pillsbury

JANUARY 28, 2026

Cybersecurity Issues in Securities Enforcement and Litigation

Presented by:

Mark Krotoski
David Oliwenstein
Bruce Ericson

Presenters

Mark Krotoski
Partner | Cyber Disputes Team Leader

Former national coordinator of the Computer Hacking and Intellectual Property (CHIP) program in the DOJ Criminal Division, Criminal Division chief in the NDCA U.S. Attorney's Office, and cybercrime prosecutor

David Oliwenstein
Partner | Securities Enforcement Practice Leader

Formerly with the SEC's Division of Enforcement

Bruce Ericson
Partner | Securities Litigation Team Leader

Regularly assists on securities class actions, derivative actions, representing board members, and related litigation

pillsbury

Agenda

- Preparing for a broad range of cyber incidents and data breaches
- Initial incident response – key steps and considerations
- Regulatory enforcement, notifications, initial inquiries, and investigations
- Litigation
- SolarWinds case study and lessons learned
- Lessons from other cases
- Best practices
- More resources

pillsbury

Disclaimer: Preliminary Note

This presentation draws upon the experience of the presenters, discusses legal and technical issues from varying perspectives, does **not** discuss or consider non-public case information in pending or past cases that they have been involved with, and does not necessarily reflect the views of our clients.

pillsbury

pillsbury

Are You Prepared for the Broad Range of Cyber Incidents and Data Breaches?

Broad Range of Cybersecurity Threats

PHISHING

RANSOMWARE

BUSINESS EMAIL COMPROMISE

CYBER FRAUD

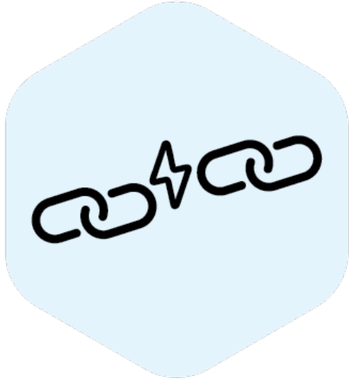
INSIDER THREATS

AI-ENABLED ATTACKS

TARGETED OR MALICIOUS ATTACKS

ATTACKS BY FORMER EMPLOYEES

EMPLOYEE INADVERTENCE



SUPPLY CHAIN ISSUES

THIRD PARTY VENDORS

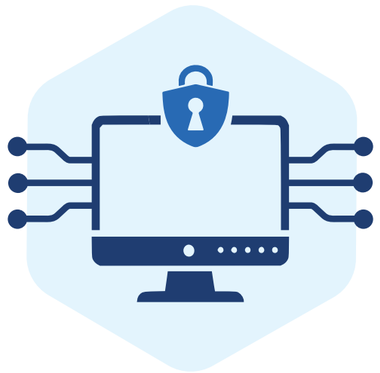
NATION STATE ATTACKS

pillsbury

Broad Range of Cybersecurity Threats

Additional SEC Concerns

CYBER INTRUSION



DENIAL OF SERVICE ATTACKS

MANIPULATION

MISUSE BY INSIDERS

AMONG OTHERS

Source: U.S. Securities and Exchange Commission | Cybersecurity

pillsbury

Broad Range of Cybersecurity Threats

Consider: On average, how long is a cyber threat actor in your network before identification and containment?

pillsbury

Phishing Email Discovery Example

- Phishing email installed malware and compromised system
- Discovered **269 days later (nearly 9 months)**
- Affected Protected Health Information (PHI) of more than 10.4 million current, former and affiliated members and employees

FOR IMMEDIATE RELEASE
September 25, 2020

Contact: HHS Press Office
202-690-6343
media@hhs.gov

Health Insurer Pays $6.85 Million to Settle Data Breach Affecting Over 10.4 Million People

Premera Blue Cross (PBC) has agreed to pay $6.85 million to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and to implement a corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules related to a breach affecting over 10.4 million people. This resolution represents the second-largest payment to resolve a HIPAA investigation in OCR history. PBC operates in Washington and Alaska, and is the largest health plan in the Pacific Northwest, serving more than two million people.

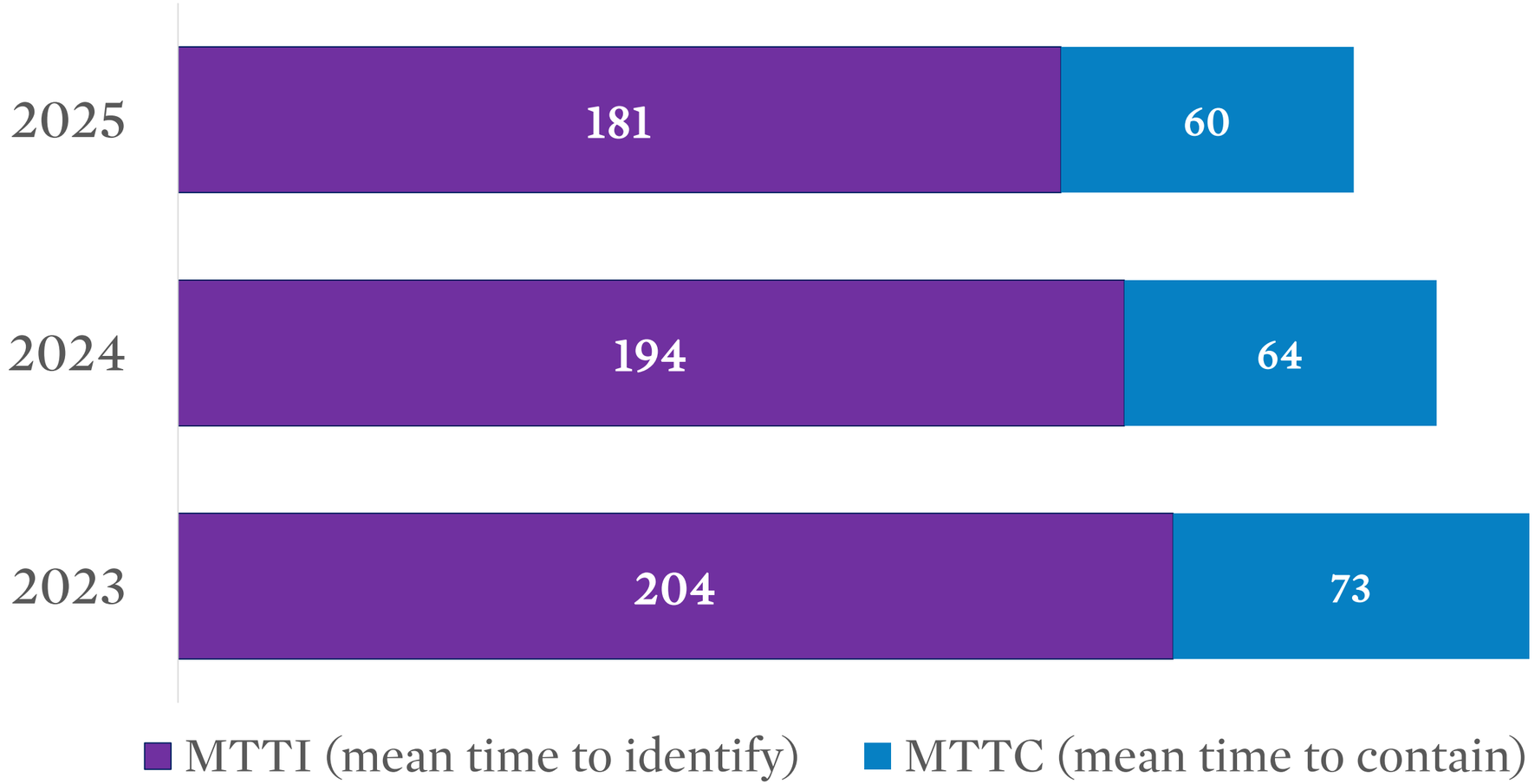
On March 17, 2015, PBC filed a breach report on behalf of itself and its network of affiliates stating that cyber-attackers had gained unauthorized access to its information technology (IT) system. The hackers used a phishing email to install malware that gave them access to PBC's IT system in May 2014, which went undetected for nearly nine months until January 2015. This undetected cyberattack, otherwise known as an advanced persistent threat, resulted in the disclosure of more than 10.4 million

Source: Health Insurer Pays $6.85 Million to Settle Data Breach Affecting Over 10.4 Million People

pillsbury

Time to Identify and Contain Data Breach

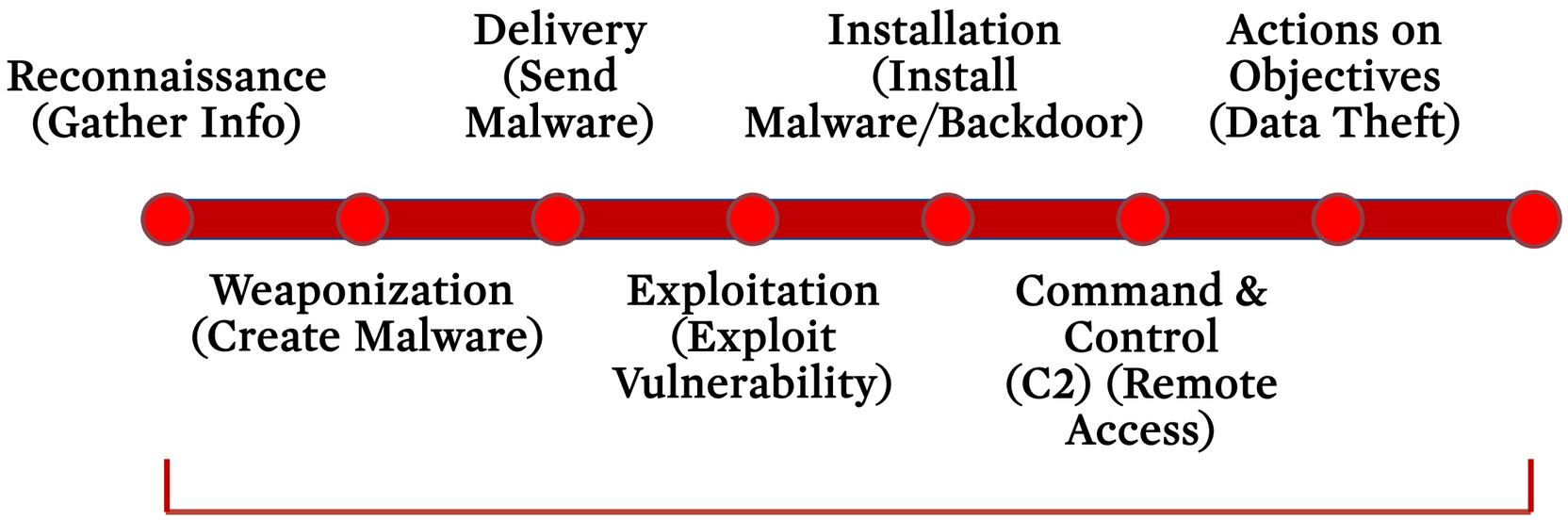
Cost of a Data Breach Report 2025
The AI Oversight Gap



Source: IBM Cost of a Data Breach Report 2025

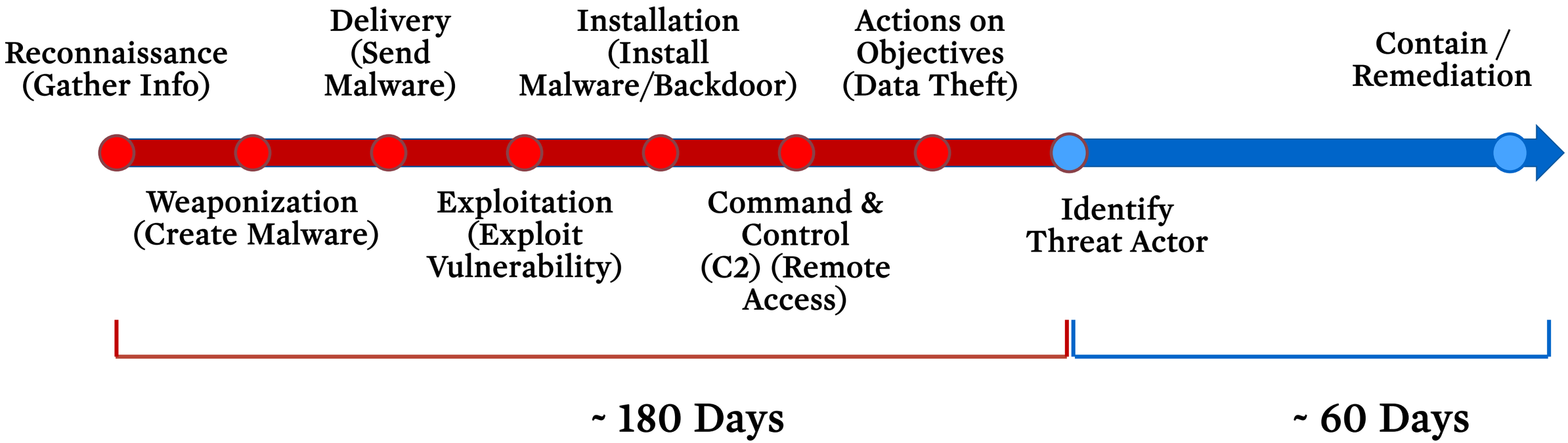
pillsbury

Threat Actor Activity Prior to Detection (Kill Chain Steps)



pillsbury

Threat Actor Activity Prior to Detection (Kill Chain Steps)



