



Morgan Lewis

PREPARING FOR THE DOJ'S NEW CIVIL CYBER-FRAUD INITIATIVE

November 11, 2021

Mark Krotoski & Doug Baruch

© 2021 Morgan, Lewis & Bockius LLP

Presenters



Mark L. Krotoski



Doug W. Baruch

Morgan Lewis

Agenda

- Overview of the Cybersecurity Landscape
- Common Government Contract Cyber Scenarios and Risks
- Common Issues Arising Under Cyber Investigations
- New Civil Cyber-Fraud Initiative
 - Focus on failures to comply with cybersecurity standards; misrepresentation of security controls and practices; timely reporting of cyber incidents
- How DOJ and Qui Tam Relators may use the False Claims Act
 - Key FCA issues
 - Prior FCA Cases Arising from Cybersecurity Violations
- Recent Lessons from Other Recent Enforcement Actions
- Next Steps





Overview of the Cybersecurity Landscape

Morgan Lewis

Cyber Risks and Landscape

- Phishing Schemes
- Business Email Compromise
- Ransomware
- Targeted cyber attacks
- Insider threat
- Third Party Vendors
- Stolen unencrypted laptop

Key Actors

Organized Cyber Crime

State Sponsored

Hackers for Hire

Hactivists

Third Party Vendor Attacks

Insider Threat

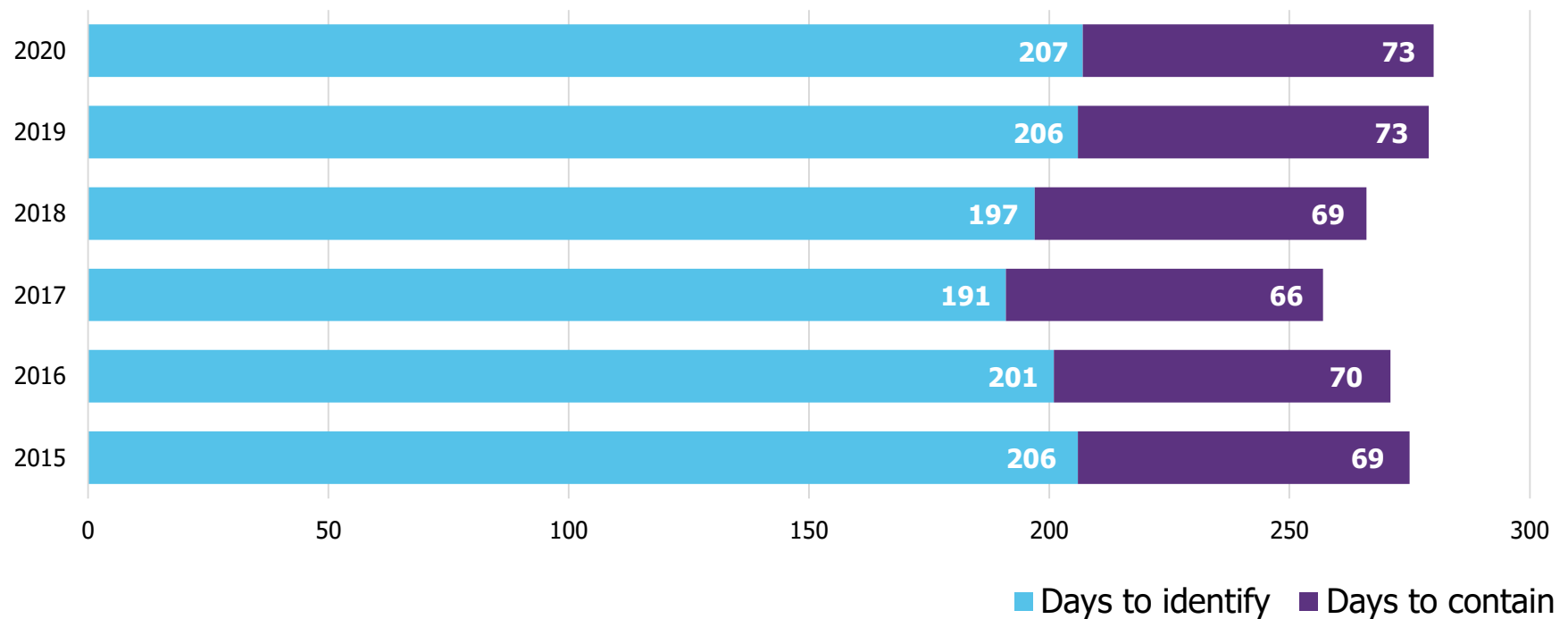
Inadvertence

Initial Questions

- What cyber incidents are you likely to encounter?
 - Based on risk assessment
- What is the average time to identify a data breach?
- How long to contain a data breach?
- Consider past incidents:
 - When and how was the incident detected?
 - What was determined about when the attack was first initiated?



Average Time to Identify and Contain a Data Breach

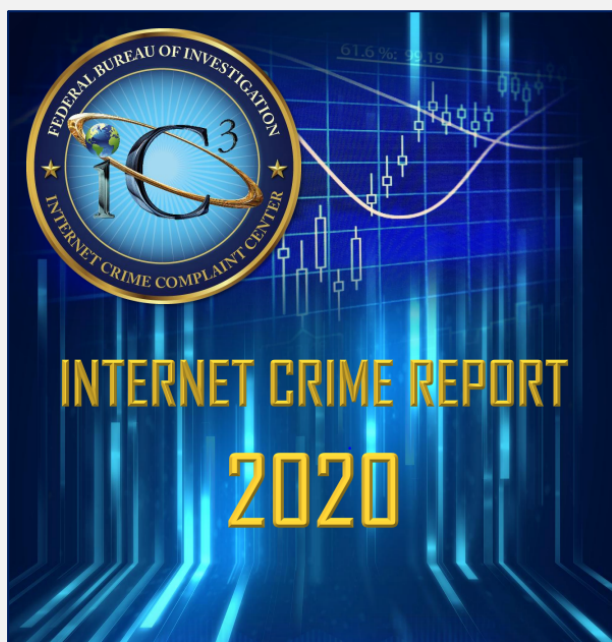


IBM Security | Cost of a Data Breach Report 2020

Morgan Lewis





Record Criminal Cyber Complaints



Last Report Issued: March 17, 2021

- “IC3 received a record number of complaints from the American public in 2020: 791,790, with reported losses exceeding **\$4.1 billion.**”
- “This represents a **69% increase** in total complaints from 2019.”
 - **Business E-mail Compromise (BEC)** schemes costliest: 19,369 complaints with an adjusted loss of approximately **\$1.8 billion.**
 - **Phishing** scams prominent: 241,342 complaints, with adjusted losses of over \$54 million.
 - **Ransomware** incidents also continues to rise, with 2,474 incidents reported in 2020.

Business Email Compromise Schemes



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

September 10, 2019

Alert Number
I-091019-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

Business Email Compromise The \$26 Billion Scam

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA 1-071218-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to July 2019.

DEFINITION

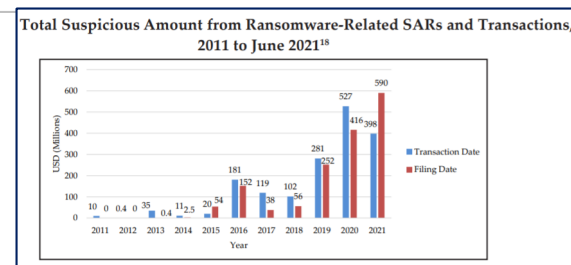
Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when a subject compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

The scam is not always associated with a transfer-of-funds request. One variation involves compromising legitimate business email accounts and requesting employees' Personally Identifiable Information or Wage and Tax Statement (W-2) forms.¹

Ransomware Trends

- “The total value of suspicious activity reported in ransomware-related SARs during the **first six months** of 2021 was **\$590 million**, which exceeds the value reported for the entirety of 2020 (\$416 million).”
- “FinCEN identified several money laundering typologies common among ransomware variants in 2021 including threat actors increasingly requesting payments in **Anonymity-enhanced Cryptocurrencies (AECs)** and avoiding reusing wallet addresses, “chain hopping” and cashing out at centralized exchanges, and using mixing services and decentralized exchanges to convert proceeds.”



Ransomware Payments Statement



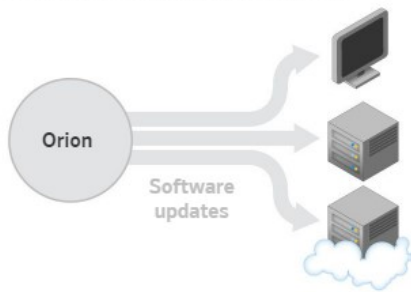
Information Requested

The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, or fund illicit activities. Paying the ransom also does not guarantee a victim's files will be recovered. However, the FBI understands when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. Regardless of whether you or your organization decides to pay the ransom, the FBI urges you to report ransomware incidents to your local field office. Doing so provides investigators and analysts with the critical information they need to track ransomware attackers, hold them accountable under US law, and prevent future attacks.

