

Morgan Lewis

**CYBERSECURITY INCIDENT RESPONSE:
PREPARING FOR THE INEVITABLE AND
MITIGATING LITIGATION AND
ENFORCEMENT ISSUES**

October 1, 2020



Presenters



Mark L. Krotoski



Andrew J. Gray IV

Morgan Lewis



Overview

- Cyber Landscape and Risks: How Prepared Are You?
- Significant Costs and Consequences
 - Case Study
- Threat Focus: Ransomware
- Early Consideration of the Scope of the Attorney Client Privilege on Data Breach Cases
- Anticipating and Addressing Regulatory Enforcement Issues
- Litigation Defense Issues
- Key Elements in Incident Response
 - Managing Notification Issues
- Best Practices, Next Steps



Morgan Lewis

4

Preliminary Note

- Comments during this presentation are based upon:
 - Publicly available information;
 - General observations and experience; and
 - **Not** on any specific client case information.

Morgan Lewis

5

DATA PRIVACY AND PROTECTION BOOT CAMP

CYBER LANDSCAPE AND RISKS

CONSIDER HOW PREPARED ARE YOU?

Cyber Landscape and Risks

Key Actors
Organized Cyber Crime
State Sponsored
Hackers for Hire
Hacktivists
Third Party Vendor Attacks
Insiders
Inadvertence

Business Email Compromise

Phishing

COVID-19 Shelter in Place Risks

Malicious Attack

Insider Threat

Ransomware

Third Party Vendors

Password Compromise

Morgan Lewis 7

Two Scenarios

SCENARIO ONE
Prepare in advance now

- Tailored cybersecurity program
- Consider new, emerging legal standards
- Legal guidance under attorney client privilege
- Risk assessments, compliance issues
- Training
- Safeguard third party vendor information
- Address unique issues, consider safeguards

LATER CYBER INCIDENT

- Cyber investigation under attorney client privilege / work product doctrine
 - Determine scope of incident
- Reputational harm
- Assess litigation exposure and risk
- Federal and state regulators

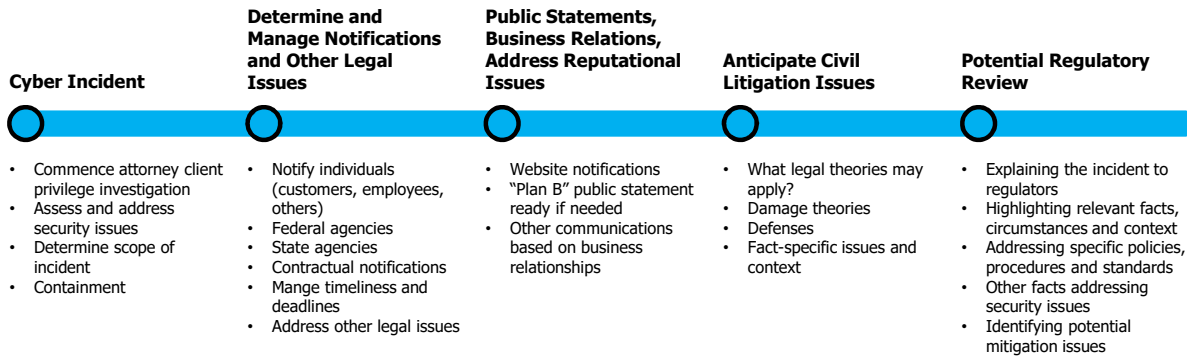
SCENARIO TWO
Respond to incident now

CYBER INCIDENT

- Ransomware, business email compromise, phishing scheme, account takeover, etc.
- Cyber investigation under attorney client privilege / work product doctrine
 - Determine scope of incident
 - Are prior vulnerabilities exposed?
 - Failure to patch
 - Lack of controls to prevent incident
 - Training issues (e.g., recurring phishing)
- Reputational harm
- Training
- Assess litigation exposure
- Federal and state regulators

Morgan Lewis 8

Incident Response Timeline Key Phases



Morgan Lewis

9

Are You Prepared?