pillsbury

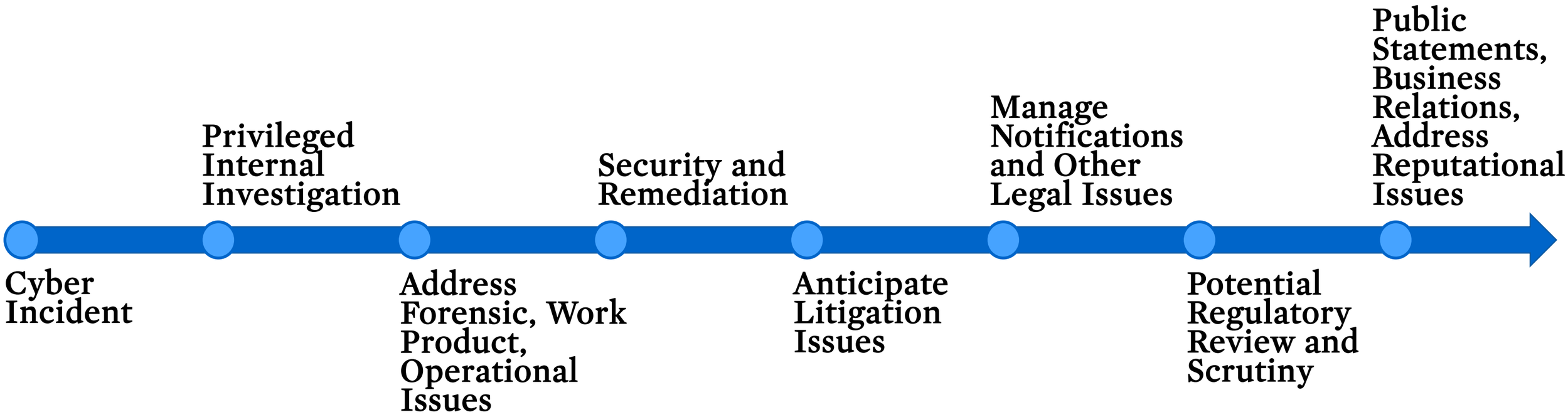
pillsbury

Initial Incident Response – Key Steps and Considerations

Key Phases of the Incident Response Timeline

pillsbury

Key Phases of the Incident Response Timeline



pillsbury

Managing Forensic and Technical Issues

- Type and scope of **cyber incident** requires different forensic analysis.
  - Malware analysis.
  - Insider access to network.
  - Business email compromise.
  - Ransomware threat actors and history.
  - Multi-factor authentication exploited.
- How and when threat actor gained access to the network?
  - Lateral movement on network?
- Analysis of Kill Chain Steps
- Whether any data was **exfiltrated**?
- Evidence for hearing, regulators or trial.
- Whether **logs** are incomplete or deleted?
  - Attackers may delete evidence to cover their tracks.
  - Requiring deeper forensic reconstruction.
- Notification standards vary.
  - When was “data breach” discovery triggering notification clock.
- What data was compromised?
  - PII
  - PHI
  - Confidential business information
  - Trade secrets.

pillsbury

Need for Separate Legal Protections in Investigations

Attorney-Client Privilege

- The attorney-client privilege "purpose to encourage full and frank communications between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice. The privilege recognizes that **sound legal advice or advocacy** serves public ends and that such advice or advocacy depends upon the lawyer's being fully informed by the client." *Upjohn Co., v. United States*, 449 U.S. 383,389 (1981).

Attorney Work-Project Doctrine

- Work prepared in anticipation of litigation by attorneys or representatives
  - Mental impressions, conclusions, legal theories, opinions.
- Fed. R. Civ. P. 26(b)(3)(A)(ii)
  - May be disclosed if "party shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means."

pillsbury

Compelled Disclosure of Forensic Report

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Capital One Judge Skeptical That Breach Report Is Privileged

By **Anne Cullen**

Law360 (May 15, 2020, 4:11 PM EDT) -- A Virginia federal magistrate judge tackling discovery issues in the sprawling litigation over Capital One's massive 2019 data breach appeared unconvinced during a hearing Friday morning that consumers suing the bank are barred from seeing a cybersecurity firm's report on the event.

Consumers **within the multidistrict litigation** are pushing to get hold of an incident report compiled in the wake of the event by prominent cybersecurity consultant Mandiant.

Capital One says that the analysis is privileged information because it was prepared to assist the bank's legal counsel in the **onslaught of litigation** that followed the breach, though U.S. Magistrate Judge John F. Anderson seemed unconvinced of that during Friday morning's virtual hearing on the dispute.

"I'm struggling with the idea of why Mandiant wouldn't have been doing this work and make this analysis even if there wasn't litigation," Judge Anderson explained. "I understand the point that when this happened, everybody knew there was going to be litigation. I don't think there's much dispute about that."

"But the question that I'm struggling with is whether Mandiant would've really done this work even if litigation wasn't going to be on the horizon," the judge said.

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Capital One Ordered To Release Report Of Massive Data Heist

By **Ben Kochman**

Law360 (May 27, 2020, 10:47 PM EDT) -- Capital One Financial Corp. has been ordered to disclose a cybersecurity firm's forensic analysis of its massive 2019 data breach, after a Virginia federal court that is hearing consumer litigation stemming from the breach rejected an argument that the report is protected by attorney-client privilege.

The Virginia-based bank, which faces an **onslaught of litigation** after a cybercriminal **allegedly exposed** the sensitive data of more than 100 million people, had claimed that it should not be forced to turn over the analysis from cybersecurity consultant Mandiant, because the document was prepared to help Capital One's attorneys deal with the lawsuits.

But Capital One, which bears the legal burden of proving why the data breach analysis should be shielded as attorney work product, would have still likely commissioned the report even if it did not expect legal action, U.S. Magistrate Judge John F. Anderson suggested on Tuesday.

"Capital One has not presented sufficient evidence to show that the incident response services performed by Mandiant would not have been done in substantially similar form even if there was no prospect of litigation," Judge Anderson wrote.

"The retention of outside counsel does not, by itself, turn a document into work product," the judge added.

Source: Capital One Judge Skeptical That Breach Report Is Privileged; Capital One Ordered To Release Report Of Massive Data Heist

Legal Protections on Investigations

- Confirm legal protections are properly memorialized to defend, if needed.
- Forensic providers and any other vendors assisting on the matter are acting at the direction of counsel.
- Legal hold under attorney-client privilege and work-product doctrine to maintain confidentiality and materials remain protected as legal strategy is developed.
- Use *Upjohn* interviews for privileged, confidential employee interviews conducted during a corporate internal investigation for the purpose of obtaining information needed by counsel to provide legal advice to the company.
- Reconstruct an accurate timeline for legal guidance and forensic review.

Day One Focus and Plan: Security, Remediation and Compliance

- **Security**
  - Contain incident, restore security and business operations.
  - Address customer questions and concerns.
  - Analyze root cause.
- **Remediation**
  - Disable accounts, patch, change passwords, address vulnerabilities.
  - Review controls to address incident or vulnerability.
  - Consider regulatory and litigation issues.
- **Compliance**
  - Regulator focus on what compliance program was in place at the time of the incident?
  - Are reasonable security procedures and practices in place.
  - Regulators ask companies to explain security issues, mitigation steps, and how deficiencies were corrected.
  - Review governance to manage cyber risks and incident.
  - Will incident recur?

pillsbury

Law Enforcement Notification and Involvement

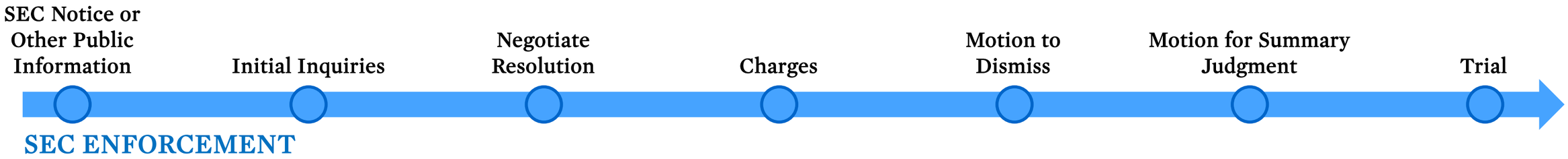
- Law enforcement may request delayed notification.
- Consider what criminal laws and jurisdictions may apply based on unauthorized access and transmissions.
- Timing considerations
  - What information is known about the incident in order to report?
  - Is there sufficient evidence for criminal enforcement.
  - Identify the loss and harm.
- Confidentiality.
  - Although initial reports to law enforcement are confidential, details can become public through public investigations, court filings, subpoenas, or leaks.
- Victim rights while responding to and managing the incident.
- Reporting may trigger multiple, parallel investigations from SEC, state AGs, FTC, HHS Office for Civil rights, NYDFS, among others.
- Preservation of logs, devices and data in a forensically sound manner.
- Parallel forensic review of incident.
- Business disruption issues.
- Maintaining privilege and work product legal protections.
- Recognizing limited resources of law enforcement in deciding to open investigation.

pillsbury

pillsbury

Regulatory Enforcement, Notifications, Initial Inquiries and Investigations

SEC Enforcement



- **Civil action:** SEC complaint in U.S. District Court requesting a sanction or remedy.
- **Administrative action:** SEC may seek sanctions through the administrative proceeding process heard by an administrative law judge (ALJ).

SEC Notification Standard

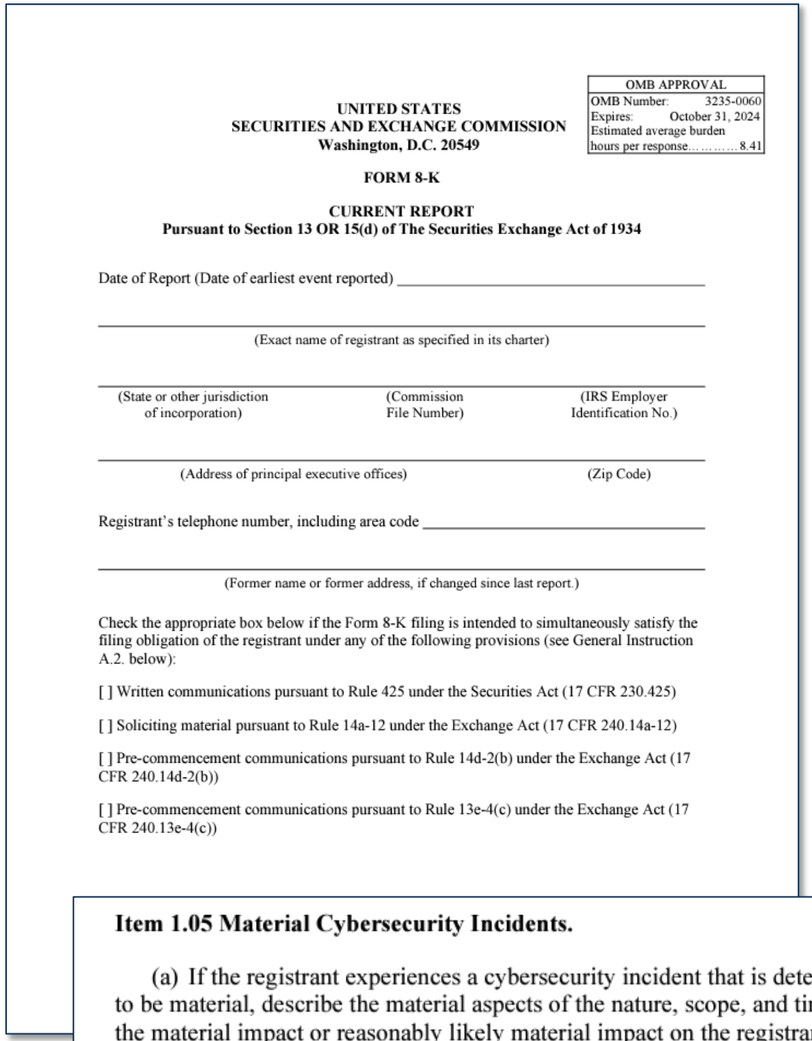
"**Cybersecurity incident**" refers to "an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."

Key Issues

- Definition is intentionally broad.
- Debate over scope of "unauthorized occurrence" – i.e., whether it includes accidents.
- Need to monitor any related occurrences.
- Includes matters that occur on the systems of *third parties*.

SEC Notification Standard

- Form 8-K, Item 1.05: **four business days** after a registrant determines that a **cybersecurity incident is material**.
  - "[D]escribe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations."
- Delayed Disclosure:
  - If the U.S. Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing.
- Effective: December 18, 2023.



OMB APPROVAL
OMB Number: 3235-0060
Expires: October 31, 2024
Estimated average burden
hours per response..... 8.41

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 OR 15(d) of The Securities Exchange Act of 1934

Date of Report (Date of earliest event reported) _____

_____
(Exact name of registrant as specified in its charter)

(State or other jurisdiction of incorporation)	(Commission File Number)	(IRS Employer Identification No.)

_____
(Address of principal executive offices) (Zip Code)

Registrant's telephone number, including area code _____

_____
(Former name or former address, if changed since last report.)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions (see General Instruction A.2. below):

[ ] Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

[ ] Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

[ ] Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

[ ] Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Item 1.05 Material Cybersecurity Incidents.

(a) If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.