SolarWinds – Supply Chain Attack – Inside the Hack

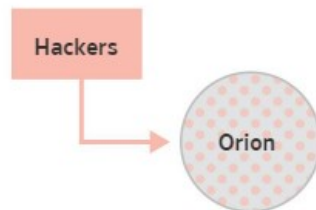
1

SolarWinds makes network management software, called Orion, that's widely used by government agencies and Fortune 500 companies. Like most software makers, they push regular updates to their customers.



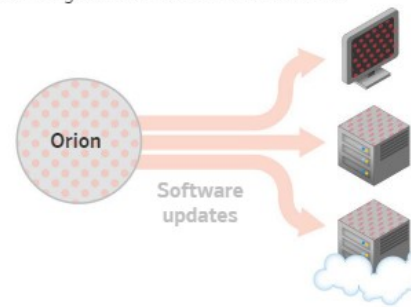
2

Hackers compromised SolarWinds and inserted their own malicious software in updates the company distributed between March and June of this year.



3

About 18,000 customers downloaded these updates, which acted like Trojan Horses, awaiting instructions from the hackers



4

For some percentage of these customers, the instructions came, and the SolarWinds computer downloaded more code, giving hackers a way to sneak around the network and steal data. They were able to access emails, download software and perform reconnaissance on the network.





Photographer: Samuel Corum/Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

- “Hackers gained entry into the networks of Colonial Pipeline Co. on April 29 through a **virtual private network account**, which allowed employees to remotely access the company’s computer network.... The account was **no longer in use at the time of the attack** but could still be used to access Colonial’s network....”



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

Colonial CEO Defends \$4.4M Ransomware Payment

By Ben Kochman

Law360 (June 8, 2021, 5:06 PM EDT) -- At a U.S. Senate hearing Tuesday, the head of Colonial Pipeline Co. defended the company's recent \$4.4 million ransomware payment, while acknowledging that the attackers cracked a key password that was not protected by a basic security practice.

"I know how critical the pipeline is to our country, and I put the country first," Colonial CEO Joseph Blount told the Senate Committee on Homeland Security and Governmental Affairs of the ransom payment, a month after Colonial **shut down a 5,500-mile pipeline** that supplies nearly half the gasoline, diesel and jet fuel used on the U.S. East Coast.

During questioning, Blount called the choice to pay 75 bitcoins to a Russia-based criminal gang in exchange for a decryption key that sped up its recovery from the attack the "hardest decision" he had made in nearly 40 years in the energy industry.

"Considering the consequences of potentially not being able to bring the pipeline online as quickly as I possibly could, I chose the option to make the ransom payment," Blount told lawmakers. He added that "it was our understanding that the decision was solely ours to make as a private company," even after speaking with investigators at the FBI, whose **official guidance** cautions ransomware victims against making payments, in part because paying criminals emboldens perpetrators of future attacks.

EQUIFAX PERSONAL BUSINESS GOVERNMENT ABOUT US ▾ Support  

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

Equifax Announces Cybersecurity Incident Involving Consumer Information

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

Sep 07, 2017

BUSINESS NEWS
OCTOBER 2, 2017 7:52 AM

Equifax failed to patch security vulnerability in March: former CEO

By David Shephardson
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 was alerted to the breach by the U.S. Homeland Security Department on March 9, Smith said in the testimony, but it was not patched.

On March 15, Equifax’s information security department ran scans that should have identified any systems that were vulnerable to the software issue but did not, the testimony said.

As a result, “the vulnerability remained in an Equifax web application much longer than it should have,” Smith said. “It was this unpatched vulnerability that allowed hackers to access personal identifying information.”

In his testimony, Smith said it appears the first date hackers accessed sensitive information may have been on May 13. He said “between May 13 and July 30, there is evidence to suggest that the attacker(s) continued to access sensitive information.”

2020 Cost of Data Breach Report

Key findings:

\$7.13 million

The average cost of a data breach in the healthcare industry, an increase of 10% compared to the 2019 study

80%

Share of breaches that included records containing customer PII, at an average cost of \$150 per record

\$5.52 million

Average total cost of a breach at enterprises of more than 25,000 employees, compared to \$2.64 million for organizations under 500 employees

\$291,870

Increase to the average total cost of a data breach associated with complex security systems

51%

Share of organizations with cyber insurance that used claims to cover the cost of consulting and legal services

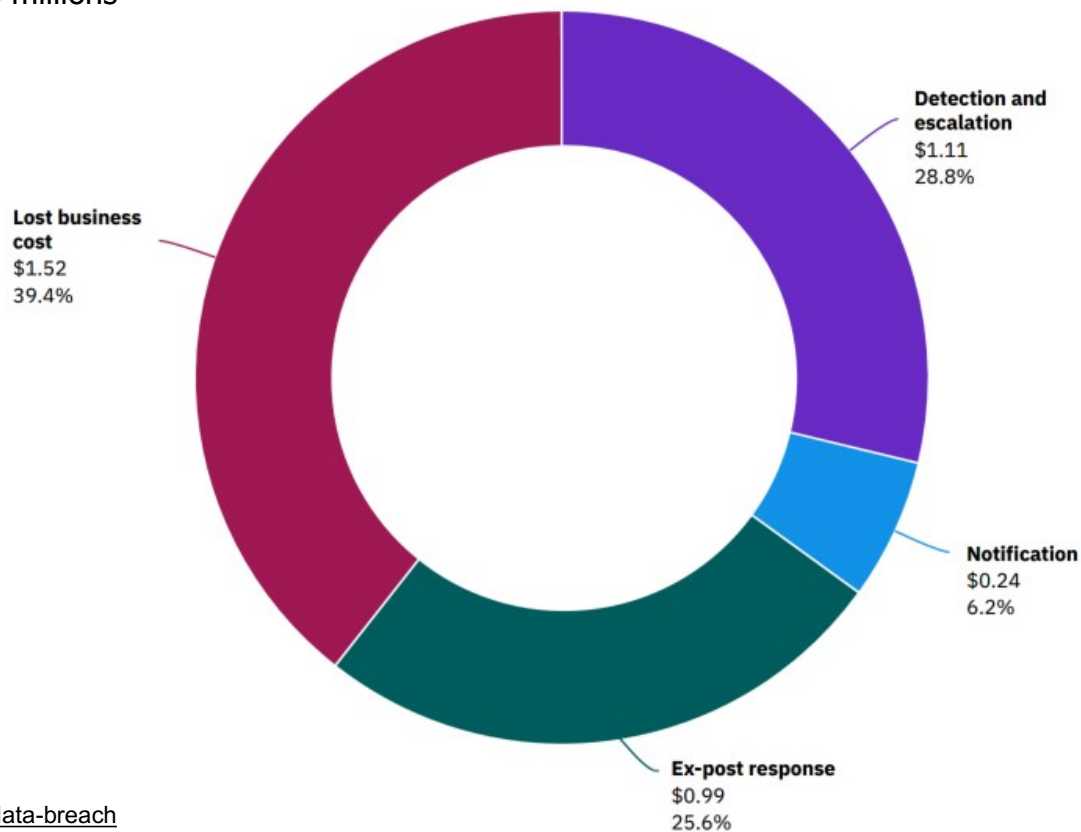
46%

Share of respondents who said the CISO is most responsible for the data breach

Data breach average total cost

Divided into four categories, measured in US\$ millions

Lost business costs comprised the largest share of the average cost of a data breach.