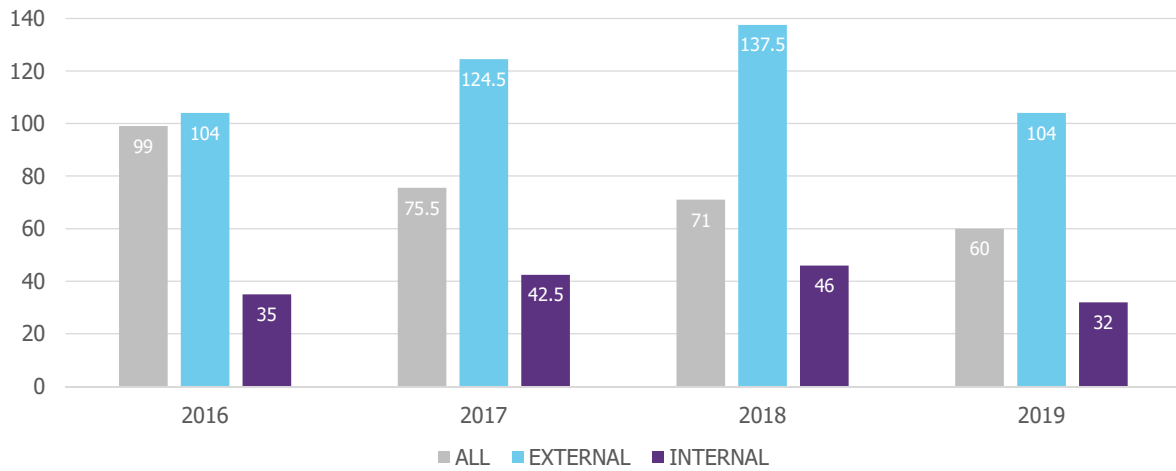
Security vulnerabilities, scope of impact, reputational harm, litigation, enforcement investigation, and other damages and costs can result from **any one weak link** in your cybersecurity program.

Not a question of "if" but "when".

Morgan Lewis

10

Learning About Attacker in Victim Network Before Detection (Americas)



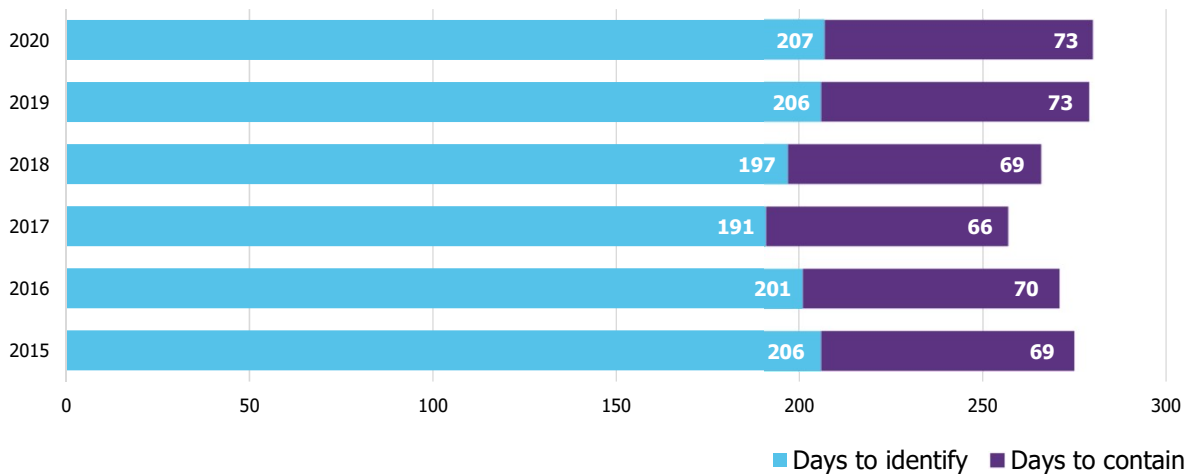
Dwell time is the number of days an attacker is present in a victim network before detection. The median represents a value at the midpoint of a data set sorted by magnitude.