Source: United States Securities and Exchange Commission Form 8-K

SEC Penalties

Monetary Penalties

- Civil monetary penalties
- Disgorgement with interest

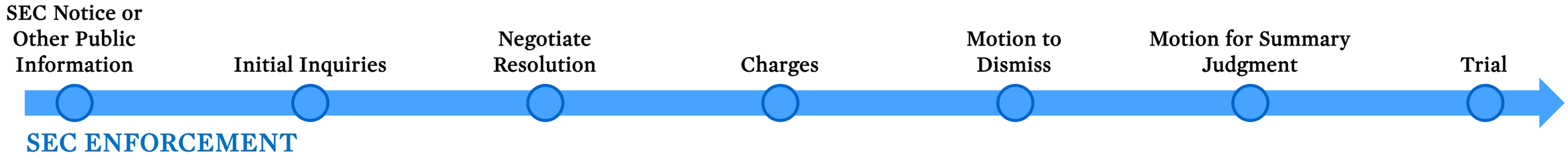
Non-Monetary Penalties

- Cease-and-Desist Orders / Injunctions
- Officer-and-Director Bars
- Industry Bars
- Rule 102(e)

Collateral Consequences

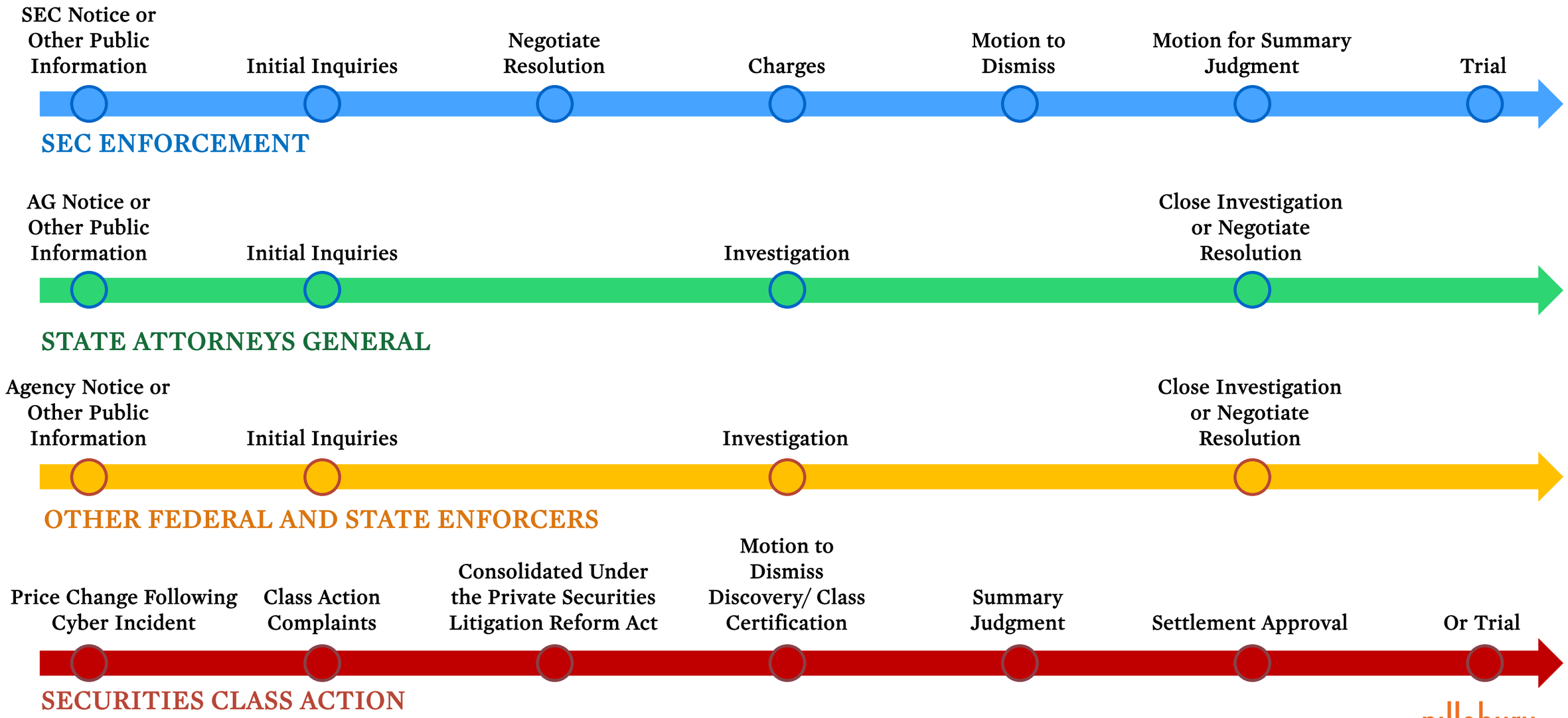
- Loss of WKSI status, Reg A and Reg exemptions, and safe harbors
- Reputational

Managing Enforcement and Litigation Overlapping Timelines



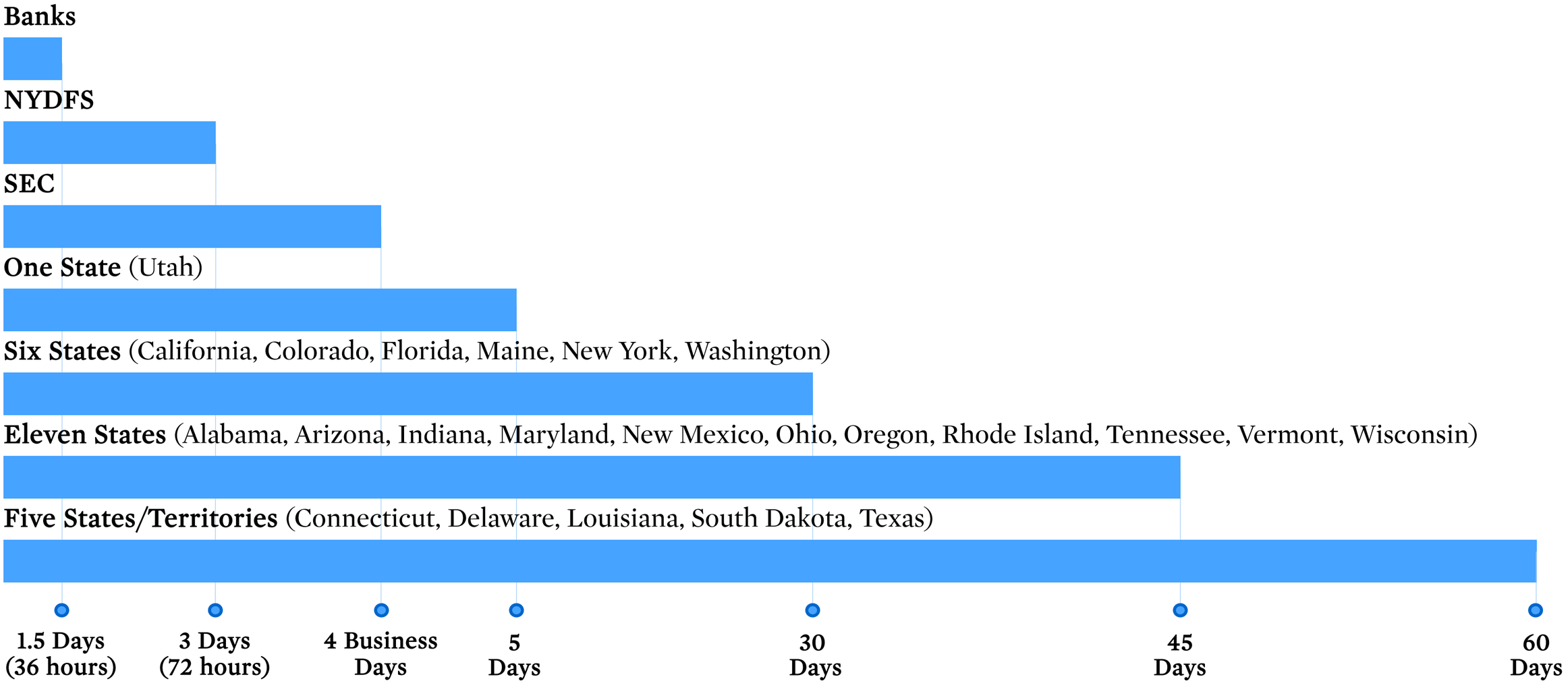
pillsbury

Managing Enforcement and Litigation Overlapping Timelines



pillsbury

Varied Notification Deadlines and Notification Triggers



Source: How Cos. Can Prep For Tightened Calif. Data Breach Notices

pillsbury

Managing Varied Notification Standards and Issues

- Notification standard examples:
  - States: "Access" or "acquisition" of PII.
  - SEC: Within four business days after a registrant determines that a cybersecurity incident is "material."
  - NYDFS: "has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity."
  - NYDFS: "deployment of ransomware within a material part of the covered entity's information systems."
  - States: Delayed notification "to determine the scope of the breach and restore the reasonable integrity of the data system."
  - Contractual notification triggers vary based on terms.

pillsbury

Focus on Disclosure Controls and Procedures

- The **timeliness** of the notification, including under varying deadlines.
  - Significant penalties for untimely notification.
- **Who** is notified?
  - Individuals and/or
  - Regulators.
- The **adequacy** of the notification.
  - Penalties for inaccurate or misleading notifications.
- Whether notification **updates** may be required.

https://www.law360.com/articles/2409109/how-cos-can-prep-for-tightened-calif-data-breach-notices

pillsbury

pillsbury

Litigation

Litigation Avenues

Civil Enforcement

- Against executives, board, and the company

Private Litigation

- Damages
- Joint and several liability
- Injunctive relief
- Attorneys' fees and interest

Criminal Prosecution

- Against individuals, the company, or both

Potential Plaintiffs

- SEC
- Federal Trade Commission
- Office for Civil Rights
- Department of Justice
- State Attorneys General

Private Parties

- Class Actions
- Derivative actions
  - Shareholders

pillsbury

Civil Litigation Issues

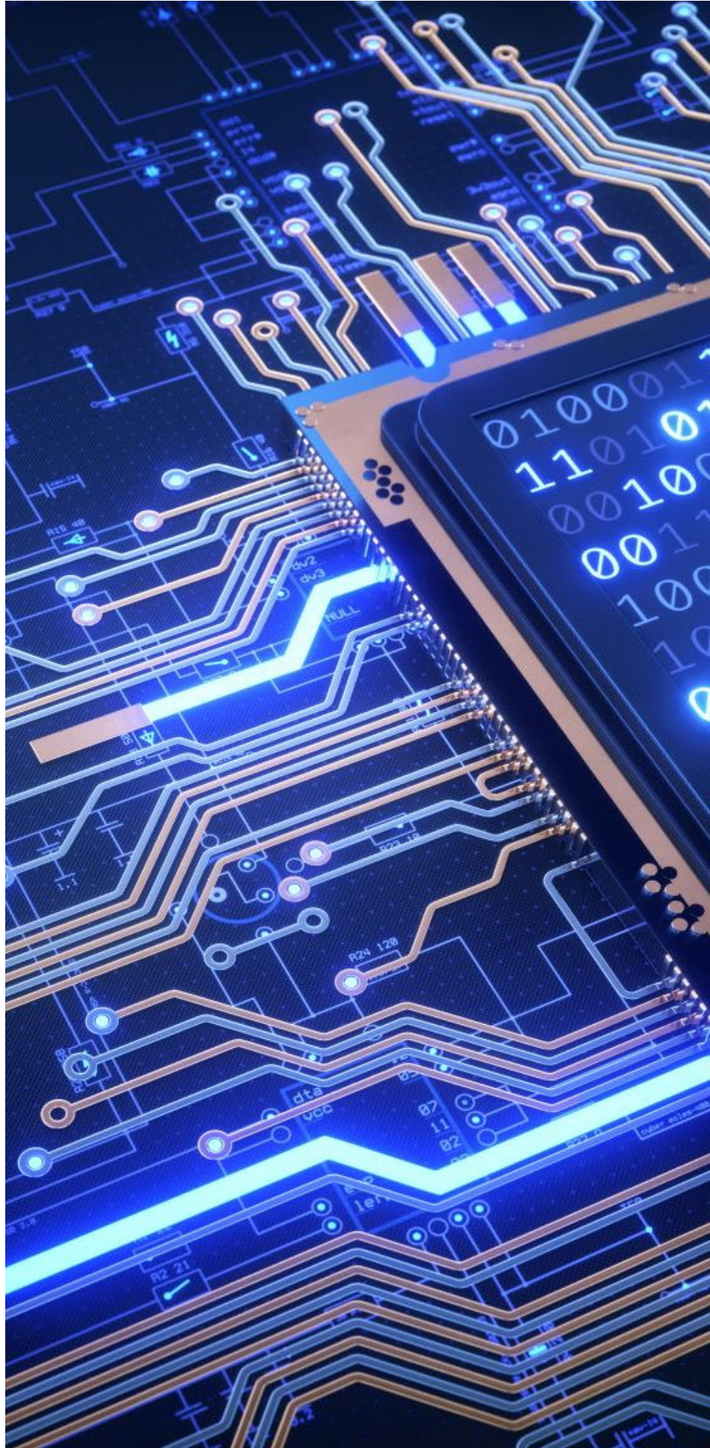
- **Consumer Class Actions**
- **Securities and Governance Actions**
  - Securities class actions (e.g., SEC Rule 10b-5)
  - Shareholder derivative actions – *Caremark* claims
    - Breach of fiduciary duty of care
    - Uptick in risk in recent years (airplanes to ice cream)
- **Privacy Litigation**
  - California Invasion of Privacy Act
  - Biometric Information Privacy Act (Illinois and others)
- **Contractual Indemnity Claims**
- **Cyber Insurance Disputes**