Common Government Contract Cyber Scenarios and Risks

Morgan Lewis

Common Cyber Scenarios



ABC COMPANY

**PROPOSAL IN RESPONSE TO
SOLICITATION NO. 21-00001**

**FOR INFORMATION MANAGEMENT AND
WEB-BASED SERVICES**

Submitted to U.S. DEPARTMENT OF HOMELAND
SECURITY

November 11, 2021

Confidential

4.0 CYBERSECURITY CAPABILITIES AND
CERTIFICATIONS



Common Issues Arising Under Cyber Investigations

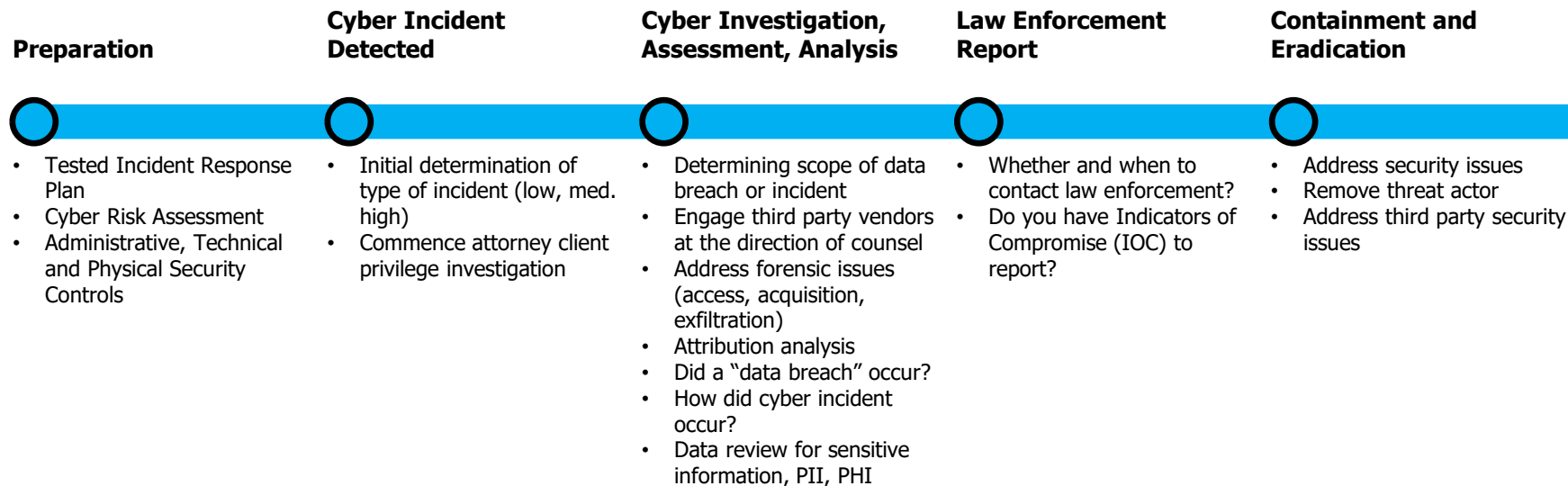
Morgan Lewis

Incident Response Timeline Key Phases

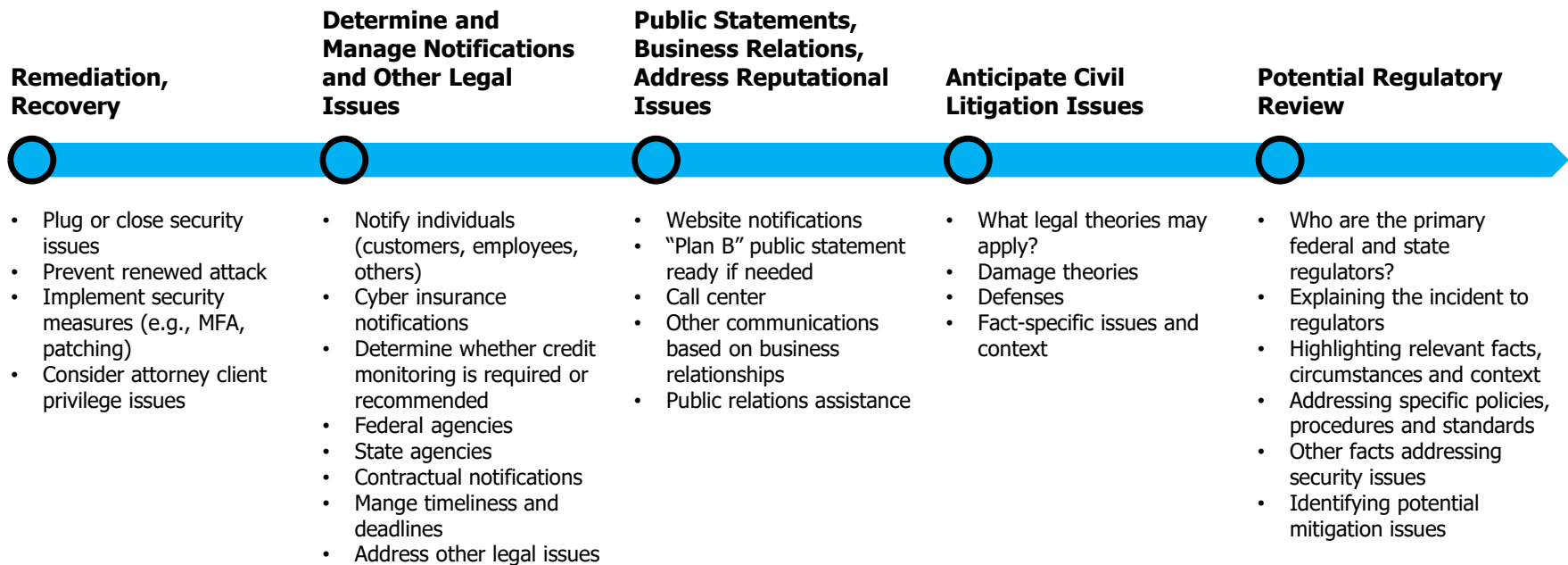
- a. Preparation
- b. Cyber Incident Detected
- c. Cyber Investigation, Assessment, Analysis
- d. Law Enforcement Report?
- e. Containment and Eradication
- f. Remediation, Recovery
- g. Determine and Manage Notifications and Other Legal Issues
- h. Public Statements, Business Relations, Address Reputational Issues
- i. Anticipated Civil Litigation Issues
- j. Potential Regulatory Review



Incident Response Timeline Key Phases



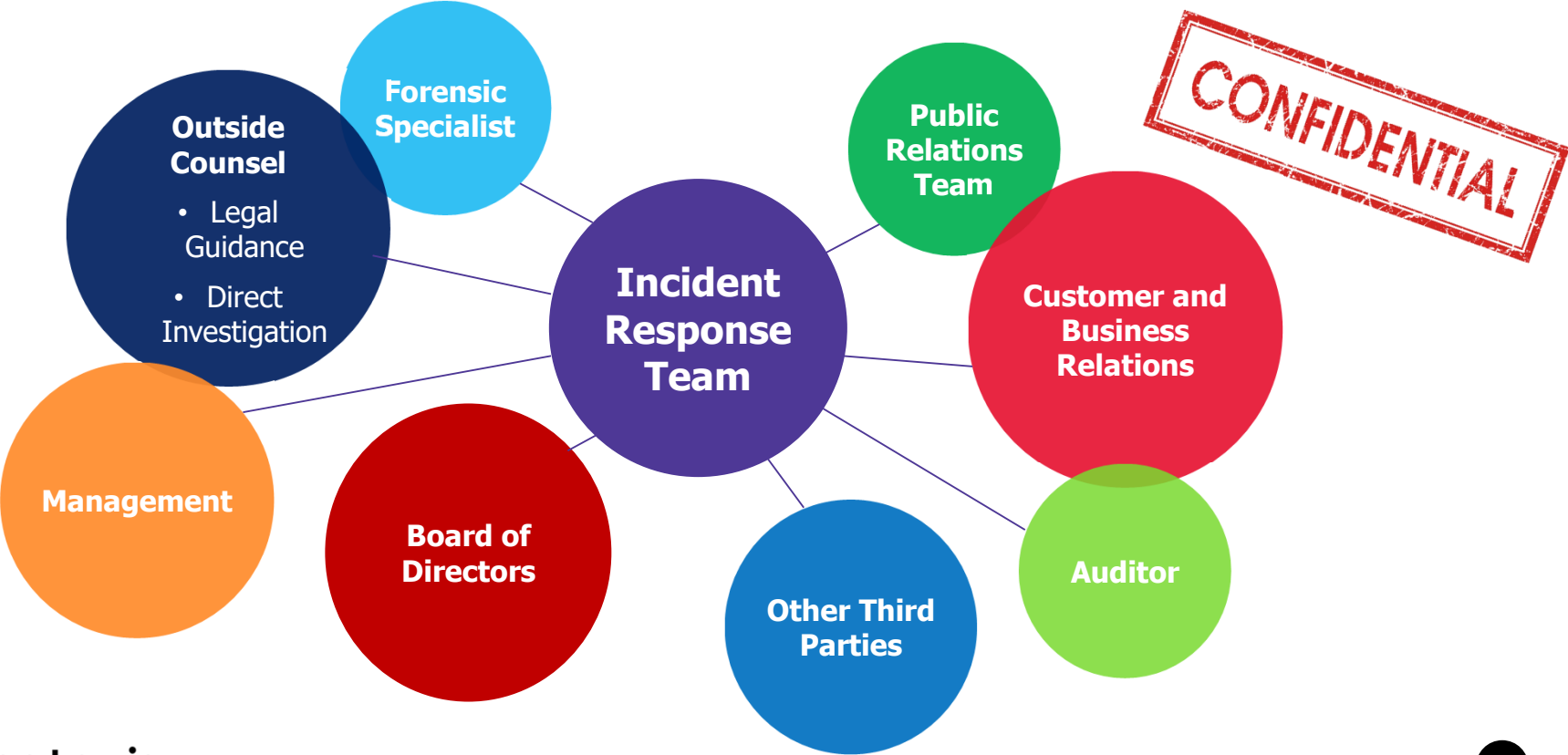
Incident Response Timeline Key Phases



Has a “Breach” Occurred?