Morgan Lewis

FireEye Mandiant Services | M-Trends 2020 Special Report | <https://content.fireeye.com/m-trends/rpt-m-trends-2020>

11

Average Time to Identify and Contain a Data Breach



IBM Security | Cost of a Data Breach Report 2020

Morgan Lewis

12

Example: Discovery of Phishing Email Resulting in Compromise

PREMERA BLUE CROSS

Shop for Plans ▾ Health Plan Basics ▾ Find a Doctor ▾ Pharmacy ▾ Member Services ▾ Healthsource Blog ▾

About the Premera cyberattack

Tuesday, March 17, 2015
 About the [Experian Cyberattack](#)

[Go here](#) for information on the cyberattack involving [Exocitus Blue Cross Blue Shield](#).

On January 29, 2015, Premera Blue Cross (Premera) discovered that cyberattackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on May 5, 2014. As part of our own investigation, we notified the FBI and are coordinating with the Bureau's investigation into this attack.

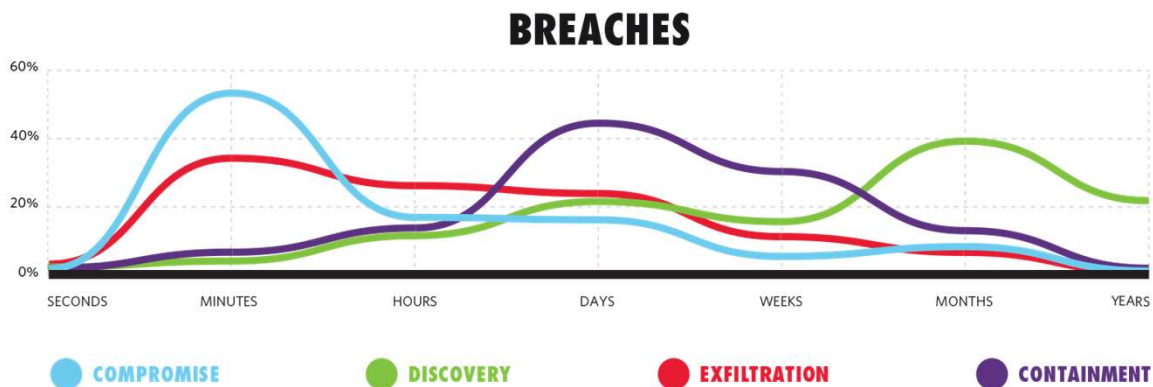
- Phishing email used to install malware and compromise system
- Discovered **269 days later (nearly 9 months)**
 - May 5, 2014 initial attack
 - Jan. 29, 2015 discovery
 - March 17, 2015 public disclosure
- Affected Protected Health Information of more than 10.4 million current, former and affiliated members and employees

Morgan Lewis

<https://www.premera.com/wa/visitor/healthsource/community/premera-cyberattack/>

13

Containment



Verizon 2019 Data Breach Investigations Report

Morgan Lewis

14

Weak Links Examples

- Failure to patch
- Third party vendor
- Passwords
- Phishing
- Training
- Lost laptop or thumb drive



Morgan Lewis

15

DATA PRIVACY AND PROTECTION BOOT CAMP

**SIGNIFICANT COSTS
AND CONSEQUENCES**

COMPLEX, COSTLY, BURDENSOME

2020 Cost of Data Breach Report: Key Findings

- \$3.86 million average total cost
- Lost business costs accounted for nearly 40% of the average total cost of a data breach of \$1.52 million
 - Including increased customer turnover, lost revenue due to system downtime and the increasing cost of acquiring new business due to diminished reputation.
- 280 days average time to detect and contain a data breach
 - 315 days average time to detect and contain a data breach caused by a malicious attack