pillsbury

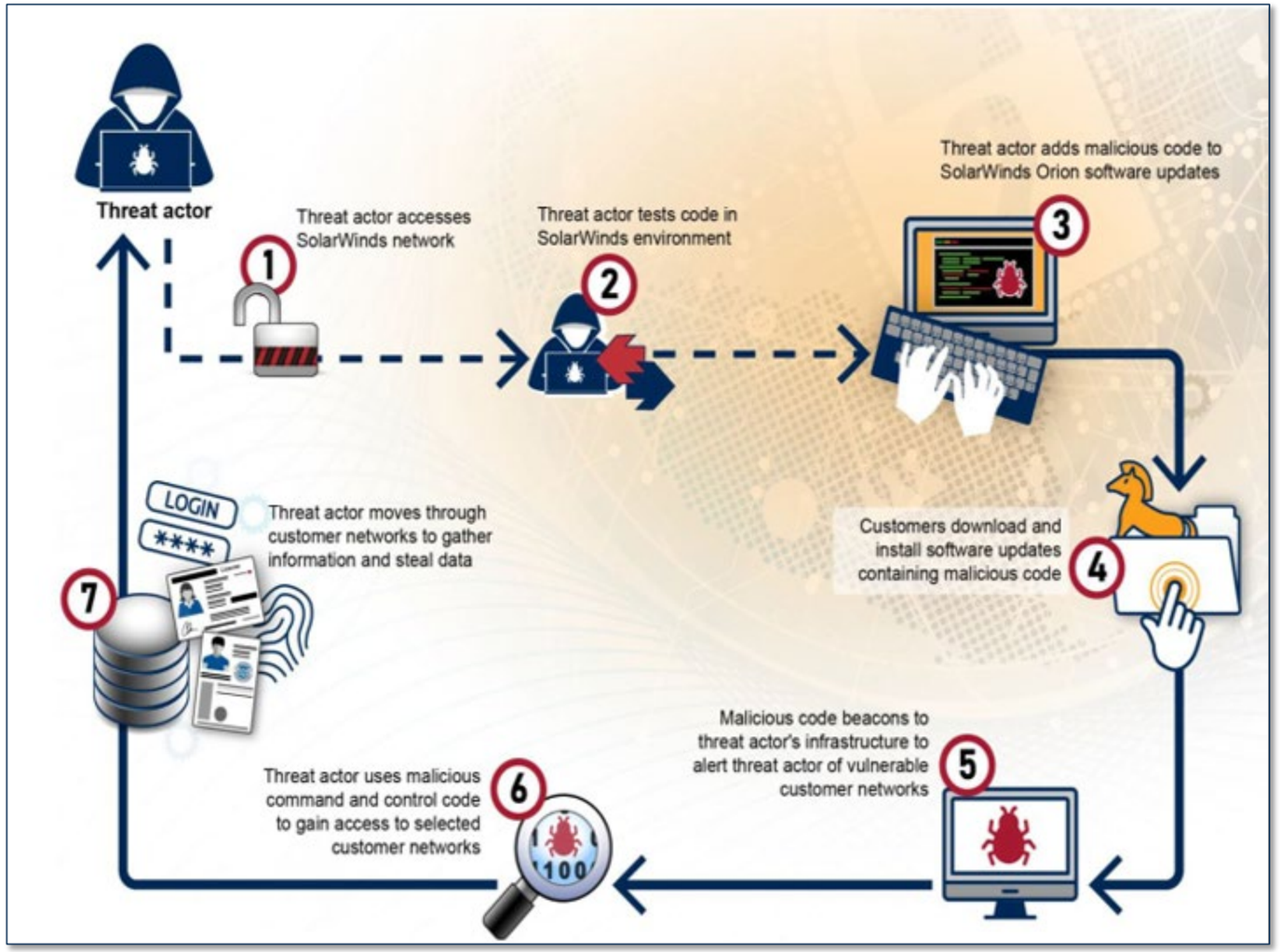
SolarWinds Case Study and Lessons Learned

Key Issues

- First SEC enforcement action charging a Chief Information Security Officer (CISO) along with the company.
- First internal **accounting** control claim based on cybersecurity failings.
- Focused on disclosures concerning the quality of the Company's security program and disclosures regarding specific cybersecurity incidents.
- SEC also brought disclosure controls and procedures-based claims



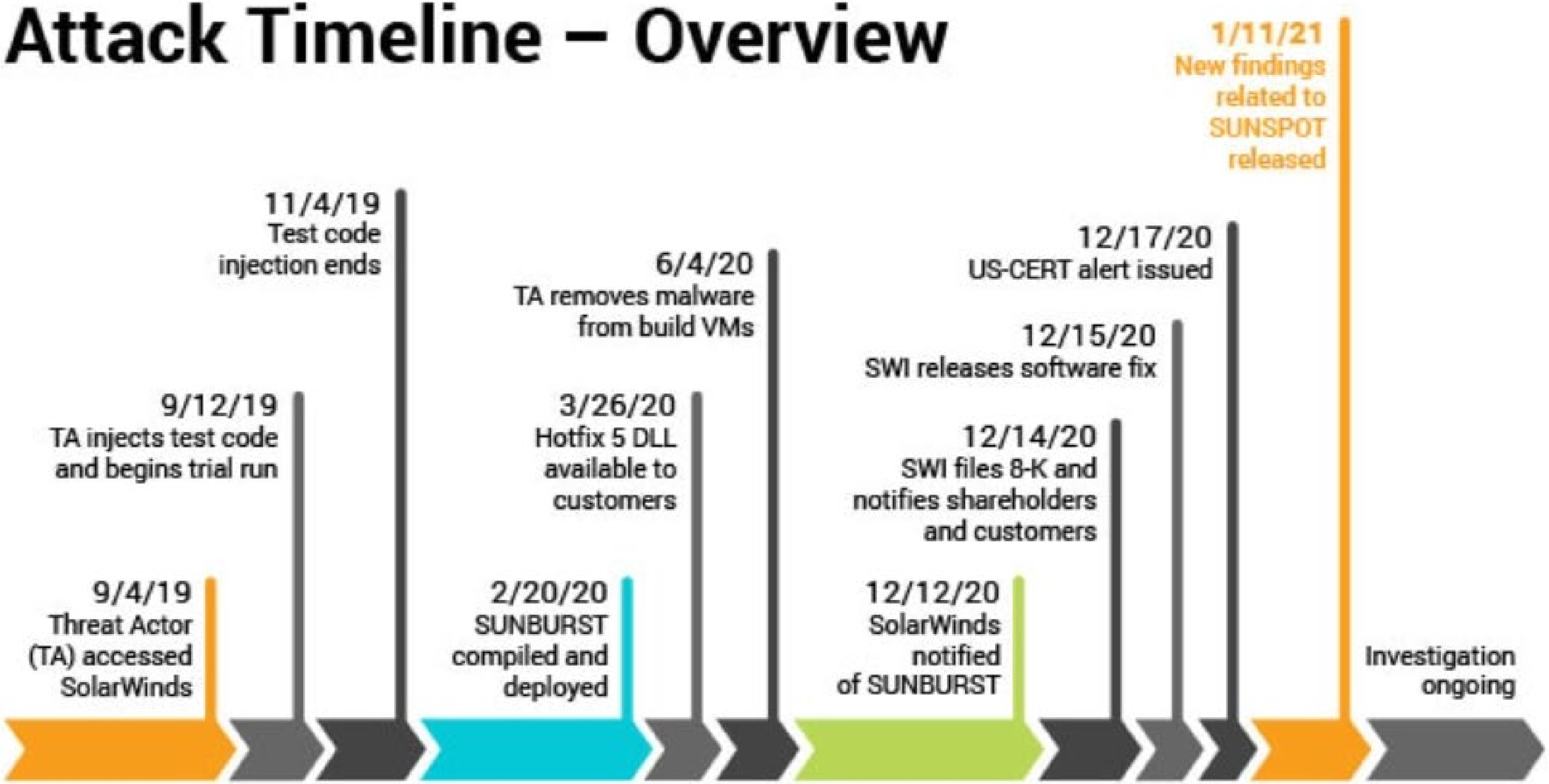
Attack



Source: Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents

pillsbury

Attack Timeline – Overview



All events, dates, and times approximate and subject to change; pending completed investigation.

Source: New Findings From Our Investigation of SUNBURST

pillsbury

SEC v. SolarWinds Corp. & CISO (Oct. 30, 2023)

PRESS RELEASE

Copy Link

SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures

Complaint alleges software company misled investors about its cybersecurity practices and known risks

FOR IMMEDIATE RELEASE | 2023-227

Washington D.C., Oct. 30, 2023 — The Securities and Exchange Commission today announced charges against Austin, Texas-based software company SolarWinds Corporation and its chief information security officer, Timothy G. Brown, for fraud and

CHRISTOPHER BRUCKMANN
(SDNY Bar No. CB-7317)
Attorney for Plaintiff
SECURITIES AND EXCHANGE COMMISSION
100 F Street, N.E.
Washington, D.C. 20549
(202) 551-5986
BruckmannC@sec.gov

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	Civil Action No. 23-cv-9518 Jury Trial Demanded

COMPLAINT

Plaintiff Securities and Exchange Commission ("SEC"), for its Complaint against Defendants SolarWinds Corp. ("SolarWinds" or "the Company") and Timothy G. Brown ("Brown") (collectively, "Defendants"), alleges as follows:

Source: SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures; *Securities Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*

SEC v. SolarWinds Corp. & CISO (Oct. 30, 2023)

- "SolarWinds chose to use the NIST [National Institute of Standards and Technology] Framework … to conduct assessments…. SolarWinds admitted in internal documents that it had no program or practice in place for a majority of the controls in the NIST Framework, and had assessed itself to be performing poorly on multiple critical controls."

Press Release

SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures

Complaint alleges software company misled investors about its cybersecurity practices and known risks

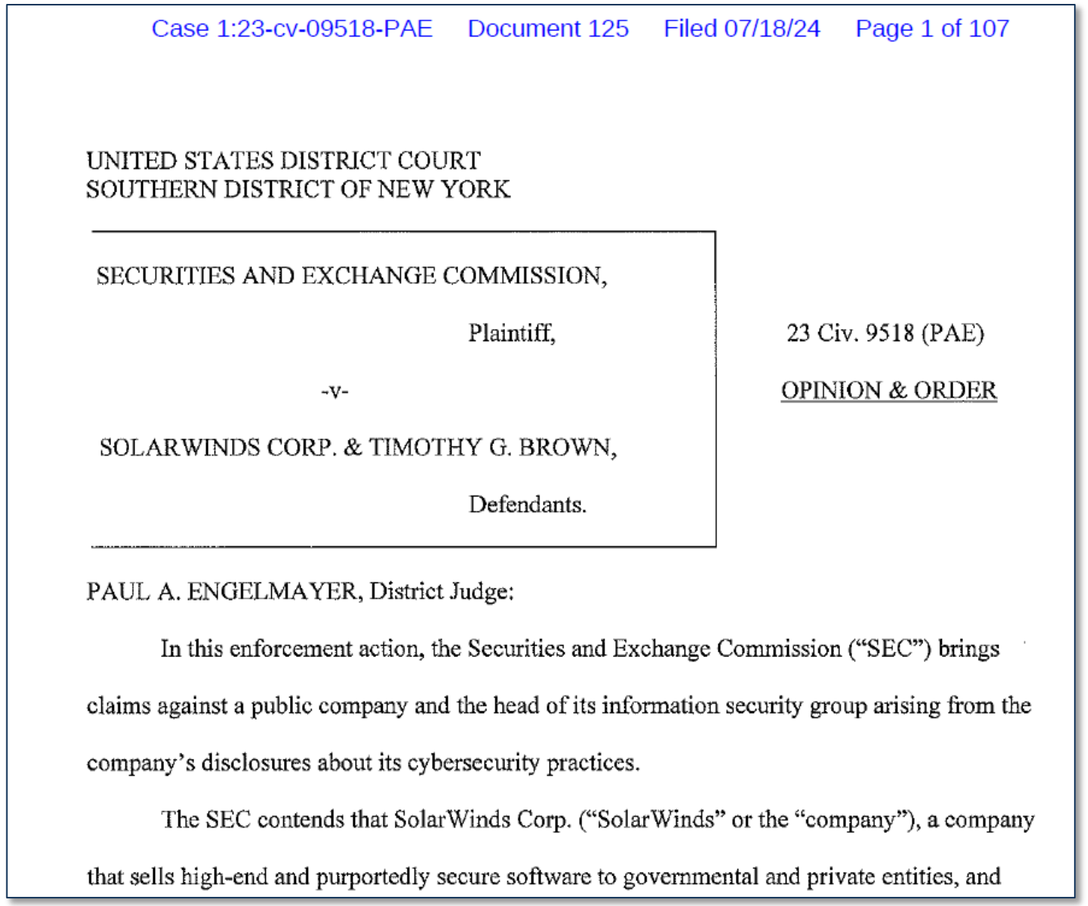
FOR IMMEDIATE RELEASE
2023-227

Washington D.C., Oct. 30, 2023 — The Securities and Exchange Commission today announced charges against Austin, Texas-based software company SolarWinds Corporation and its chief information security officer, Timothy G. Brown, for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities. The complaint alleges that, from at least its October 2018 initial public offering through at least its December 2020 announcement that it was the target of a massive, nearly two-year long cyberattack, dubbed "SUNBURST," SolarWinds and Brown defrauded investors by overstating SolarWinds' cybersecurity practices and understating or failing to disclose known risks. In its filings with the SEC during this period, SolarWinds allegedly misled investors by disclosing only generic and hypothetical risks at a time when the company and Brown knew of specific deficiencies in SolarWinds' cybersecurity practices as well as the increasingly elevated risks the company faced at the same time.

Source: SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures

Motion to Dismiss Ruling (July 18, 2024)

- Granted most of motion to dismiss against the company and its former CISO including on Form 8-K filings.
- Allowed claims against company and CISO alleging that a "Security Statement" posted on its website in 2017 may have been false or misleading.



Case 1:23-cv-09518-PAE Document 125 Filed 07/18/24 Page 1 of 107

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION,

Plaintiff,

-v-

SOLARWINDS CORP. & TIMOTHY G. BROWN,

Defendants.

23 Civ. 9518 (PAE)

OPINION & ORDER

PAUL A. ENGELMAYER, District Judge:

In this enforcement action, the Securities and Exchange Commission ("SEC") brings claims against a public company and the head of its information security group arising from the company's disclosures about its cybersecurity practices.

The SEC contends that SolarWinds Corp. ("SolarWinds" or the "company"), a company that sells high-end and purportedly secure software to governmental and private entities, and

Source: United States Securities and Exchange Commission Form 8-K

Voluntary Dismissal (Nov. 20, 2025)

Joint stipulation with SolarWinds Corporation and its Chief Information Security Officer "to dismiss, with prejudice, the Commission's ongoing civil enforcement action. As stated in the joint stipulation, the Commission's decision to seek dismissal is "in the exercise of its discretion" and 'does not necessarily reflect the Commission's position on any other case.'"

SolarWinds Corp. and Timothy G. Brown

U.S. SECURITIES AND EXCHANGE COMMISSION

Litigation Release No. 26423 / November 20, 2025

***Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, No. 1:23-cv-09518-PAE (S.D.N.Y. filed Oct. 30, 2023)**

SEC Dismisses Civil Enforcement Action Against SolarWinds and Chief Information Security Officer

Source: *SolarWinds Corp. and Timothy G. Brown* | Litigation Release No. 26423

The SolarWinds "Sweep"

- In addition to pursuing SolarWinds, the SEC conducted a sprawling sweep in which it investigated dozens of other issuers.
- All of those companies were impacted by SolarWinds' software compromise and by related activity.
- SEC charged four additional companies; investigation concluded with new administration
- SEC stressed the importance of proactive remedial measures to address perceived security deficiencies.