Standard	State Examples
Unauthorized Acquisition of Personal Information	Alabama, Alaska, Arkansas, California, Colorado, Delaware, District of Columbia, Idaho, Iowa, Missouri, Montana, Nevada, North Carolina, Oregon, Tennessee, Wisconsin, Wyoming
Unauthorized Access to Personal Information	Florida
Unauthorized Acquisition of and Access to Personal Information	Arizona, Hawaii, Louisiana, Missouri, New York, North Carolina, Ohio, Pennsylvania
Unauthorized Acquisition or Use	Massachusetts
Materiality	Arizona, Idaho, Pennsylvania, Montana, Nevada, Tennessee, Wyoming

Consider Range of Incident Communications



Legal Protections

- **Attorney Client Privilege**

- The attorney-client privilege “purpose is to encourage full and frank communication 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 US 383, 389 (1981).

- **Work Product 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.”

Capital One Case (May 26, 2020)



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.

Morgan Lewis

<https://www.law360.com/articles/1276981/print?section=banking>
<https://www.law360.com/articles/1274115/print?section=banking>

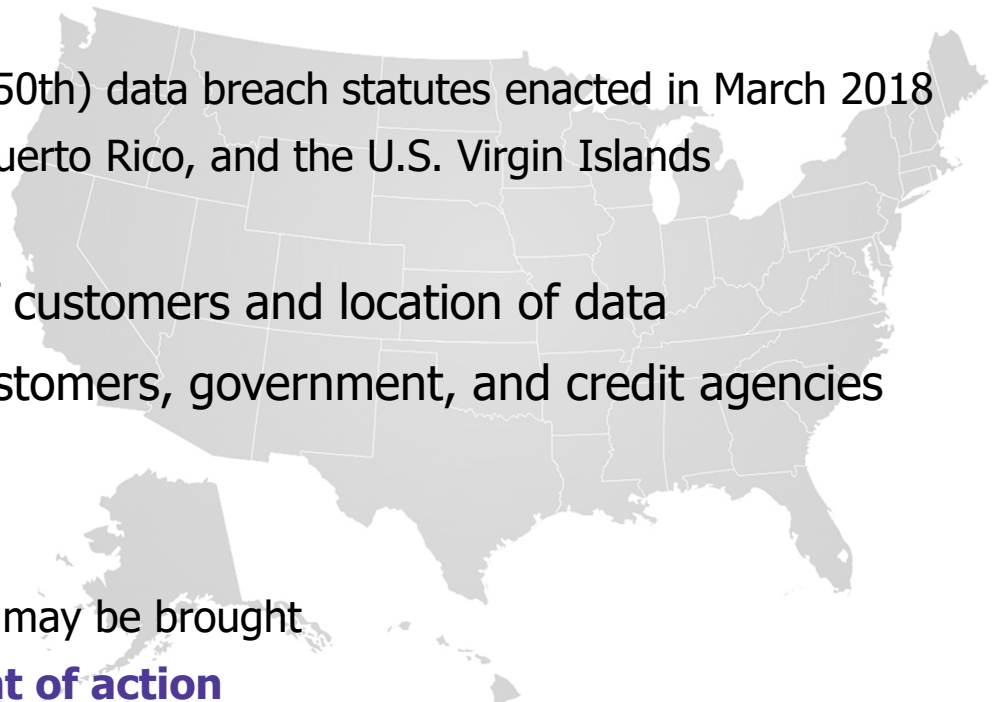
27

State Data Breach Notification Laws

- **54 US Jurisdictions**

- South Dakota (49th) and Alabama (50th) data breach statutes enacted in March 2018
- Also: District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands

- State law depends on residency of customers and location of data
- Notification may be required to customers, government, and credit agencies
- Enforcement and Actions
 - Separate **AG enforcement action** may be brought
 - Some States provide a **private right of action**





SEC Guidance on Cybersecurity Disclosures

- **Feb. 21, 2018**
- Disclosures Based on Reporting Obligations
 - Management’s Discussion and Analysis of Financial Condition and Results of Operations
 - Cybersecurity Risk Factors
- Materiality Standard
- Timing of Disclosures
- Board Role
 - Managing Cyber Risk
- Cybersecurity Policies and Procedures
- Insider Trading Policies and Procedures Related to Cyber Risks and Incidents

Press Release

SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures

FOR IMMEDIATE RELEASE
2018-22

Washington D.C., Feb. 21, 2018 — Yesterday, the Securities and Exchange Commission voted unanimously to approve a statement and interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.

“I believe that providing the Commission’s views on these matters will promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors,” said SEC Chairman Jay Clayton. “In particular, I urge public companies to examine their controls and procedures, with not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives.”

The guidance provides the Commission’s views about public companies’ disclosure obligations under existing law with respect to matters involving cybersecurity risk and incidents. It also addresses the importance of cybersecurity policies and procedures and the application of disclosure controls and procedures, insider trading prohibitions, and Regulation FD and selective



DOD Cybersecurity Maturity Model Certification

U.S. Department of Defense

News ▾ Spotlights ▾ About ▾

NEWS

DOD to Require Cybersecurity Certification in Some Contract Bids

JAN. 31, 2020 BY C. TODD LOPEZ, DOD NEWS

f t

By the end of September, the Defense Department will require at least some companies bidding on defense contracts to certify that they meet at least a basic level of cybersecurity standards when responding to a request for proposals.



DOD Enhanced "CMMC 2.0" Program

U.S. Department of Defense

News ▾ Spotlight

Release

IMMEDIATE RELEASE

Strategic Direction for Cybersecurity Maturity Model Certification (CMMC) Program

NOV. 4, 2021

[f](#) [t](#)

Today, the Department of Defense announced the strategic direction of the Cybersecurity Maturity Model Certification (CMMC) program, marking the completion of an internal program assessment led by senior leaders across the Department.

U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) Advisory



- U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities (“persons”) on OFAC’s **Specially Designated Nationals and Blocked Persons List (SDN List)**, other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria).”
- “OFAC may impose civil penalties for sanctions violations based on **strict liability**, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.”

The image shows two overlapping screenshots of OFAC advisories. The top screenshot is titled "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments¹" and is dated October 1, 2020. It features the OFAC logo and the text: "The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. Demand for ransomware payments has increased during the COVID-19 pandemic." The bottom screenshot is titled "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments¹" and is dated September 21, 2021. It also features the OFAC logo and the text: "The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be 'mitigating factors' in any related enforcement action.²"



New Civil Cyber-Fraud Initiative

Morgan Lewis

Cybersecurity Focus



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify,

DOJ Cybersecurity Review May 2021

PowerPost • Analysis

The Cybersecurity 202: The Justice Department launched a 120-day review into its cybersecurity strategy



By [Tonya Riley](#)

Technology and cybersecurity policy researcher

May 3, 2021 at 7:12 a.m. EDT

with Aaron Schaffer



Morgan Lewis

<https://www.washingtonpost.com/politics/2021/05/03/cybersecurity-202-justice-department-launched-120-day-review-into-its-cybersecurity-strategy/>

New Civil Cyber-Fraud Initiative: October 6, 2021



- “The initiative will hold accountable entities or individuals that put U.S. information or systems at risk by **[a]** knowingly providing deficient cybersecurity products or services, **[b]** knowingly misrepresenting their cybersecurity practices or protocols, or **[c]** knowingly violating obligations to monitor and report cybersecurity incidents and breaches.”

JUSTICE NEWS

Department of Justice
Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, October 6, 2021

Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative

Deputy Attorney General Lisa O. Monaco announced today the launch of the department’s Civil Cyber-Fraud Initiative, which will combine the department’s expertise in civil fraud enforcement, government procurement and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems.

“For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it,” said Deputy Attorney General Monaco. “Well that changes today. We are announcing today that we will use our civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards — because we know that puts all of us at risk. This is a tool that we have to ensure that taxpayer dollars are used appropriately and guard the public fisc and public trust.”

The creation of the Initiative, which will be led by the Civil Division’s Commercial Litigation Branch, Fraud Section, is a direct result of the department’s ongoing comprehensive cyber review, ordered by Deputy Attorney General Monaco this past May. The review is aimed at developing actionable recommendations to enhance and expand the Justice Department’s efforts against cyber threats.



New Civil Cyber-Fraud Initiative

“At bottom, the department’s Civil Cyber-Fraud Initiative will hold accountable entities or individuals that put U.S. information or systems at risk.”

JUSTICE NEWS

Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Cybersecurity and Infrastructure Security Agency (CISA) Fourth Annual National Cybersecurity Summit

Washington, DC ~ Wednesday, October 13, 2021

Remarks as Delivered

Good afternoon. My name is Brian Boynton and I am the Acting Assistant Attorney General for the Civil Division at the Department of Justice.

It is a pleasure to speak with you today. I am grateful to our partners at CISA for hosting this conference, and giving us the opportunity to share our thoughts on fighting the ever-evolving cyber threat.