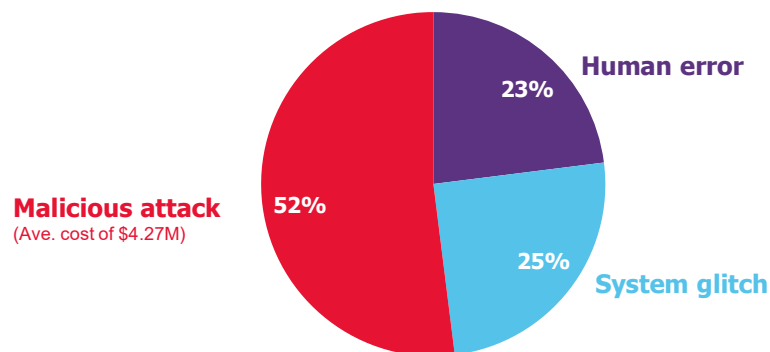


Morgan Lewis IBM Security | Cost of a Data Breach Report 2020
https://www.ibm.com/security/data-breach?mhsrc=ibmsearch_a&mhq=cost%20of%20a%20data%20breach%20report

17

Data Breach Root Cause Breakdown

Malicious attacks cause a majority of data breaches

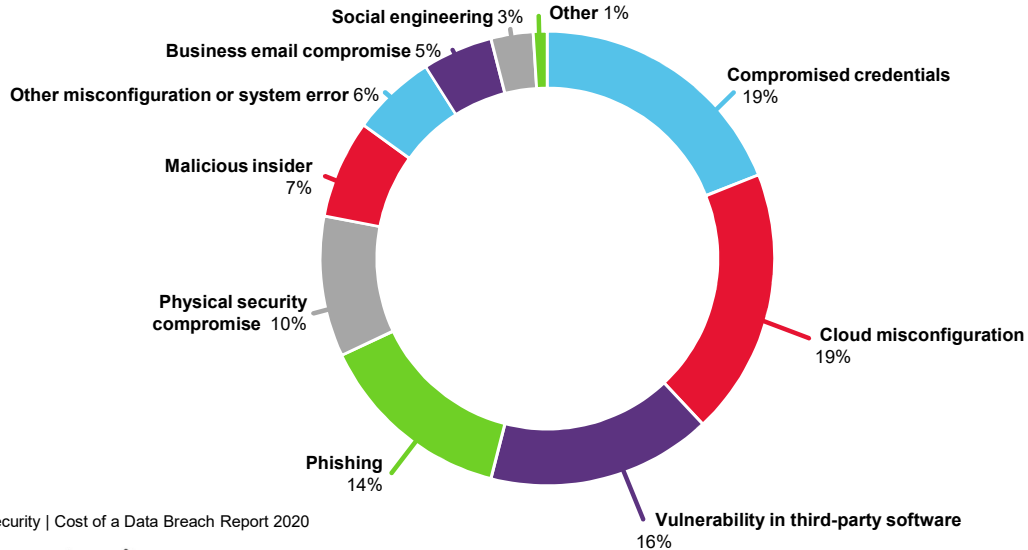


IBM Security | Cost of a Data Breach Report 2020

Morgan Lewis

18

Breakdown of Malicious Data Breach Root Causes



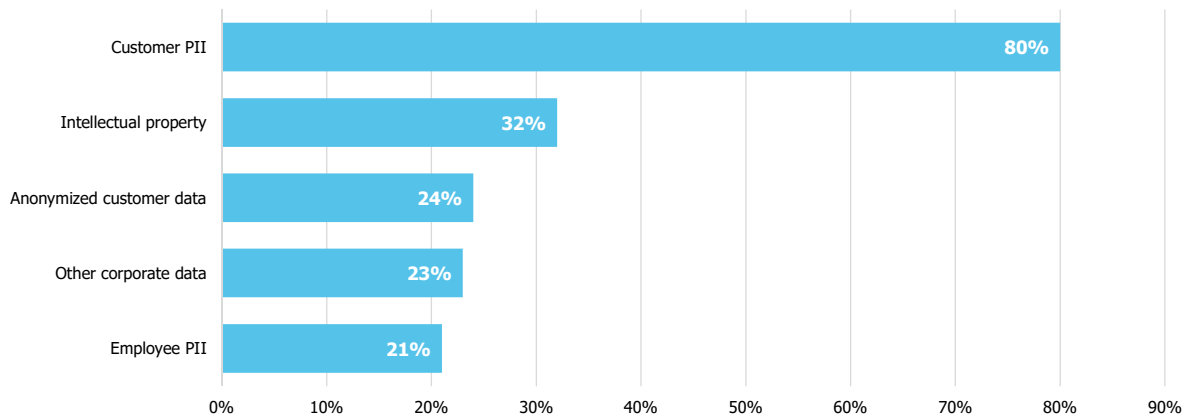
IBM Security | Cost of a Data Breach Report 2020

Morgan Lewis

19

Types of Compromised Records

Percentage of breaches involving data in each category



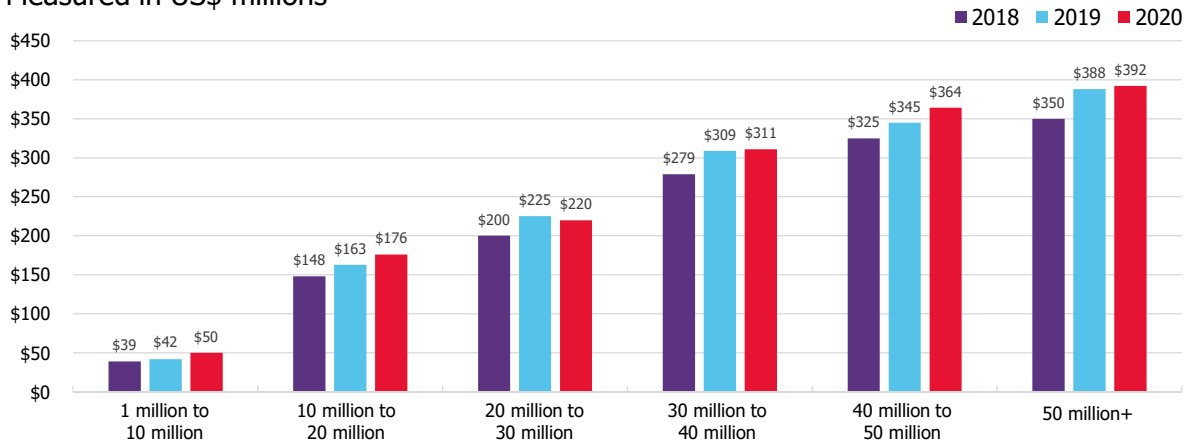
IBM Security | Cost of a Data Breach Report 2020

Morgan Lewis

20

Average Total Cost of A Mega Breach by Number of Records Lost

Measured in US\$ millions



IBM Security | Cost of a Data Breach Report 2020

Morgan Lewis

21

DATA PRIVACY AND PROTECTION BOOT CAMP

SIGNIFICANT COSTS AND CONSEQUENCES

CASE STUDY - EQUIFAX

Equifax Inc. – Incident and Response Timeline

- **March 2017**

- United States Computer Emergency Readiness Team (“US-CERT”) alerts Equifax to a new security vulnerability found in Apache Struts, an open source framework used to build Java web applications. The alert encouraged a software update to a new version.

- **May 2017**

- Hackers began to access personal identifying information.

- **July 2017**

- Equifax discovered “suspicious network traffic” associated with its consumer dispute website. Its information security department applied the Apache patch.
- Equifax’s information security department observed further suspicious activity and took the web application offline.
- Equifax’s Chief Information Officer notified CEO Richard Smith of the suspicious activity.