PRESS RELEASE

SEC Charges Four Companies With Misleading Cyber Disclosures

One company, Unisys Corp., also charged with controls violations

FOR IMMEDIATE RELEASE | 2024-174

Washington D.C., Oct. 22, 2024 — The Securities and Exchange Commission today charged four current and former public companies – Unisys Corp., Avaya Holdings Corp., Check Point Software Technologies Ltd, and Mimecast Limited – with making materially misleading disclosures regarding cybersecurity risks and intrusions. The SEC also charged Unisys with disclosure controls and procedures violations. The companies agreed to pay the following civil penalties to settle the SEC's charges:

- Unisys will pay a $4 million civil penalty;
- Avaya. will pay a $1 million civil penalty;
- Check Point will pay a $995,000 civil penalty; and
- Mimecast will pay a $990,000 civil penalty.

pillsbury

In re SolarWinds Corp. Securities Litigation, No. 1:21-cv-00138-RP (W.D. Tex.)

- Class action on behalf of persons or entities who purchased or otherwise acquired publicly traded SolarWinds securities between October 18, 2018 and December 17, 2020
- Defendants:
  - Company – which sells network monitoring software
  - CEO
  - VP Security Architecture
  - Two private equity firms that controlled SolarWinds, having taken it private in 2016 and then taken it public again in 2018 (first day of class period)

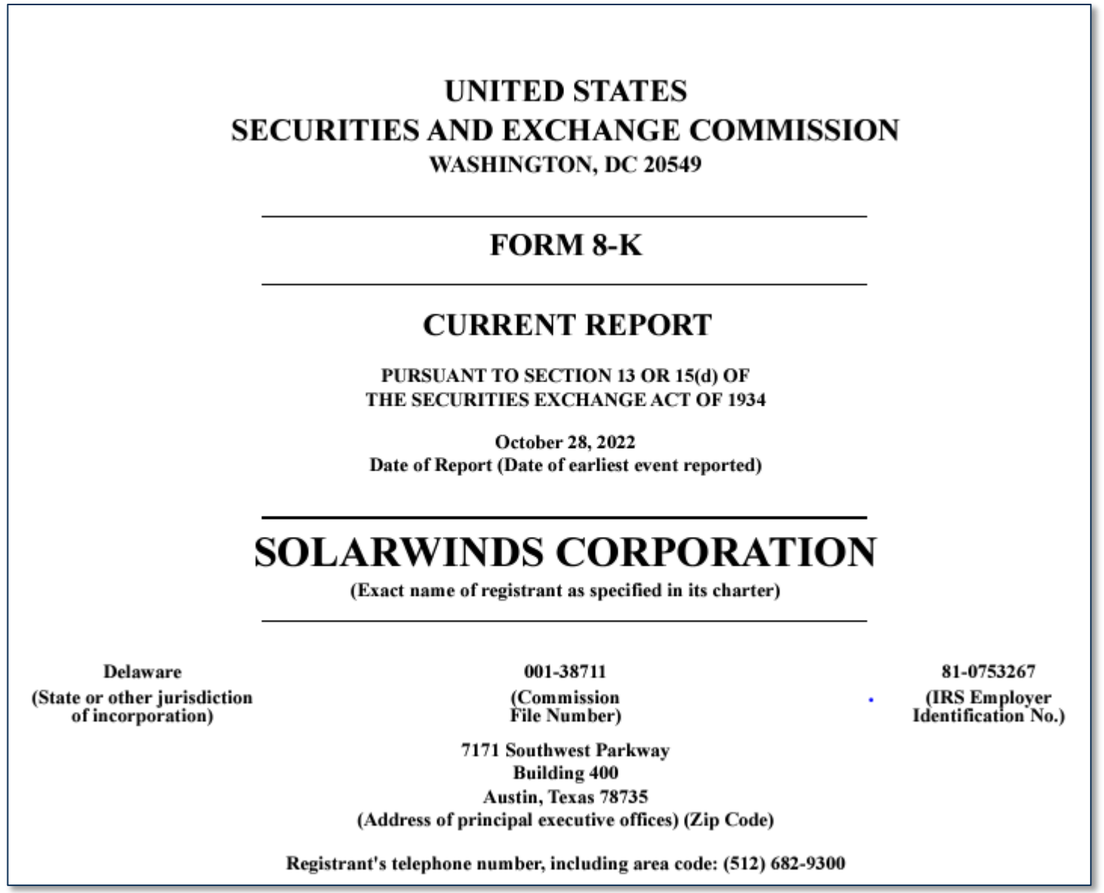
Allegations:

- SolarWinds told investors it had a robust cyber security program and adhered to practices outlined in its "Security Statement"
- But SolarWinds suffered "the largest cyberattack in U.S. history"
- SolarWinds former Global Cybersecurity Strategist told plaintiffs' counsel "from a security perspective, SolarWinds was an incredibly easy target to hack":
  - No security team
  - No password policy
  - User access was not limited
- Password to Update Server—"solarwinds123"--was publicly posted for 16 months
- December 13, 2020: press reports that cybercriminals had accessed to SolarWinds' server for nearly two years and disseminated malware to tens of thousands of customers
- Stock price fell 34%
- During class period, Defendants sold $730 million of SolarWinds stock

Source: FORM 8-K SolarWinds Corporation

SolarWinds Shareholder Class Action Settlement – October 2022

- Mediation followed denial in substantial part of motion to dismiss.
- Settled for cash payment of $26 million
- Resolved all claims against “the Company and the other named defendants.”
- Authorized and approved by the Company’s insurers and expected to “be funded entirely by applicable directors’ and officers’ liability insurance.”



UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, DC 20549

FORM 8-K

CURRENT REPORT

PURSUANT TO SECTION 13 OR 15(d) OF
THE SECURITIES EXCHANGE ACT OF 1934

October 28, 2022
Date of Report (Date of earliest event reported)

SOLARWINDS CORPORATION
(Exact name of registrant as specified in its charter)

Delaware	001-38711	81-0753267
(State or other jurisdiction of incorporation)	(Commission File Number)	(IRS Employer Identification No.)

7171 Southwest Parkway
Building 400
Austin, Texas 78735
(Address of principal executive offices) (Zip Code)

Registrant's telephone number, including area code: (512) 682-9300

Source: FORM 8-K SolarWinds Corporation

Derivative Actions and *Caremark* Claims – 1

- Derivative actions frequently free-ride on securities class actions
  - Bootstrap allegations: breaches of fiduciary duty led to data breaches which led to class actions; corporation harmed financially by need to defend class action; reputational harm, too
  - Derivative plaintiffs seek a place at the table when settlement is discussed
- "Bad faith is established, under *Caremark*," by way of either prong one, "when the directors completely fail to implement any reporting or information system or controls," or via prong two, when directors, "having implemented such a system or controls, consciously fail to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."

  — *Marchand v. Barnhill*, 212 A.3d 805, 821 (Del. 2019).

pillsbury

Derivative Actions and *Caremark* Claims – 2

Caremark claims alleging data breaches largely have been unsuccessful:

- *Firemen's Ret. Sys. of St. Louis v. Sorenson*, C.A. No. 2019-0965-LWW (Del. Ch. Oct. 5, 2021) (Marriott):
  - "plaintiff has not shown that the directors completely failed to undertake their oversight responsibilities, turned a blind eye to known compliance violations, or consciously failed to remediate cybersecurity failures."
- *Construction Industry Laborers Pension Fund v. Bingle*, C.A. No. 2021-0940-SG (Del. Ch. Sept. 6, 2022) (SolarWinds)
  - Case dismissed despite inattentive board where board committee actively considered cyber security; most alleged red flags never reached the board.
- Both complaints failed to allege facts showing "bad faith" or conscious disregard of duty.

pillsbury

Lessons From Other Cases

Other Data Breach and Cyber Cases

- Securities Class Actions and Derivative Actions
  - Equifax
    - Multiple regulators and cases
  - Yahoo! Data Breach
    - SEC and other cases
  - Recent Trends: *Block*, *Marriott* and *PayPal*
  - New Class Actions in 2025: *Coupang* and *F5*
- FTC: *In the Matter of Drizly, LLC & CEO*
- Criminal Case: *U.S. v. Joseph Sullivan*

pillsbury

Equifax Inc. – Security Vulnerability Identified

BUSINESS NEWS
OCTOBER 2, 20177:52 AM

Equifax failed to patch security vulnerability in March: former CEO

By David Shepardson
3 MIN READ

WASHINGTON (Reuters) - Equifax Inc EFX.N was alerted in March to the software security vulnerability that led to hackers obtaining personal information of more than 140 million Americans but took months to patch it, its former CEO said in testimony to be delivered to Congress on Tuesday.

"It appears that the breach occurred because of both human error and technology failures," former CEO Richard Smith said in written testimony released on Monday by the Energy and Commerce Committee.

EQUIFAX | PERSONAL | BUSINESS | GOVERNMENT | ABOUT US | Support

About Us > Investor Relations > News and Events > Press Releases > 2017

Equifax Chairman, CEO, Richard Smith Retires; Board of Directors Appoints Current Board Member Mark Feidler Chairman; Paulino do Rego Barros, Jr. Appointed Interim CEO; Company to Initiate CEO Search

Financial Information | News and Events | Stock Information | Stockholder Services | Contact Us

Sep 26, 2017

ATLANTA, Sept. 26, 2017 /PRNewswire/ -- The Board of Equifax Inc. (NYSE: EFX) today announced that Richard Smith will retire as Chairman of the Board and Chief Executive Officer, effective September 26, 2017. The Board of Directors appointed current Board member, Mark Feidler, to serve as Non-Executive Chairman. Paulino do Rego Barros, Jr., who most recently served as President, Asia Pacific, and is a seven-year veteran of the company, has been appointed as interim Chief Executive Officer, succeeding Smith. The Board will undertake a search for a new permanent Chief Executive Officer, considering candidates both from within and outside the company. Mr. Smith has agreed to serve as an unpaid adviser to Equifax to assist in the transition.

Source: Equifax | Investor Relations - Press Releases; Equifax failed to patch security vulnerability in March: former CEO

Equifax Inc. – FTC and CFPB Enforcement

12/22/25, 6:03 AM CFPB, FTC and States Announce Settlement with Equifax Over 2017 Data Breach | Consumer Financial Protection

cfpb Consumer Financial Protection Bureau

CFPB, FTC and States Announce Settlement with Equifax Over 2017 Data Breach

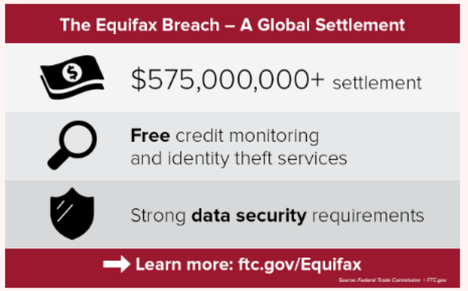
JUL 22, 2019

WASHINGTON, D.C. – The Consumer Financial Protection Bureau (Bureau), the Federal Trade Commission (FTC), and 48 states, the District of Columbia and Puerto Rico announced a global settlement today with Equifax that would provide up to $700 million in monetary relief and penalties. In a complaint and proposed stipulated judgment filed in federal district court in the Northern District of Georgia, the Bureau alleges that Equifax engaged in unfair and deceptive practices in connection with the 2017 data breach of Equifax's systems that impacted approximately 147 million consumers. The proposed settlement with the Bureau, if approved by the court, will provide up to $425 million in monetary relief to consumers, a $100 million civil money penalty, and other relief. The Bureau coordinated its investigation with the FTC and attorneys general from across the country. In total, the settlements with these entities would impose up to $700 million in relief and penalties.

Equifax Inc. has agreed to pay at least $575 million, and potentially up to $700 million, as part of a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau (CFPB), and 50 U.S. states and territories, which alleged that the credit reporting company's failure to take reasonable steps to secure its network led to a data breach in 2017 that affected approximately 147 million people.

In its complaint, the FTC alleges that Equifax failed to secure the massive amount of personal information stored on its network, leading to a breach that exposed millions of names and dates of birth, Social Security numbers, physical addresses, and other personal information that could lead to identity theft and fraud.