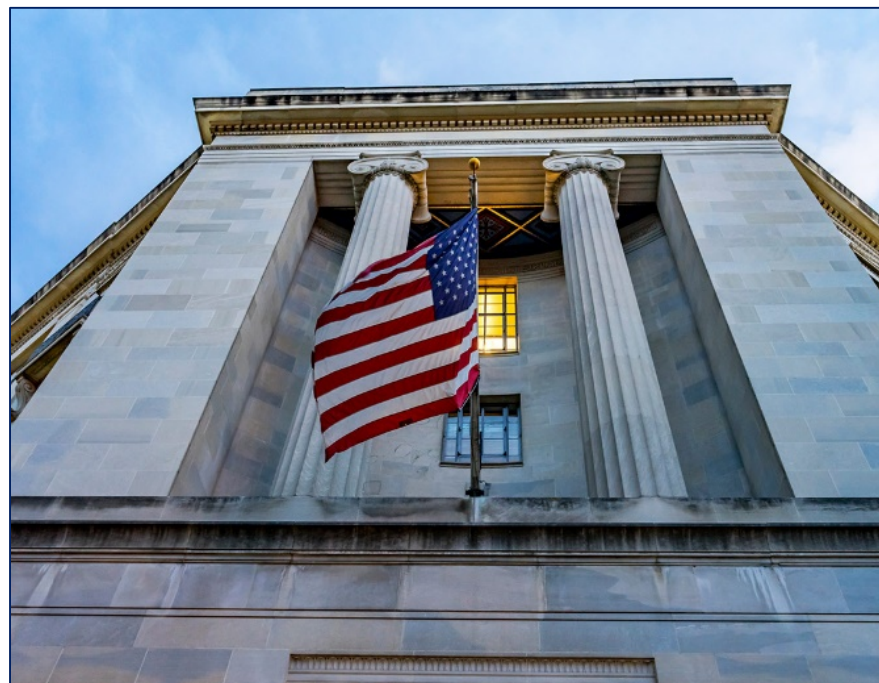
Today, I want to talk about the Justice Department’s newly announced Civil Cyber-Fraud Initiative. This initiative will combine the department’s expertise in civil fraud enforcement, government procurement and cybersecurity to promote the critical mission of combating new and emerging cyber-threats.

The Civil Cyber-Fraud Initiative arises out of the cyber review ordered by the Deputy Attorney General this past May. The purpose of the review is to develop recommendations to enhance and expand the department’s efforts against cyber threats.



DOJ Initiative Key Areas of Focus

- Knowing:
 - “failures to comply with cybersecurity standards”
 - “misrepresentation of security controls and practices”
 - “failure to timely report suspected breaches”





How DOJ and Qui Tam Relators may use the False Claims Act

Morgan Lewis

False Claims Act Overview

- Civil False Claims Act, 31 U.S.C. §§ 3729-3733
 - “Lincoln’s Law”
 - Revived through amendments in 1986
- Other Key Amendments
 - Fraud Enforcement and Recovery Act of 2009 (“FERA”)
 - Affordable Care Act (“ACA”) and Dodd-Frank Act
- State and Municipal False Claims Acts

False Claims Act Liability

Commonly Invoked Sources of Substantive Liability

- § 3729(a)(1)(A): “direct” false claims for payment or approval
- § 3729(a)(1)(B): false records/statements to support a false claim
- § 3729(a)(1)(C): conspiracy to commit violations of (a)(1)(A)-(G)
- § 3729(a)(1)(G): “reverse” false claim provision

False Claims Act Liability

Key Elements of FCA Claims

- Falsity
- Scienter
 - “Knowingly” standard
- Materiality
- Causation

False Claims Act Liability

Substantive Claims: Potential Consequences

- Damages and Penalties Exposure
 - Treble damages
 - Per claim penalties
- Related Concerns
 - Debarment or suspension
 - Program exclusion or corporate integrity agreement (“CIA”)

False Claims Act Liability

Substantive Defenses

- Materiality
 - Conduct by the government after it learns of the allegations
- Ambiguity
 - Is the statute/contract/regulation clear? Subject to reasonable alternative interpretations? Is there authoritative agency guidance?
- Intent
 - Even with lower scienter standard, FCA does not reach mistakes or mere negligence



FCA Cases – DOJ Statistics*

- 672 *qui tam* suits filed in FY2020; 250 Affirmative FCA suits
- Of the \$2.23B recovered in FY2020, \$1.68B related to *qui tam* suits
- In FY2020, the government paid out \$309M to *qui tam* relators

* Excludes State FCA enforcement

Department of Justice
Office of Public Affairs

FOR IMMEDIATE RELEASE Thursday, January 14, 2021

Justice Department Recovers Over \$2.2 Billion from False Claims Act Cases in Fiscal Year 2020

The Department of Justice obtained more than \$2.2 billion in settlements and judgments from civil cases involving fraud and false claims against the government in the fiscal year ending Sept. 30, 2020, Acting Assistant Attorney General Jeffrey Bossert Clark of the Department of Justice's Civil Division announced today. Recoveries since 1986, when Congress substantially strengthened the civil False Claims Act, now total more than \$64 billion.

"Even in the face of a nationwide pandemic, the department's dedicated employees continued to investigate and litigate cases involving fraud against the government and to ensure that citizens' tax dollars are protected from abuse and are used for their intended purposes," said Acting Assistant Attorney General Clark. "The continued success of the department's False Claims Act enforcement efforts are a testament to the dedication of the civil servants who pursue these important cases as well as to the fortitude of whistleblowers who report fraud."

Of the more than \$2.2 billion in settlements and judgments recovered by the Department of Justice this past fiscal year, over \$1.8 billion relates to matters that involved the health care industry, including drug and medical device manufacturers, managed care providers, hospitals, pharmacies, hospice organizations, laboratories, and physicians. The amounts included in the \$1.8 billion reflect only federal losses, and, in many of these cases, the department was instrumental in recovering additional tens of millions of dollars for state Medicaid programs.

Qui Tam Provisions

Unique Features

- Specific relator filing/seal requirements
- Investigation timing and tools
 - IG Subpoenas, CIDs
- DOJ options
 - Declination, intervention, dismissal

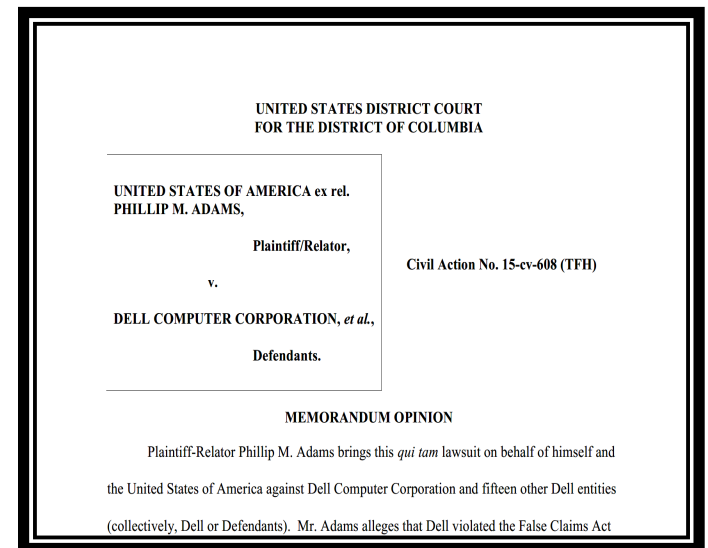
Qui Tam Provisions

Whistleblower Retaliation: 31 U.S.C. § 3730(h)

- Essentially a personal employment claim
- Different than substantive FCA claims
 - SOL
 - Sealing
 - Relief/damages

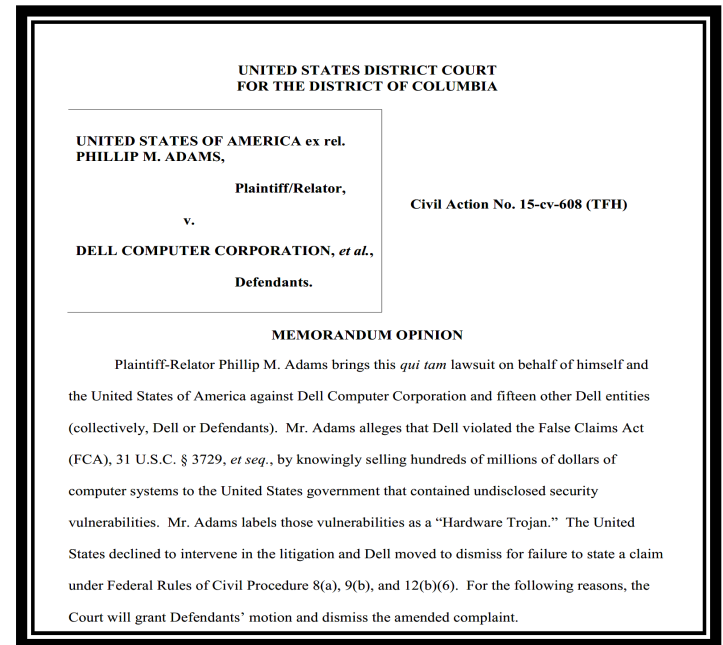
FCA Cases Arising from Cybersecurity Violations

