
- On November 25, 2024, the NY AG and NYDFS announced a settlement with Geico and Travelers for cybersecurity violations which led to the personal information of more than 120,000 New Yorkers being compromised.
  - The NYDFS imposed penalties of $9.7 million on Geico and $1.5 million on Travelers
- Beginning in 2020 hackers obtained New Yorker's driver's license numbers from Geico's **public-facing insurance quoting tools** and then exploited vulnerabilities in Geico's **insurance agent quoting tool**.
  - Personal information of the 116,000 affected NY residents was later used to file unemployment claims during the COVID-19 pandemic
- Between January and April 2021, Travelers received several **NYDFS industry alerts** warning that hackers were obtaining driver's license numbers through insurance quoting tools. In April 2021, hackers gained access to Travelers' **agent portal** using compromised credentials. The portal did not use MFA.
  - The attack exposed the PI of approximately 4,000 New Yorkers.
- In addition to the penalties, the settlement agreement requires the companies to adopt a series of **remediation measures**, including a comprehensive cybersecurity risk assessment and penetration testing, and the development of an action plan to address any resulting concerns.

SEC CASE STUDY: R.R. DONNELLEY & SONS COMPANY (RRD)

- June 18, 2024 – R.R. Donnelley & Sons Co. agreed to pay $2.1 million to settles disclosure and internal control failure charges relating to cybersecurity incidents and alerts in 2021.
- RRD experienced **a ransomware attack** that resulted in the exfiltration of 70 GB of data and business service disruptions
- The SEC claimed that RRD failed to take timely and adequate steps to investigate and mitigate the threat – **ignoring multiple alerts** from its intrusion detection systems.
- The ransomware attack was addressed only after another company alerted RRD – one month after the first alert.
- The SEC claimed that RRD failed to:
  - prioritize and manage security alerts
  - Supervise its third-party cybersecurity vendor managing the alerts
  - Internal policy deficiencies

DOJ CASE STUDY: UBER

- On October 5, 2022, after a one-month trial, a jury convicted former CSO of Uber, Joseph Sullivan, on federal charges of (1) obstructing a FTC investigation of Uber's data security practices and (2) failing to report a felony.
- The charges resulted from Sullivan's attempt to conceal a 2016 data breach that exposed the PII of 57 million users.
- Sullivan was charged with lying to the FTC and certain Uber executives
- On May 5, 2023, the ex-CSO was sentenced to three years' probation and 200 hours of community service.



SEC CASE STUDY: EQUINITI TRUST CO.

- August 20, 2024 – the SEC announced settled charges against Equiniti Trust Company LLC, formerly known as American Stock Transfer & Trust, for failing to assure that client securities and funds were protected against theft or misuse. Equiniti agreed to pay $850,000.
- **Classic BEC** (business email compromise)
  - Loss of more than $6.6 million of client funds because of two separate cyber intrusions in 2022 and 2023.
  - American Stock Transfer was able to recover approximately $2.6 million of losses and fully reimbursed the clients for their losses.
- Notably, **Equinity was not hacked** – the threat actors hacked the email accounts of Equinity customer
- The SEC claimed that Equinity lacked adequate controls to **prevent this fraud**

BEST PRACTICES

- Thorough documentation of risk assessment, policies, and procedures in all required areas
  - But make sure these are realistic
- Most enforcement defense starts with incident response
  - An opportunity to start making your record in anticipation of regulatory scrutiny
  - Conduct your investigation under privilege
  - Document what you did
  - Document what you learning and when
  - Coordinate and manage communications
- The mere fact of an incident is not a compliance violation
- Be prepared to explain the incident and the details of the cybersecurity program to the regulator
- Cybersecurity risk mitigation = enforcement risk mitigation

INVESTIGATIVE PROCESS | BEST PRACTICE CONSIDERATIONS

The five-step process to ensure and maintain integrity during an investigation.

Data Identification
Evidence

Acquisition
Proper Collection and Data Preservation

Processing
Human Readable Format

Analysis

Production for Review

Data Identification

- Identify involved third parties and engage appropriately for their support

Acquisition

- Preserve as much evidence as possible
- Enforce a chain of custody documentation policy to prevent tampering or alteration

Processing

Analysis

Production for Review

- Documentation that meets investigative standards
  - Audit Logs
  - Change Control
  - Forensic Summary

Coordination with government agencies (e.g., law enforcement, regulatory bodies)

DISCLAIMER

These materials are provided by Mayer Brown and reflect information as of the date of presentation.

The contents are intended to provide a general guide to the subject matter only and should not be treated as a substitute for specific advice concerning individual situations.