As part of the proposed settlement, Equifax will pay $300 million to a fund that will provide affected consumers with credit monitoring services. The fund will also compensate consumers who bought credit or identity monitoring services from Equifax and paid other out-of-pocket expenses as a result of the 2017 data breach. Equifax will add up to $125 million to the fund if the initial payment is not enough to compensate consumers for their losses. In addition, beginning in January 2020,



Source: CFPB, FTC and States Announce Settlement with Equifax Over 2017 Data Breach ; https://www.ftc.gov/node/47878

Equifax Data Breach Cases

Case	Case Name	Settlement Amount
FTC and CFPB and State Enforcement Actions	*In re: Equifax Inc. Customer Data Security Breach Litigation*, No. 1:17-md-2800-TWT (NDGA)	**$575-700M**
Securities Class Action	*In re. Equifax Inc. Securities Litigation*, No. 1:17-cv-03463 (NDGA)	**$149M**
Derivative Lawsuit	*In re. Equifax Inc. Derivative Litigation*, No. 1:18-cv-00317 (NDGA)	**$32.5M**
Indiana	*State of Indiana v. Equifax Information Services LLC*, No, 49D11-1905-PL-018398 (Marion County Circuit and Superior Court)	**$19.5M**
New York State Department of Financial Services	*In the Matter of Equifax Inc.* (NYDFS)	**$19.2M**
Massachusetts	*Commonwealth of Massachusetts v. Equifax Inc.*, No. 1784-CV-3009BLS2 (Suffolk County Superior Court)	**$18.225M**
Chicago	*City of Chicago v. Equifax Inc.*, No. 1:17-cv-07798 (NDIL)	**$1.5M**

Equifax Securities Class Action

Motion to Dismiss Denied in Significant Part, 357 F. Supp. 3d 1189 (N.D. Ga. 2019)

Key Holdings:

- Plaintiff adequately alleged statements about strength of cybersecurity were false.
- Plaintiff adequately alleged statement that cybersecurity experts continually reviewed systems was false.
- Equifax's representations that its cybersecurity efforts were extensive or that it was committed to data security were not inactionable puffery.
- Defendants had no duty to disclose data breach before becoming aware of it.
- Statement in securities filings that Equifax "could be vulnerable" to cybersecurity breach was not false or misleading.
- Equifax's statements in securities filings about its internal controls were not false.
- Plaintiff raised strong inference of scienter as to CEO but not CFO, SVP IR or president of operating segment.

pillsbury

Equifax Securities Class Action

Chronology:

- 2014, 2016, March 2017: consultants warn of data security issues
- 2016: two long-lasting hacks obtained data as to hundreds of thousands of customer's employees
- March 2017: public warnings of key app's vulnerability
- July 29-31, 2017: hack discovered
- Early August: FBI notified; CFO and OpCo President sold over $1 million in stock
- August 17, 2017: CEO gives speech saying data fraud is his #1 worry
- September 7, 2017: hack affecting 143 Americans disclosed
- September 8-15, 2017: stock falls 36%

Alleged deficiencies:

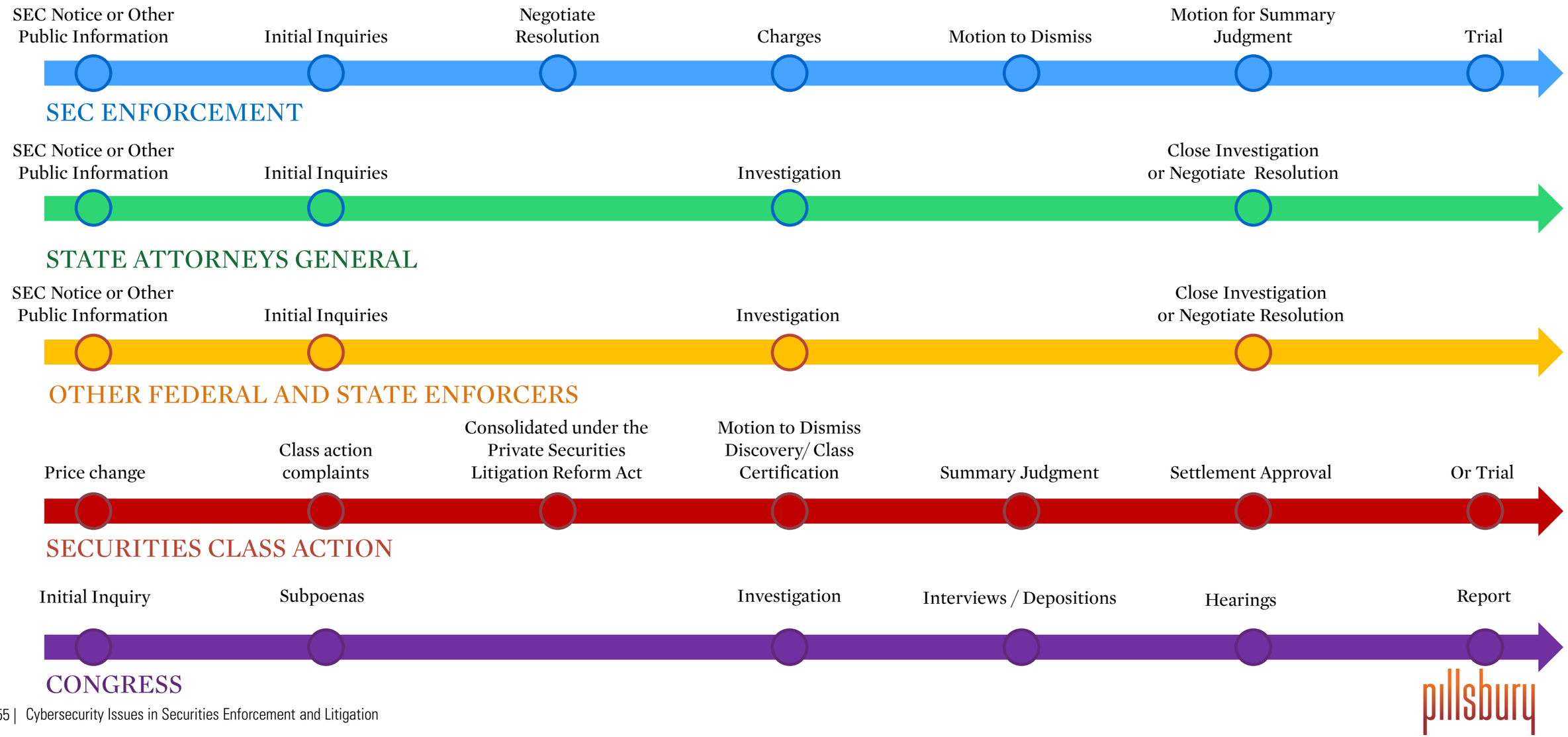
- Patch management—one employee, manual
- Customers' PII unencrypted
- Authentication measures weak
- PII stored in public channels
- Obsolete unneeded PII not warehoused

Actionable misstatements:

- "Rigorous" data management
- Regular reviews and updating protocols
- "Strong" data security
- "Trusted steward" of PII
- "Highly sophisticated data information network"

pillsbury

Managing Enforcement and Litigation Overlapping Timelines



pillsbury

House Oversight and Government Reform Committee

- "**Entirely preventable**. Equifax failed to fully appreciate and mitigate its cybersecurity risks. Had the company taken action to address its observable security issues, the data breach could have been prevented."
- "**Lack of accountability and management structure**. Equifax failed to implement clear lines of authority within their internal IT management structure, leading to an execution gap between IT policy development and operation. Ultimately, the gap restricted the company's ability to implement security initiatives in a comprehensive and timely manner."
- "**Complex and outdated IT systems**. Equifax's aggressive growth strategy and accumulation of data resulted in a complex IT environment. Both the complexity and antiquated nature of Equifax's custom-built legacy systems made IT security especially challenging."
- "**Failure to implement responsible security measurements**. Equifax allowed over 300 security certificates to expire, including 79 certificates for monitoring business critical domains. Failure to renew an expired digital certificate for 19 months left Equifax without visibility on the exfiltration of data during the time of the cyberattack."


COMMITTEE RELEASES REPORT REVEALING NEW INFORMATION ON EQUIFAX DATA BREACH

PUBLISHED: DEC 10, 2018

WASHINGTON, DC – House Oversight and Government Reform Committee Republicans released a staff report after the Co... each, one of the largest data breaches...

Through the investigatio... nts, conducted transcribed in... olved with

U.S. House of Representatives
Committee on Oversight and Government Reform

OVERSIGHT & GOVERNMENT REFORM EST 1814

The Equifax Data Breach

Majority Staff Report
115th Congress

December 2018

Source: The Equifax Data Breach Majority Staff Report; Committee Releases Report Revealing New Information on Equifax Data Breach

pillsbury

Yahoo! Data Breach: SEC Enforcement Action

PRESS RELEASE

Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million

FOR IMMEDIATE RELEASE | 2018-71

Washington D.C., April 24, 2018 —The Securities and Exchange Commission today announced that the entity formerly known as Yahoo! Inc. has agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose one of the world's largest data breaches in which hackers stole personal data relating to hundreds of millions of user accounts.

Source: Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million

Yahoo! Data Breach Litigation

Case	Case Name	Settlement Amount / Date
SEC Enforcement Action	*In the Matter of ALTABA INC., f/d/b/a YAHOO! Inc.*, Administrative Proceeding File No. 3-18448	**$35 million** SEC Order (April 2018)
Securities Class Action	*In Re Yahoo! Inc. Securities Litigation*, Case No. 17-CV-00373-LHK (NDCA)	**$80 million settlement** (Sept. 2018)
Shareholder and Derivative Actions	*In Re Yahoo! Inc. Shareholder Litigation*, Lead Case No. 17-CV-307054 (Superior Court Santa Clara County) *Summer v. Mayer, et al*, No. 17-cv-00787 (NDCA) *Bowser v. Mayer, et al.*, No. 5:17-cv-00810-LHK (NDCA) *Oklahoma Firefighters Pension & Retirement System v. Brandt*, No. 2017-0133-SG (Delaware Chancery)	**$29 million settlement** (Jan. 2019)
Consumer Class Action	*Yahoo! Inc. Customer Data Security Breach Litigation*, Case No. 5:16-MD-02752-LHK (NDCA)	**$117.5 million settlement** (July 2020)
DOJ Prosecution of Russian Hackers	*United States of America v. Dmitry Dokuchaev, Igor Sushchin, Alexsey Belan, and Karim Baratov*, Case No. CR 17-00277 LHK (NDCA)	Conviction of one hacker who was sentenced to five years in prison

Source: Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million; International Hacker-For-Hire Who Conspired With And Aided Russian FSB Officers Sentenced To Five Years In Prison; *In re: Yahoo! Inc. Customer Data Security Breach Litigation* | Order Denying Motion for Preliminary Approval of Class Action Settlement

Yahoo! Securities Class Action

Motion to dismiss First Amended Complaint briefed but never argued

Allegations of Second Amended Complaint filed February 2, 2018:

- 2013: Hackers stole records of three billion users – not disclosed until 2016
- 2014: Hacker compromised the accounts of 500 million users – not disclosed until 2016
- 2015 and 2016: Cookie-forging data breaches affected 32 million users – not disclosed until 2017
- Yahoo! represented that it had "best practices" security
- Yahoo! said it would disclose any breach within 90 days of discovery

- Settlement reached March 3, 2018.

pillsbury

The Tide Turns?

"During the last five years, there have been 19 securities class action suits with claims related to cybersecurity and/or customer privacy breaches. Twelve of these were filed in 2021–2022, while only two suits were filed in each of 2023 and 2024. There were three suits filed in 2025 against Fortinet, Inc., Coupang, Inc., and F5, Inc., all in the second half of the year."

— NERA, *Recent Trends in Securities Class Action Litigation: 2025 Full-Year Review* 12 (Jan. 21, 2026). This is against a backdrop of 200+ securities class actions filed in each of the past five years.

"There was a time, not that long ago, that commentators (including me) were predicting that there would be massive amounts of cyber-related D&O litigation. Since that earlier time there have indeed been some cyber-related securities suits filed, but these kinds of suits have never really accumulated in the volume anticipated."

— Kevin LaCroix, *The D&O Diary*, Dec. 21, 2025.

pillsbury

Alphabet, Block, Marriott and *PayPal*—The Tide Turns?

Sgarlata v. PayPal Holdings, Inc., 409 F. Supp. 3d 846 (N.D. Cal. 2019):

- Allegations:
  - July 2017: PayPal buys TIO Networks
  - November 2017: PayPal suspends TIO's operations after discovery of security vulnerabilities
  - December 2017: Announcement PII compromised for 1.6 million TIO customers, stock price drops 5.75%
  - November announcement said compromise when there was an actual data breach
- Holding on motion to dismiss second amended complaint:
  - Falsity sufficiently alleged because November announcement said vulnerability, not actual breach
  - Scienter fails despite three confidential witnesses and one expert
    - Lack of motive to deceive
    - Confidential witnesses did not show November speaker knew of actual breach in November
    - Expert did not speak to employees or review documents – just guesswork
  - Ninth Circuit affirmed dismissal: suspension of TIO's operations rebuts scienter; defendants sold no stock or had other motive to mislead investors

pillsbury

Alphabet, *Block*, *Marriott* and *PayPal*—The Tide Turns?

In re Alphabet, Inc. Securities Litigation, 1 F.4th 687 (9th Cir. 2021):

- Allegations:
  - March 2018: Google discovered security bug in Google+ left PII of users vulnerable to developers for three years even if user had designated their PII non-public
  - Google concealed vulnerability, made generic statements about risks, never changed risk factors
    - Risk factor: "Concerns about our practices with regard to the collection, use, disclosure, or security of personal information or other privacy related matters, even if unfounded, could damage our reputation and adversely affect our operating results."
  - April 2018: senior management advised of bug, publicly said no material changes in risk
  - October 2018: *Wall St. Journal* discloses bug, lawsuits begin
- District court dismissed, holding allegations of falsity and scienter both failed
- Ninth Circuit reversed in part:
  - April and July 2018 statement "no material changes" in risk sufficiently alleged falsity, as did failure to disclose bug (even though bug had been remedied) and even though no allegations that PII had been released
  - Strong inference of scienter as to Sergei Page, motive to buy time while Facebook was being publicly slammed
  - No scienter based on Pichai's statements about Google's commitment to data security – puffery
- Case settled in 2024 for $350 million

pillsbury

Alphabet, Block, Marriott and *PayPal*—The Tide Turns?

In re Marriott International, Inc., 31 F.4th 898 (4th Cir. 2022):

- Allegations:
  - 2018: Marriott discovered malware impacted 500 million guest records
  - Plaintiffs alleged 73 misstatements, mainly "statements about the importance of protecting customer data; privacy statements on Marriott's website; and cybersecurity-related risk disclosures"
- District court dismissed, Fourth Circuit affirmed—falsity not adequately pled:
  - Statements about importance were not false, unlike *Equifax*, no claim Marriott's security was superior; Marriott admitted its security efforts could fail
  - Website statements that Marriott sought to take reasonable steps but could fail also were not false
  - While warning of risks when one knows of actualities is actionable, no showing that defendants knew of malware when they warned of risks—risk factors were updated once malware was discovered

pillsbury

Alphabet, *Block*, *Marriott* and *PayPal*—The Tide Turns?