- **U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.**, 381 F. Supp. 3d 1240 (E.D. Cal. 2019)
 - Declined *qui tam* and 3730(h) case alleging noncompliance with contractual cybersecurity requirements
 - Relator was insider - former Senior Director of Cyber Compliance/Controls
 - Alleged fraudulent inducement and non-compliance with standards
 - Court allowed some FCA claims to survive motion to dismiss



FCA Cases Arising from Cybersecurity Violations

- **U.S. ex rel. Adams v. Dell Computer**, No. 15-cv-608 (D.D.C. 2020)
 - Declined qui tam case alleging sale of computer products with undisclosed cybersecurity hardware vulnerabilities
 - Relator was self-identified expert but not an insider
 - Alleged false claims/statements and false certifications related to compliance with contract and certain DoD regulations
 - Materiality based on allegations that government agencies are obliged to ensure technology acquisitions comply with security requirements
 - Motion to dismiss granted because of insufficient allegations to satisfy demanding materiality standard and “knowing” conduct



FCA Cases Arising from Cybersecurity Violations

- **U.S. ex rel. Glenn v. Cisco Systems**, No. 1:11-cv-00400 (W.D. NY 2019)
 - Qui tam case alleging product did not comply with security requirements
 - Settled for \$8.6 million (Relator received \$1.7 million)



Expected Focus of FCA Cyber – Enforcement Efforts

- Non-compliance with cybersecurity standards on goods and services provided by federal contractors
 - Failure to adhere to specific contractual requirements
 - Failure to protect government data and unauthorized access
- Misrepresentation of security controls and practices.
 - False representations regarding System Security Plans and security controls
 - Misrepresentations in the bidding process – fraudulent inducement
 - Misrepresentations re periodic reporting
 - Failure to disclose violations
- Failure to report suspected breaches of cybersecurity protocols
- These are in addition to other potential remedies – e.g., SEC, HIPAA

FCA Liability in Cyber Cases

- False statements of capabilities in proposal leading to contract award that company was not eligible to receive
- False certifications of compliance (express or implied) in invoices/claims for payment to federal/state agencies
- False claims for payment for services not provided
 - Data protection
 - MFA and Password protection services
- Conspiracy
- Company and individual accountability

FCA Damages in Cyber Cases

- Benefit of the bargain damages where product does not meet contractual standards
- Fraud in the inducement damages where misrepresentations made in the proposal and contractor otherwise not eligible for award
- Nature of the false statement – potentially placing government systems or data at risk – could impact damages/penalties assessments
- Mandatory trebling of single damages
- Statutory penalties for each false claim

Hypothetical Scenario

- RFP requires verification of compliance with certain cybersecurity protocols
- Bid team plans to put protocols in place post-award but falsely certifies pre-award compliance
- Implementation delays post-award (80% compliance) with requisite controls
- Continued billing while team works to comply
- No disclosure to agency
- Team member reports non-compliance to Company hotline

Increased Relator Activity

- DOJ Initiative likely to encourage relators and relators' counsel
 - Dedicated team within Civil Frauds will be receptive audience
- Potential “insider” relators may have increased access to company systems
- Expect qui tam relators to include business competitors

Increased Affirmative Enforcement

- DOJ can and likely will bring affirmative FCA suits
- Investigations in this space – based on referrals from agencies and even voluntary disclosures – likely will be swift and intensive
- Cooperation and transparency will be important considerations

Mitigating FCA Risk

- Developing effective compliance program
- Ongoing monitoring and training
- FAR Mandatory Disclosure
 - FAR 52.203-13
- Elevating potential non-compliance followed by prompt investigations to determine facts and assess risk/disclosure obligations

Mitigating FCA Risk

- Employee engagement
- Documenting compliance
- Tracking updated standards and regulations
- Documenting and managing agency communications re changes to SSPs
- Subpoena / CID compliance



Lessons from Other Enforcement Initiatives

Morgan Lewis

Special Inspector General for Pandemic Recovery (SIGPR)



Whistleblower Reprisal Complaint Form

You may use this form to submit your complaint via email to whistleblower@sigpr.gov. Please use this form only to file complaints of **Whistleblower Reprisal**. If your complaint does not meet the requirements for whistleblower reprisal, please file your complaint as a fraud, waste, or abuse complaint with the **SIGPR hotline**.

If your complaint alleges reprisal due to race, color, sex, national origin, religion, disability, or genetic information, or you feel you have been retaliated against for filing an earlier complaint with EEO, **then please file your complaint with your EEO office or the Equal Employment Opportunity Commission, not SIGPR.**

PART I - Your Information

*CHOOSE ONE OF THE FOLLOWING THREE OPTIONS

Please keep in mind that your decision to elect anonymity or confidentiality may limit SIGPR's ability to conduct a complete investigation or take further action if warranted.

- I wish to remain anonymous** (If you select this option, do not identify yourself below)
- Keep my identity confidential** (Provide contact information below in the event we need additional information)
- I waive confidentiality** (My name may be released to another entity or OIG if determined not to be within SIGPR jurisdiction or during the course of an investigation, audit or other official action.)

Morgan Lewis

Special Inspector General for Pandemic Recovery

Call the Hotline +1 (202) 927-7899

REPORT FRAUD, WASTE & ABUSE | WHISTLEBLOWER PROTECTION | REPORTS | NEWS | ABOUT SIGPR | CONTACT | SEARCH

Welcome to SIGPR's website.

The Coronavirus Aid, Relief, and Economic Security (CARES) Act established the Special Inspector General for Pandemic Recovery (SIGPR) to provide CARES Act oversight.

[Learn more](#)

“SIGPR is an independent organization within the U.S. Department of the Treasury whose mission is to promote the economy, efficiency, effectiveness, and integrity of CARES Act funds and programs. SIGPR was established by Section 4018 of the CARES Act with duties, responsibilities, and authority under the Inspector General Act of 1978.”

<https://www.sigpr.gov/>

Antitrust Division Procurement Collusion Strike Force

DOJ Announcement: November 5, 2019

- “Lead a coordinated national response to combat antitrust crimes and related schemes in government procurement, grant, and program funding at all levels of government.”
- Innovative “district-based task organization model” that partners with US Attorney offices and other agencies
- Targeted outreach training and education at federal, state and local public procurement process
- Use of criminal and civil enforcement tools



Lessons from Other Enforcement Initiatives

- **Cyber Enforcement by Other Federal, State Agencies**

- Timeliness of notification
- Misleading statements





Timeliness of Notification

- Commission Statement and Guidance on Public Company Cybersecurity Disclosures
- “Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents **in a timely fashion**, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack.”

Morgan Lewis

Press Release

SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures

FOR IMMEDIATE RELEASE
2018-22

Washington D.C., Feb. 21, 2018 — Yesterday, the Securities and Exchange Commission voted unanimously to approve a statement and interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.

“I believe that providing the Commission’s views on these matters will promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors,” said SEC Chairman Jay Clayton. “In particular, I urge public companies to examine their controls and procedures, with not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives.”

The guidance provides the Commission’s views about public companies’ disclosure obligations under existing law with respect to matters involving cybersecurity risk and incidents. It also addresses the importance of cybersecurity policies and procedures and the application of disclosure controls and procedures, insider trading prohibitions, and Regulation FD and selective

<https://www.sec.gov/news/press-release/2018-71>

63




Notification Enforcement

FOR IMMEDIATE RELEASE

January 9, 2017

Contact: HHS Press Office

202-690-6343 

media@hhs.gov

First HIPAA enforcement action for lack of timely breach notification settles for \$475,000

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR), has announced the first Health Insurance Portability and Accountability Act (HIPAA) settlement based on the **untimely reporting of a breach** of unsecured protected health information (PHI). Presence Health has agreed to settle potential violations of the HIPAA Breach Notification Rule by paying \$475,000 and implementing a corrective action plan. Presence Health is one of the largest health care networks serving Illinois and consists of approximately 150 locations, including 11 hospitals and 27 long-term care and senior living facilities. Presence also has multiple physicians' offices and health care centers in its system and offers home care, hospice care, and behavioral health services. With this settlement amount, OCR balanced the need to emphasize the importance of timely breach reporting with the desire not to disincentive breach reporting altogether.

Notification Enforcement

- **Oct. 31, 2017**
- NY and VT Attorneys General
 - VT: **\$300,000**
 - NY: **\$400,000**
- Failure to provide timely notice and maintain reasonable data security
 - **287 days** after aware of first incident
 - **100 days** after aware of second incident
- Two separate incidents in 2014 and 2015
 - 350,000 credit card numbers



STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

2017 OCT 31 A 9:51
CIVIL DIVISION
Docket No. *683-19-17 AW*

IN RE: HILTON DOMESTIC
OPERATING COMPANY INC.)
)
)

ASSURANCE OF DISCONTINUANCE

This Assurance of Discontinuance ("Assurance") is entered into between the State of Vermont ("State"), and Respondent Hilton Domestic Operating Company Inc., as successor in interest to Park Hotels & Resorts Inc. f/k/a Hilton Worldwide, Inc., including all of its subsidiaries, affiliates, successors, and assigns ("Hilton" or "Respondent," and, together with the State, the "Parties"). This Assurance applies only to Hilton owned or managed properties and does not apply to franchise properties, where Hilton does not maintain a majority interest.