- **August 2017**

- Three senior Equifax executives sold stock worth almost \$1.8 million.

- **Fall 2017**

- Equifax announced the security breach to the public on Twitter.
- Two Equifax executives resigned.
- Equifax issued a press release confirming that the vulnerability was Apache Struts CVE-2017-5638.
- Equifax CEO Richard Smith retired and Board of Directors appointed Paulino do Regos Barros Jr. as Interim CEO.
- Interim CEO Paulino do Regos Barros Jr. published a public apology on behalf of Equifax, and announced a new free service allowing people to lock and unlock their credit.

Morgan Lewis

<https://epic.org/privacy/data-breach/equifax/>

23

Equifax Inc. – Public Disclosures (Sept. 7, 2017)

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

No Evidence of Unauthorized Access to Core Consumer or Commercial Credit Reporting Databases
 Company to Offer Free Identity Theft Protection and Credit File Monitoring to All U.S. Consumers

ATLANTA, Sept. 7, 2017 /PRNewswire/ -- Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's

Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately **143 million U.S. consumers**. Criminals exploited a U.S. website application vulnerability to gain access to certain files.

leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.

Morgan Lewis

<https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>

24

Equifax Inc. – Public Disclosures

September 7, 2017

Equifax Announces Cybersecurity Incident Involving Consumer Information



No Evidence of Unauthorized Access to Core Consumer or Commercial Credit Reporting Databases

Company to Offer Free Identity Theft Protection and Credit File Monitoring to All U.S. Consumers

Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.



Morgan Lewis

<https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information/>
<https://www.equifaxsecurity2017.com/frequently-asked-questions/>

25

Security Vulnerability Identified

BUSINESS NEWS

OCTOBER 2, 2017:52 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 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."

Morgan Lewis

<https://www.reuters.com/article/us-equifax-breach/equifax-failed-to-patch-security-vulnerability-in-march-former-ceo-idUSKCN1C71VY>

26

Security Vulnerability Alert (March 8, 2017)

Morgan Lewis <https://us-cert.cisa.gov/ncas/current-activity/2017/03/08/Apache-Software-Foundation-Releases-Security-Updates>
<https://cwiki.apache.org/confluence/display/WWW/S2-045>

27

Public Apology

On Behalf of Equifax, I'm Sorry

A new free service will let consumers lock or unlock access to their credit data any time they like.

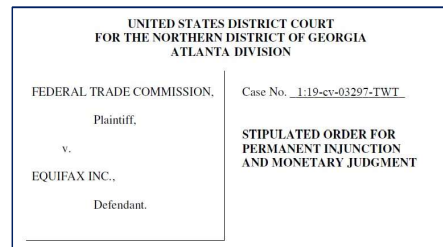
- On behalf of Equifax, I want to express my sincere and total apology to every consumer affected by our recent data breach. People across the country and around the world, including our friends and family members, put their trust in our company. We didn't live up to expectations.
- **We were hacked.** That's the simple fact. But we compounded the problem with insufficient support for consumers. Our website did not function as it should have, and our call center couldn't manage the volume of calls we received. Answers to key consumer questions were too often delayed, incomplete or both. **We know it's our job to earn back your trust.**
- Interim CEO Paulino do Regos Barros Jr. (Sept. 27, 2017)

Morgan Lewis <https://www.wsj.com/articles/on-behalf-of-equifax-im-sorry-1506547253>

28

FTC and CFPB and State Enforcement Actions – Northern District of Georgia (July 23, 2019)

- Federal Trade Commission v. Equifax, Inc.
- **\$575-700 million**
 - The settlement includes up to \$425 million to provide affected consumers with credit monitoring services.



Morgan Lewis

<https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc>
<https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related>

29

NYDFS, Indiana, Massachusetts and Chicago Actions



Attorney General Curtis Hill under a settlement reached with Equifax, Inc. Indiana was one of two states in July 2019 — choosing its own settlement with Equifax, Inc.