In re Block, Inc. Securities Litigation, 2025 WL 2607890 (S.D.N.Y. Sept. 25, 2025):

- Allegations:
  - December 2021: former Block employee stole PII of 8.2 million users of the Cash App investment brokerage business
  - April 2022: Block announces breach via 8-K
  - Before April 2022 announcement:
    - Block emphasized risk of data breach but omitted to say its security was below standards
    - January and February 2022 SEC filings omitted mention of breach
    - Plaintiffs' expert said security subpar (but could not say how hack occurred)
- Case dismissed on both falsity and scienter grounds
  - Pre-incident statements too general—allegations do not show security was deficient and Block did not make claims as to the quality of its security beyond puffery that it took reasonable measures
  - Post-incident statements did not address security and no showing speakers knew of incident
  - Scienter allegations insufficient—no motive or showing speakers knew of incident
- Motion for reconsideration pending

Data Breach Securities Class Actions Filed in 2025

- *Barry v. Coupang, Inc.*, No. 3:25-cv-10795-VC (N.D. Cal. Dec. 18, 2025)
- *Smith v. F5, Inc. et al.*, No. 2:25-cv-2619 (W.D. Wash. Dec. 19, 2025)
- A third case, against a data security company, is really not a data breach case
  - *Oklahoma Firefighters Pension and Retirement System v. Fortinet, Inc.*, No. 25-cv-8037 (N.D. Cal. Sept. 22, 2025) and Consolidated Actions
    - **Allegations:**

      Between Nov. 8, 2024, and Aug. 6, 2025, Fortinet misrepresented the profitability and scale of a firewall upgrade cycle. The company allegedly concealed that the upgrades involved older products representing a small part of Fortinet's business.

      No allegations about data security or data breaches, though a hacker called "Fortibitch" claimed to have leaked 440GB of data affecting less than 0.3% of its customers in September 2024
    - Case just beginning, lead plaintiff and plaintiff counsel not chosen yet

pillsbury

Barry v. Coupang, Inc., No. 3:25-cv-10795-VC (N.D. Cal. Dec. 18, 2025)

- Nov. 18, 2025: Coupang discovered massive data breach, compromising PII of over 33 million customers, "the largest data breach in South Korean history," with the breach caused by former employee who retained log-in credentials exploiting a vulnerability in systems.
- Nov. 30, 2025: Coupang apologizes publicly for breach (seven business days later)
- Dec. 10, 2025: CEO resigned; South Korean police opened investigation.
- Complaint alleges that misrepresented or failed to disclose that: "(1) Coupang had inadequate cybersecurity protocols that allowed a former employee to access sensitive customer information for nearly six months without being detected; (2) this subjected Coupang to a materially heightened risk of regulatory and legal scrutiny; (3) When Defendants became aware that Coupang had been subjected to this data breach, they did not report it in a current report filings (to be filed with the SEC) in compliance with applicable reporting rules; and (4) as a result, Defendants' public statements were materially false and/or misleading at all relevant times."

pillsbury

Smith v. F5, Inc. et al., No. 2:25-cv-2619 (W.D. Wash. Dec. 19, 2025)

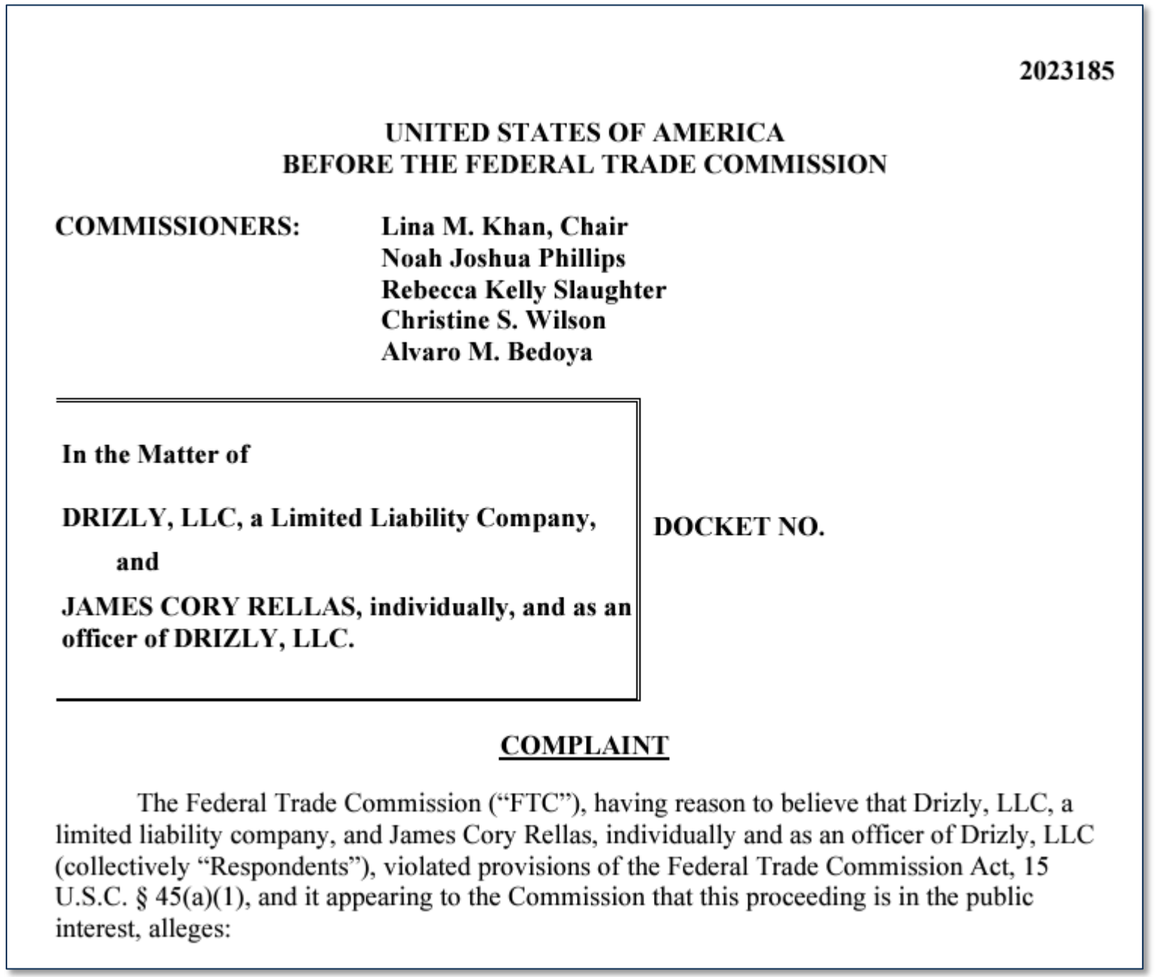
- Allegations:
  - Defendants touted their application security systems— ”a security and software leader in today′s hybrid multicloud world”
  - Oct. 15, 2025: F5 announced it had learned in August of a “long-term, persistent” security breach caused by a “nation-state threat actor”—source code for key product was stolen—but said the “incident has not had a material impact on the Company’s operations, and the Company is evaluating the impact this incident may reasonably have on its financial condition or results of operations”; stock price fell 13.9%
  - Oct. 27, 2025: F5 announced record Q4 financial results but lowered guidance for Q1 and FY2026; stock price fell 10.9%
  - Scienter allegations focus on claims of “best in class” security and Oct. 15 claim of no material impact

pillsbury

FTC— In the Matter of Drizly, LLC & CEO

Allegations

- Failed to implement basic security measures to secure personal information collected and stored. No two-factor authentication for GitHub, limiting employee access, adequate written security policies, or training employees.
- Stored critical database information on an unsecured platform including login credentials on GitHub.
- Neglected to monitor network for security threats including a senior executive ensuring its data was secure and monitoring network.
- Exposed customers to hackers and identity thieves.



2023185

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Noah Joshua Phillips
Rebecca Kelly Slaughter
Christine S. Wilson
Alvaro M. Bedoya

In the Matter of

DRIZLY, LLC, a Limited Liability Company,
and
JAMES CORY RELLAS, individually, and as an officer of DRIZLY, LLC.

DOCKET NO.

COMPLAINT

The Federal Trade Commission ("FTC"), having reason to believe that Drizly, LLC, a limited liability company, and James Cory Rellas, individually and as an officer of Drizly, LLC (collectively "Respondents"), violated provisions of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1), and it appearing to the Commission that this proceeding is in the public interest, alleges:

Source: FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers; In the Matter of Drizly, LLC and James Cory Rellas | Complaint

FTC – In the Matter of Drizly, LLC & CEO

Enforcement Order to Follow CEO

- Order "applies personally to" the CEO.
- "In the modern economy, **corporate executives frequently move** from company to company, notwithstanding blemishes on their track record."
- "Recognizing that reality, the Commission's **proposed order will follow** [the CEO] even if he leaves Drizly."
- "Specifically, [the CEO] will be required to implement an information security program at future companies if he moves to a business collecting consumer information from more than 25,000 individuals, and where he is a majority owner, CEO, or senior officer with information security responsibilities."

Source: FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers;
In the Matter of Drizly, LLC and James Cory Rellas | Complaint

FTC – In the Matter of Drizly, LLC & CEO

Enforcement Order to Follow CEO

- "**[F]or 10 years** after issuance of this Order" Company Chief Executive Officer "for any Relevant Business that he is: 1) majority owner; or 2) employed or functions as a Chief Executive Officer or other senior officer with direct or indirect responsibility for information security,
- "must within 180 days ensure that the business has established and implemented, and thereafter maintains, a **comprehensive information security program** ("Business ISP") that protects the security, confidentiality, and integrity of Covered Information."
- Specific requirements for Business ISP.

Source: FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers;
In the Matter of Drizly, LLC and James Cory Rellas | Complaint

FTC Oversight Role through Orders

Example: Annual Certification

- By "Chief Executive Officer, President" or equivalent
  - "The certification must be based on the **personal knowledge** of" the CEO or whom the CEO "reasonably relies in making the certification."

Certification that the business:

- (1) "has established, implemented, and maintained the requirements of this Order;"
- (2) "is **not aware of any material noncompliance** that has not been (a) corrected or (b) disclosed to the Commission;" and
- (3) "includes a brief description of all **Covered Incidents** that Corporate Respondent verified or confirmed during the certified period."

pillsbury

NYDFS Cybersecurity Regulation Overview for Covered Entities

Annual Submission of Certification of Material Compliance or Acknowledgement of Noncompliance [Section 500.17(b)(1)]

- By **April 15th**, for prior calendar year
- Signed by the **highest-ranking executive** and the **CISO**
- Submitted electronically
- Maintain records "for examination and inspection by" DFS "for a period of five years"

U.S. v. Joseph Sullivan: Trial Conviction (Oct. 5, 2022)

PRESS RELEASE

Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records

Wednesday, October 5, 2022

Share

For Immediate Release

U.S. Attorney's Office, Northern District of California

Federal Jury Finds Joseph Sullivan Guilty of Obstruction of the Federal Trade Commission and Misprision of a Felony

SAN FRANCISCO – A federal jury convicted Joseph Sullivan, the former Chief Security Officer of Uber Technologies, Inc. ("Uber"), of obstruction of proceedings of the Federal Trade Commission ("FTC") and misprision of felony in connection with his attempted cover-up of a 2016 hack of Uber. The announcement was made by United States Attorney Stephanie M. Hinds and FBI San Francisco Special Agent in Charge Robert K. Tripp following a four week trial before the Hon. William H. Orrick, United States District Judge.

Source: Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records

Non-Prosecution Agreement for Company

- First, changed management and prompt investigation by new leadership.
- Second, “substantial resources to significantly restructure and enhance the company’s compliance, legal, and security functions.”
- Third, FTC agreement “to maintain a comprehensive privacy program for 20 years and to report to the FTC any incident reported to other government agencies relating to unauthorized intrusion into individuals’ consumer information.”
- Fourth, ”full cooperation” with government investigations including “ongoing criminal case” against former CISO.
- Finally, 148 million civil settlement “with the attorneys general for all 50 States and the District of Columbia.”

PRESS RELEASE

Uber Enters Non-Prosecution Agreement Related to 2016 Data Breach

Friday, July 22, 2022

Share

For Immediate Release

U.S. Attorney's Office, Northern District of California

SAN FRANCISCO – Uber Technologies, Inc., has entered a non-prosecution agreement with federal prosecutors to resolve a criminal investigation into the coverup of a significant data breach suffered by the company in 2016, announced United States Attorney Stephanie M. Hinds and Federal Bureau of Investigation Special Agent in Charge Sean Ragan.

As part of a non-prosecution agreement to resolve the investigation, Uber admitted to and accepted responsibility for the acts of its officers, directors, employees, and agents in concealing its 2016 data breach from the Federal Trade Commission (“FTC”), which at the time of the 2016 breach had a pending investigation into the company’s data security practices. The FTC’s investigation continued from 2015 into 2017, and its written questions to Uber required Uber to provide information about any unauthorized access to personal information.

Source: Uber Enters Non-Prosecution Agreement Related to 2016 Data Breach

FTC Enforcement

Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims

Company failed to monitor access to, and provide reasonable security for, consumer data

August 15, 2017

Tags: Consumer Protection | Bureau of Consumer Protection | Technology | Automobiles | Privacy and Security | Consumer Privacy | Data Security

Note: *A conference call for media with FTC Acting Chairman Maureen K. Ohlhausen and Consumer Protection Acting Director Tom Pahl was held on August 15, 2017. FTC staff took questions from the media.*

Uber Technologies, Inc. has agreed to implement a comprehensive privacy program and obtain regular, independent audits to settle Federal Trade Commission charges that the ride-sharing company deceived consumers by failing to monitor employee access to

Related Cases

Uber Technologies, Inc., In the Matter of

Related actions

Uber Technologies, Inc; Analysis to Aid Public Comment; Proposed Consent Agreement

Settlement:

- "Required to implement a **comprehensive privacy program**."
- "Required to obtain within 180 days, and every two years after that for the **next 20 years, independent, third-party audits** certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order."
- "Prohibited from **misrepresenting** (a) how it monitors internal access to consumers' personal information" and (b) how it protects and secures that data.