This Assurance resolves the State of Vermont's concerns regarding Hilton's compliance with the Vermont Security Breach Notice Act, 9 V.S.A. §§ 2430-35 and Consumer Protection Act, 9 V.S.A. Chapter 63.

I. PARTIES

1. The State is acting through its Attorney General with its office located at 109 State Street, Montpelier, Vermont, 05609.
2. Respondent Hilton is one of the largest hospitality companies in the world.

In Re Hilton Domestic Operating Company, Inc.



Enforcement Action on Timeliness of Notification

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.

According to the SEC's order, within days of the December 2014 intrusion, Yahoo's information security team learned that Russian hackers had stolen what the security team referred to internally as the company's "crown jewels": usernames, email addresses, phone numbers, birthdates, encrypted passwords, and security questions and answers for hundreds of millions of user accounts. Although information relating to the breach was reported to members of Yahoo's senior management and legal department, Yahoo failed to properly investigate the circumstances of the breach and to adequately consider whether the breach needed to be disclosed to investors. The fact of the breach was not disclosed to the investing public until more than two years later, when in 2016 Yahoo was in the process of closing the acquisition of its operating business by Verizon

- **Fine: \$35 million;** SEC Order (April 24, 2019)
- **Failure to Disclose:** "Despite its knowledge of the 2014 data breach, Yahoo **did not disclose the data breach in its public filings for nearly two years.**"
 - 2014 data breach disclosed in September 2016 in a press release attachment to a Form 8-K.
- **Misleading Disclosures:** Risk factor disclosures in annual and quarterly reports (2014 through 2016) "were materially misleading" by claiming "the risk of potential future data breaches . . . without disclosing that a massive data breach had in fact already occurred."
- **Stock Purchase Agreement:** "Affirmative representations denying the existence of any significant data breaches in a July 23, 2016 stock purchase agreement with Verizon."
- Ongoing cooperation



Enforcement Action Misleading Statements

- “[M]isleading language suggesting that the notifications were issued much sooner than they actually were after discovery of the incidents”

Press Release

SEC Announces Three Actions Charging Deficient Cybersecurity Procedures

FOR IMMEDIATE RELEASE
2021-169

Washington D.C., Aug. 30, 2021 — The Securities and Exchange Commission today sanctioned eight firms in three actions for failures in their cybersecurity policies and procedures that resulted in email account takeovers exposing the personal information of thousands of customers and clients at each firm. The eight firms, which have agreed to settle the charges, are: Cetera Advisor Networks LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC, Cetera Advisors LLC, and Cetera Investment Advisers LLC (collectively, the Cetera Entities); Cambridge Investment Research Inc. and Cambridge Investment Research Advisors Inc. (collectively, Cambridge); and KMS Financial Services Inc. (KMS). All were Commission-registered as broker dealers, investment advisory firms, or both.

According to the SEC's order against the Cetera Entities, between November 2017 and June 2020, cloud-based email accounts of over 60 Cetera Entities' personnel were taken over by unauthorized third parties, resulting in the exposure of personally identifying information (PII) of at least 4,388 customers and clients. None of the taken over accounts were protected in a manner consistent with the Cetera Entities' policies. The SEC's order also finds that Cetera Advisors LLC and Cetera Investment Advisers LLC sent breach notifications to the firms' clients that included misleading language suggesting that the notifications were issued much sooner than they actually were after discovery of the incidents.

<https://www.sec.gov/news/press-release/2021-169>



Enforcement Action Misleading Statements

- “[M]isleading statements and omissions about the 2018 data breach involving the theft of student data and administrator log-in credentials of 13,000 school, district and university customer accounts.”
- “In its semi-annual report, filed in July 2019, Pearson referred to a data privacy incident as a hypothetical risk, when, in fact, the 2018 cyber intrusion had already occurred.”
- “And in a July 2019 media statement, Pearson stated that the breach may include dates of births and email addresses, when, in fact, it knew that such records were stolen, and that Pearson had "strict protections" in place, when, in fact, it failed to patch the critical vulnerability for six months after it was notified. The media statement also omitted that millions of rows of student data and usernames and hashed passwords were stolen.”

Press Release

SEC Charges Pearson plc for Misleading Investors About Cyber Breach

FOR IMMEDIATE RELEASE
2021-154

Washington D.C., Aug. 16, 2021 — The Securities and Exchange Commission today announced that Pearson plc, a London-based public company that provides educational publishing and other services to schools and universities, agreed to pay \$1 million to settle charges that it misled investors about a 2018 cyber intrusion involving the theft of millions of student records, including dates of births and email addresses, and had inadequate disclosure controls and procedures.

Misleading Statements on Data Security Practices

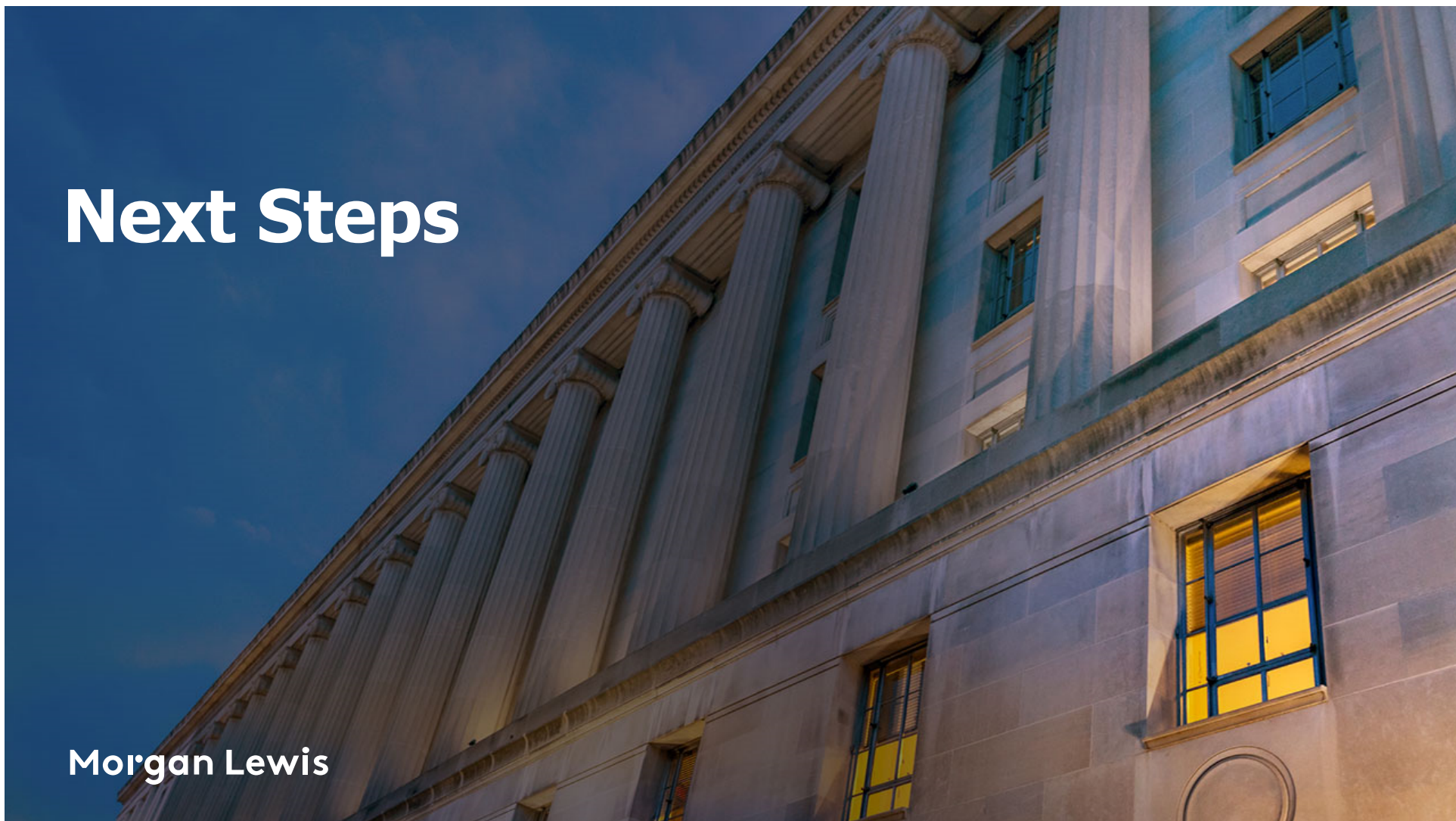


- Final Order requires company to:
 - Implement comprehensive security program,
 - Review software updates for security flaws before release,
 - Ensure updates will not hamper third-party security features,
 - Obtain biennial assessments of its security program by an independent third party, which the FTC has authority to approve, and
 - Notify the FTC of any data breach.