Source: Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims

State Attorneys General Settlement

OFFERED BY Office of the Attorney General

PRESS RELEASE

AG Healey Leads Multistate Coalition in Reaching $148 Million Settlement With Uber Over Nationwide Data Breach

Massachusetts to Receive $7.1 Million in Settlement Over Data Breach that Compromised the Personal Data of More Than 57 Million Uber Passengers and Drivers

- **$148 million** settlement with multiple states.
- "As part of today's settlement, Uber has agreed to **settle the claims of all 50 states and the District of Columbia by consent judgments filed separately in each state**."
- "According to the complaint, instead of reporting the breach as soon as practicable, as required by Massachusetts Data Security Law, Uber tried to cover it up at the direction of its top executives by **paying the hackers $100,000 in exchange for a non-disclosure agreement**. Uber did not notify its riders or drivers or the AG's office of the breach until nearly a year later."

Source: AG Healey Leads Multistate Coalition in Reaching $148 Million Settlement With Uber Over Nationwide Data Breach

International Fines

TECH

Uber fined nearly $1.2 million by British and Dutch authorities for 2016 data breach

PUBLISHED TUE, NOV 27 2018•6:02 AM EST | UPDATED TUE, NOV 27 2018•6:12 AM EST

Elizabeth Schulze
@ESCHULZE

SHARE

- "The U.K.'s Information Commissioner's Office (ICO) announced a **£385,000 fine ($491,284)** against the ride-sharing company for "failing to protect customers' personal information during a cyber attack" in October and November of 2016. The Dutch Data Protection Authority imposed its own **€600,000 ($679,257)** penalty for the same incident."

Source: Uber fined nearly $1.2 million by British and Dutch authorities for 2016 data breach

Best Practices

Best Practices

- **Manage Forensic Issues**
  - Understand scope of incident.
  - Determine data exfiltration, access or acquisition to data.
  - Use forensics to guide security and remediation efforts and develop litigation and regulator strategy.

- **Implement Attorney Client Privilege and Work Product Legal Protections**
  - Protections to obtain legal guidance and work product analysis based on the unique circumstances of the incident.
  - Ensure that forensic providers and any other vendors are acting at the direction of counsel.

- **Remediation Day One Focus**
  - Disable accounts, patch, change passwords, address vulnerabilities.
  - Early remediation will help address regulatory inquiries and litigation issues.
  - Review controls to address incident vulnerabilities.

Source: How Cos. Can Prep For Tightened Calif. Data Breach Notices

Best Practices

- **Disclosure Controls and Procedures**
  - Implement governance process and legal review of any notifications.
  - Review timeliness and adequacy of each notification under applicable notification standards.
- **Address SEC Notification Issues**
  - Broad definition of "cybersecurity incident."
  - Prompt review of "materiality" issues.
    - SEC focus on the "material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations."
  - Form 8-K, Item 1.05, notification within four business days that a cybersecurity incident is material.
- **Manage and Determine Other Notifications**
  - Manage notifications for multiple jurisdictions.
  - Consider divergent notification standards.
  - Manage staggered notification deadlines.
  - Ensure consistent regulatory and other notifications.
  - Address contractual notice obligations.
- **Customer and Public Relations and External Messaging**
  - Coordinate customer notifications and public relation issues, as needed.
  - Implement legal protections for guidance and strategy for customer and public relations.

Source: How Cos. Can Prep For Tightened Calif. Data Breach Notices

Best Practices

- **Securities Litigation Takeaways**
  - **Pre-incident**
    - Develop a rapid-response team and process so you can react quickly.
    - Board and senior management should review risks and security on a regular basis.
    - Don't brag or overpromise about data security.
    - Disclose risks and update risk factors as risks and security processes change.
  - **Post-incident**
    - Disclose promptly, within four days of "materiality" determination.
      - Per Form 8-K, Item 1.05 (eff. Dec. 23, 2023).
    - Be transparent both about what you know and what you don't know.
    - Update disclosures as facts are uncovered and confirmed.

- **Governance**
  - Demonstrate structure and process to manage cyber risk.
  - Risk assessment informs cybersecurity governance.
  - Board cyber committees.
  - Regular board-level cyber briefings
  - Cyber included in Enterprise Risk Management.
  - Did the company follow its own written cybersecurity policies?

Source: How Cos. Can Prep For Tightened Calif. Data Breach Notices

Best Practices

- **Anticipate and Develop Other Litigation Strategy**
  - Develop forensic and case narrative based on facts and incident.
  - Assess exposure and anticipate claims and defenses based on forensics, vulnerabilities, remediation and privileged internal investigation:
    - Consumer class actions.
    - Shareholder derivative suits.
    - Contractual indemnity claims.
    - Cyber insurance disputes.
  - Protect privileged communications and work product including on forensic analyses and reports.
  - Assess litigation focus and defense on the "reasonableness" of the company's cybersecurity practices **before** the incident.
  - Assess damages, harm and lack of standing (no concrete injury).
  - Consider arbitration and class waivers, if applicable,
  - Consider jurisdictional issues.

Source: How Cos. Can Prep For Tightened Calif. Data Breach Notices

More Resources

Resources

pillsbury

Checklist for Cybersecurity Issues in Securities Enforcement and Litigation

This checklist identifies issues and risks that may arise on cybersecurity matters and data breaches in securities enforcement and litigation. For these cases, determining the "materiality" of the cybersecurity incident can be dynamic and time-sensitive, focus on the initial forensic, remediation and responses, and test the company controls and governance of cybersecurity risk.

1) 1) Cybersecurity Incident.

☐ Confirm whether a "cybersecurity incident" occurred as defined by the SEC.

☐ "Cybersecurity incident" refers to "an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."

☐ Confirm if a cybersecurity incident or data breach occurred as defined under other applicable federal or state law standards. Consult with counsel if you have questions.

LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How Cos. Can Prep For Tightened Calif. Data Breach Notices

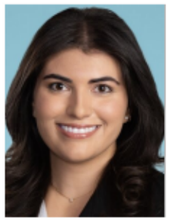
By **Mark Krotoski and Alexandria Marx** (November 10, 2025, 5:54 PM EST)

On Oct. 3, California enacted S.B. 446, which significantly amends the state's data breach notification laws.[1] The measure, which takes effect on Jan. 1, 2026, establishes specific deadlines for notifying affected individuals and the California attorney general about a data breach.

Mark Krotoski

Based on the new law, companies should prepare by reviewing and updating their incident response plans to ensure compliance with the new timelines, along with other federal and state notification deadlines.

Companies should also ensure they have effective processes in place to verify that notification content is accurate and complete. Enforcers carefully review the notifications for their timeliness and accuracy, and violations have been subject to substantial penalties and strict enforcement actions.



Alexandria Marx

Key Changes

As an overview, under the new law, businesses and government agencies must notify affected California residents "within 30 calendar days of discovery or notification of the data breach."[2]

If a breach affects more than 500 California residents, a sample copy of the consumer notification is required to be sent to the California attorney general "within 15 days of notifying affected consumers of the security breach."[3]

Notification may be delayed if necessary under two exceptions: (1) if a law enforcement agency "determines that the notification will impede a criminal investigation";[4] and (2) if it is "necessary to determine the scope of the breach and restore the reasonable integrity of the data system."[5]

New 30-Day Deadline for Notification to Individuals

Since 2002, California has mandated disclosure of a data breach "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement ... or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."[6] No deadline was specified.

Source: How Cos. Can Prep For Tightened Calif. Data Breach Notices

pillsbury

pillsbury

Questions

Mark L. Krotoski

Partner
Litigation
Full Biography
+1.650.233.4021
mark.krotoski@pillsburylaw.com

Mark Krotoski is an accomplished litigator, former DOJ leader and federal prosecutor who assists clients in their highest stakes issues, as well as managing crises, with a focus on antitrust and cartels, cybersecurity and cybercrime, and economic espionage. He leads the Cyber Disputes team and Cartel Enforcement team, drawing on his DOJ leadership and private sector experience.

Mark is a highly skilled litigator with nearly 20 years of DOJ experience, including leadership positions in three DOJ offices. His practice involves a diverse range of areas, with a strong focus on cybersecurity, antitrust matters, trade secrets, criminal and civil litigation, government investigations and white collar cases. With a proven track record, Mark has successfully navigated complex legal terrain, earning a reputation for managing high-stakes cases and providing strategic counsel. His wealth of knowledge and proficiency in the field allow him to consistently deliver exceptional results for his clients.

Mark has significant experience helping clients manage crises, including ransomware attacks and other cyber incidents, economic espionage and trade secret misappropriation, and responding to antitrust investigations, including navigating dawn raids. Leveraging his experience as a former federal prosecutor, Mark provides clients with practical advice to handle difficult issues as well as their collateral effects.

Prior to joining private practice, Mark most recently served as the Assistant Chief of the National Criminal Enforcement Section in the DOJ's Antitrust Division, where he supervised international criminal antitrust matters and prosecuted cartel cases. For more than nine years, Mark served as co-head of the privacy and cybersecurity practice of another international law firm.

He served as the national coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the Computer Crime and Intellectual Property Section of the DOJ's Criminal Division and as a federal prosecutor in Silicon Valley in the Northern District of California as a cybercrime prosecutor. As national coordinator, he oversaw approximately 250 federal prosecutors specially trained to prosecute cybercrime and intellectual property enforcement cases. He successfully prosecuted and investigated virtually every type of computer intrusion, cybercrime and criminal intellectual property violation.

He also served as the chief and deputy chief of the Criminal Division of the Northern District of California U.S. Attorney's Office.

Representative Experience

- In representing an international retail company, led the forensic investigation concerning a cyberattack involving the acquisition of millions of customer records in all U.S. jurisdictions and more than 100 countries, provided guidance on legal obligations and coordinated with law enforcement, resulting in the identification and conviction of the perpetrator outside the United States.
- In an active "no-poach" investigation by the Antitrust Division, coordinated an internal company investigation and response resulting in the closing of the investigation with no charges or enforcement action.
- Represents clients on cyberattacks and violations of the Computer Fraud and Abuse Act including data breach class action cases.

David Oliwenstein

Partner
Corporate Investigations & White Collar Defense
Full Biography
+1.212.858.1031
david.oliwenstein@pillsburylaw.com

David Oliwenstein, formerly with the SEC's Division of Enforcement, leads Pillsbury's Securities Enforcement practice. David advises clients on complex investigations, regulatory and criminal enforcement of the securities laws, and securities litigation.

Both in private practice and during his tenure at the SEC, David has led matters involving insider trading, cybersecurity, crypto assets, accounting misconduct, market manipulation, algorithmic trading, disclosure issues, ESG, recordkeeping requirements and offering frauds. In his final role at the SEC, David served as senior counsel in the Market Abuse Unit, the inaugural unit responsible for investigating crypto-asset-related misconduct. David's broad client base includes public companies, broker-dealers, investment advisers, digital asset issuers and exchanges, as well as corporate executives and other individuals.

David handles securities matters at all phases. In addition to representing clients in investigations, as well as in criminal and civil litigation, David works proactively with companies to design compliance programs and to develop and implement policies, procedures and controls, all with an eye toward preventing potential violations of law.

Representative Experience

- Represents public companies, audit committees, special litigation committees, broker-dealers, investment advisers, as well as other entities and individuals in government investigations regarding insider trading, accounting misconduct, crypto asset matters, cybersecurity, and other regulatory matters.
- As senior counsel in the SEC's Enforcement Division, investigated sophisticated insider trading schemes, complex market manipulation cases and market structure violations, and litigated accounting cases, insider trading actions and broker-dealer matters in federal district court and SEC administrative proceedings.
- Advises public companies and regulated entities regarding the development and implementation of policies, procedures, controls and compliance programs designed to ensure compliance with the securities laws.
- Represented executive in SEC investigation of crypto asset platform; convinced SEC leadership to decline to bring enforcement action.
- Represented publicly traded entertainment company and executives in SEC investigation regarding revenue recognition practices; convinced SEC staff to decline to pursue enforcement action.
- Represented various issuers in connection with SEC's "SolarWinds" sweep regarding potential cybersecurity violations; SEC staff declined to pursue enforcement action.
- Represented educational institution and senior executives in CFTC investigation regarding alleged insider trading in connection with COVID-19 pandemic.
- Led internal investigation for SEC regulated entity in response to approximately 50 distinct allegations of fraud, accounting violations, and related misconduct; represented Special Litigation Committee in related derivative action.

pillsbury

Bruce A. Ericson

Partner
Securities Litigation & Enforcement
Full Biography
+1.415.983.1560
bruce.ericson@pillsburylaw.com

Bruce Ericson, leader of Pillsbury's Securities Litigation team, has a stellar record of obtaining—and defending on appeal—dismissals of securities class actions and derivative actions.

Bruce, the managing partner of Pillsbury's San Francisco office (2008–2016), represents banks, companies (both large and small), boards and senior management in securities, M&A and corporate governance disputes, SEC investigations and litigation, and internal investigations. He has represented bank and bank regulatory agencies in all kinds of investigations and litigation, and has deep experience in antitrust, appellate, fraud and unfair competition litigation.

Representative Experience

- Won affirmance of dismissal of class action against Wells Fargo & Co. alleging wrongful redemption of $837.5 million of trust-preferred securities.
- Won affirmance of dismissal of securities class action against a leading aluminum company challenging its $1 billion accounting restatement.
- Won dismissal with prejudice of all claims in $6.8 billion action by federal regulators against the directors of the nation's largest corporate credit union.
- Bruce represents public companies, their boards and their senior management in securities and corporate governance disputes of all kinds, in SEC investigations and SEC litigation, and in internal investigations, including situations involving disputes among senior management and significant questioning by outside auditors. He has obtained many dismissals of class and derivative actions and is undefeated in defending such dismissals on appeal.
- Represented a major telephone company in *In re National Security Agency Telecommunications Records Litigation*, MDL No. 06-1791, a series of 40 actions alleging that telephone companies cooperated with the NSA's Terrorist Surveillance Program.
- Represented a geothermal developer in a 45-day jury trial of allegations that the developer had unlawfully recorded thousands of telephone conversations in violation of California's Invasion of Privacy Act and on appeal, ultimately obtaining complete victory for clients.

pillsbury

Thank you!

pillsbury