A screenshot of the Federal Trade Commission's website showing a press release. The page has a dark blue header with navigation links: "ABOUT THE FTC", "NEWS & EVENTS", "ENFORCEMENT", "POLICY", and "TIPS &". The main content area is white with a blue title: "FTC Gives Final Approval to Settlement with Zoom over Allegations the Company Misled Consumers about Its Data Security Practices". Below the title is the date "February 1, 2021" and social media sharing icons for Facebook, Twitter, and LinkedIn. A green "FOR YOUR INFORMATION" banner is followed by "TAGS: Coronavirus (COVID-19) | deceptive/misleading conduct | Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security | Tech". The main text of the press release is visible, starting with "The Federal Trade Commission finalized a settlement with Zoom Video Communications, Inc., over allegations it misled consumers about the level of security it provided for its Zoom meetings and compromised the security of some Mac users." and "The final order requires Zoom to implement a comprehensive security program, review any software updates for security flaws prior to release and ensure the updates will not hamper third-party security features. The company must also obtain biennial assessments of its security program by an independent third party, which the FTC has authority to approve, and notify the Commission if it experiences a data breach."

Next Steps

Morgan Lewis



The Best Offense is a Good Defense

- Risk Assessment and Management Program
- Internal Controls, Policies, Procedures and Standards
- Access Management
- Training
- Third Party Vendors
- Governance
- Managing Cyber Incident
- Address Disclosure Issues
- Address Unique Jurisdiction Standards and Requirements
- Insider Trading Controls
- Legal Review of Key Phases

Prepared for All Cyber Incident Phases

- Before, during, and after a data breach.
- Data breach-prevention guidance.
 - Implementing policies and training regarding data breaches, including governance and risk assessments, data loss prevention, and vendor management.
- Guidance on managing data breach.
 - Conducting confidential, privileged cyber incident investigations.
- Regulatory enforcement investigations and actions by federal and state regulators.
- FCA investigations and cases
- Class action litigation or other litigation that often results from a data breach.
 - Successfully defended more than two dozen data privacy class actions – either winning motions to dismiss or defeating class certifications in lawsuits brought after data breaches or based upon alleged violations of a company’s privacy policy.

Questions?



Mark L. Krotoski



Doug W. Baruch

Morgan Lewis

Mark L. Krotoski



Partner

Morgan Lewis

mark.krotoski@morganlewis.com

+1.650.843.7212

Litigation Partner, Privacy and Cybersecurity and Antitrust practices

- Co-Head of Privacy and Cybersecurity Practice Group
- More than 20 years' experience handling cybersecurity cases and issues
- Assists clients on litigation, mitigating and addressing cyber risks, developing cybersecurity protection plans, responding to a data breach or misappropriation of trade secrets, conducting confidential cybersecurity investigations, responding to federal and state regulatory investigations, and coordinating with law enforcement on cybercrime issues.
- Variety of complex and novel cyber investigations and cases including under the Computer Fraud and Abuse Act
- At DOJ, prosecuted and investigated nearly every type of international and domestic computer intrusion, cybercrime, economic espionage, and criminal intellectual property cases.
- Served as the national coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the DOJ's Criminal Division, in addition to other DOJ leadership positions, and as a cybercrime prosecutor in Silicon Valley.

Morgan Lewis

Douglas W. Baruch



Partner

Morgan Lewis

douglas.baruch@morganlewis.com

+1.202.739.5219

Doug represents corporations and individuals in a variety of complex civil and criminal litigation and enforcement matters, ranging from investigations and subpoena compliance to federal and state court litigation and appeals, with an emphasis on cases arising under the False Claims Act (FCA) and Financial Institutions Reform, Recovery, and Enforcement Act (FIRREA)

- He represents clients in the full spectrum of industries that are targeted for civil fraud enforcement by federal, state, and private parties (qui tam relators), including government contractors, aerospace and defense businesses, financial institutions, healthcare entities, and federal grant recipients.
- Doug also has an extensive commercial litigation practice. In addition, he has handled numerous international arbitration matters, acting as counsel to domestic and foreign corporations in a variety of International Chamber of Commerce and ad hoc arbitrations.
- He writes and lectures extensively on various aspects of the FCA and FIRREA. He is co-author of Civil False Claims and Qui Tam Actions (Wolters Kluwer, 5th Ed.), the comprehensive, two-volume treatise that frequently is cited by federal and state courts as an authority on the False Claim Act.

Morgan Lewis

Coronavirus COVID-19 Resources

We have formed a multidisciplinary **Coronavirus/COVID-19 Task Force** to help guide clients through the broad scope of legal issues brought on by this public health challenge.

Morgan Lewis

To help keep you on top of developments as they unfold, we also have launched a resource page on our website at www.morganlewis.com/topics/coronavirus-covid-19

If you would like to receive a daily digest of all new updates to the page, please visit the resource page to [subscribe](#) using the purple "Stay Up to Date" button.



Our Global Reach

Africa

Asia Pacific

Europe

Latin America

Middle East

North America

Our Locations

Abu Dhabi

Almaty

Beijing

Boston

Brussels

Century City

Chicago

Dallas

Dubai

Frankfurt

Hartford

Hong Kong

Houston

London

Los Angeles

Miami

Moscow

New York

Nur-Sultan

Orange County

Paris

Philadelphia

Pittsburgh

Princeton

San Francisco

Shanghai

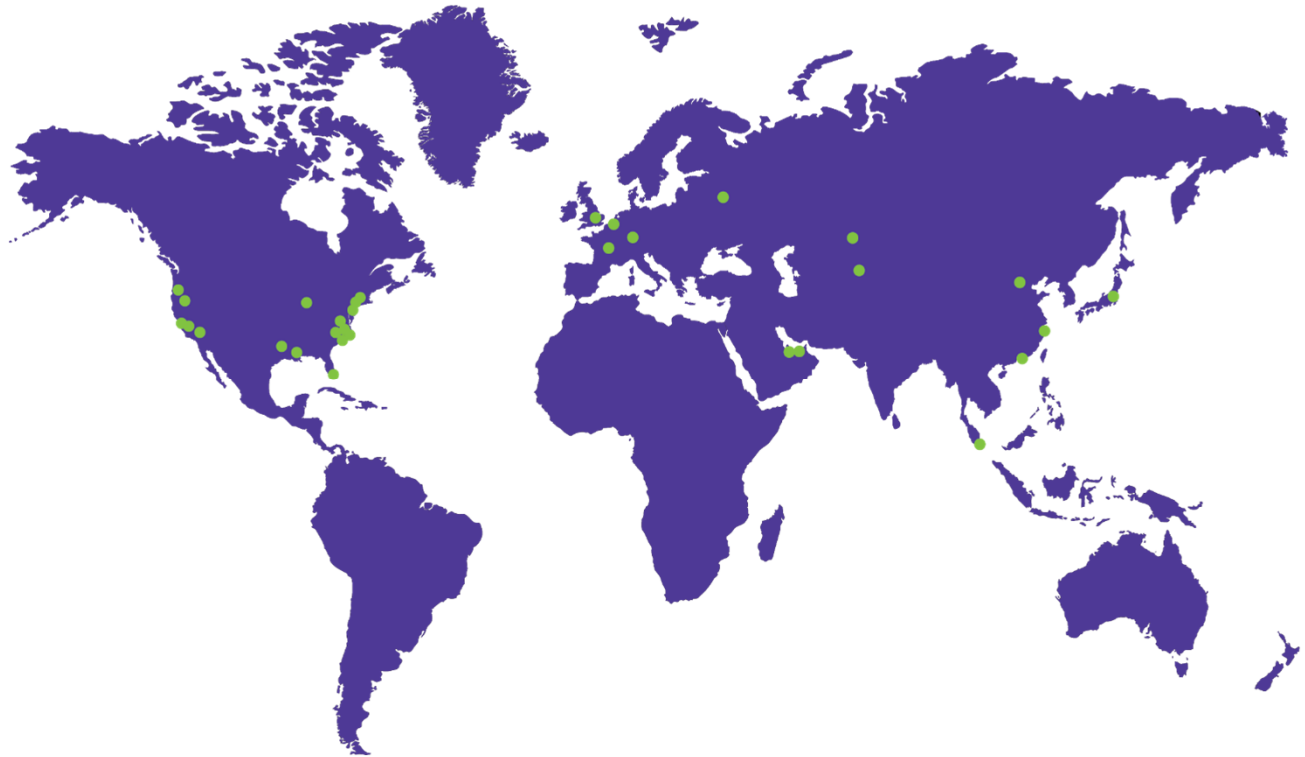
Silicon Valley

Singapore

Tokyo

Washington, DC

Wilmington



Morgan Lewis

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU

© 2021 Morgan, Lewis & Bockius LLP
© 2021 Morgan Lewis Stamford LLC
© 2021 Morgan, Lewis & Bockius UK LLP

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.

Morgan Lewis