Press Release
July 22, 2019

GOVERNOR CUOMO AND NEW YORK ATTORNEY GENERAL LETITIA JAMES ANNOUNCE \$19.2 MILLION SETTLEMENT WITH EQUIFAX OVER 2017 DATA BREACH

Department of Financial Services and New York Attorney General's Office Fine Equifax and Two Subsidiaries



Law360 (April 17, 2020, 10:09 PM EDT) -- Massachusetts has become the last state to settle with Equifax over its massive 2017 data breach, with Attorney General Maura Healey announcing a deal Friday that will require the credit reporting giant to pay \$18.2 million and make "significant" business practice changes to fall into step with the state's robust data security law.

While the Massachusetts attorney general's office has fielded more than 28,000 data breach reports during the past year, the state's attorney general's office has not yet reached a settlement with other sensitive residents —



Law360 (April 10, 2020, 7:47 PM EDT) -- The city of Chicago says it has reached a \$1.5 million settlement to resolve a lawsuit against Equifax Inc. over a massive 2017 data breach that exposed the sensitive personal information of roughly 147 million people.

Chicago is one of a few municipalities, along with the District of Columbia, to receive a settlement in litigation against Equifax, city officials said Tuesday. It complements other deals reached with the credit bureau by the federal government, state governments and private plaintiffs, said Stephen Kane, the city's deputy corporation counsel.

Morgan Lewis

https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1907221
<https://www.law360.com/articles/1264893/print?section=banking>
<https://www.law360.com/articles/1264893/equifax-mass-ag-ink-18-2m-deal-to-end-data-breach-suit>
<https://calendar.in.gov/site/oag/event/ag-curtis-hill-secures-195-million-equifax-settlement-for-hoosier-consumers/>

30

Equifax Class Actions



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

Equifax Investor Suits Get Early OKs For \$149M, \$33M Deals

By Dave Simpson

Law360 (February 25, 2020, 11:01 PM EST) -- A Georgia federal judge on Tuesday preliminarily approved a \$149 million deal to end a securities suit from a putative class of Equifax investors related to the credit reporting agency's massive 2017 data breach, just a day after he did the same for a \$32.5 million deal in a derivative shareholder suit stemming from the same incident.

The putative class of investors in the stock-drop suit, headed by Union Asset Management Holding AG, would recover about \$2.08 per affected share before fees, expenses and costs under the deal preliminarily approved by U.S. District Judge Thomas W. Thrash Jr., according to court filings. Counsel for the investors plan to request fees not to exceed 20% of the settlement fund, according to the proposed deal.

Earlier this month, the putative class said that given the risks of litigation, the proposed deal is a good one.



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

Equifax Inks \$30M Deal With Credit Unions Over Data Breach

By Dave Simpson

Law360 (May 15, 2020, 10:32 PM EDT) -- Equifax Inc. has agreed to pay \$5.5 million to a putative class of thousands of banks and credit unions, and to spend at least \$25 million on the financial institutions' data security, to end their claims in multidistrict litigation stemming from a massive 2017 data breach, the banks said Friday.

The financial institutions had argued that the money and time they spent to protect their customers' data is a valid injury directly tied to Equifax's allegedly deficient data security measures. But, in their bid for preliminary approval of the deal filed in Georgia federal court, the banks said the proposed settlement is fair.

"Class counsel presented theories of liability based on the unique nature of Equifax's role in the financial 'ecosystem' in addition to the traditional negligence claims related to the compromised payment card data," they said. "Some of these theories were rejected by the court at the Rule 12 pleading stage. If plaintiffs were to attempt to revive those claims, they would have to litigate the case to completion and await a post-judgment appeal, the outcome of which would be uncertain and likely several years away."

Morgan Lewis

<https://www.law360.com/articles/1274366/print?section=banking>
<https://www.law360.com/articles/1247297/print?section=banking>

31

Equifax Cases

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

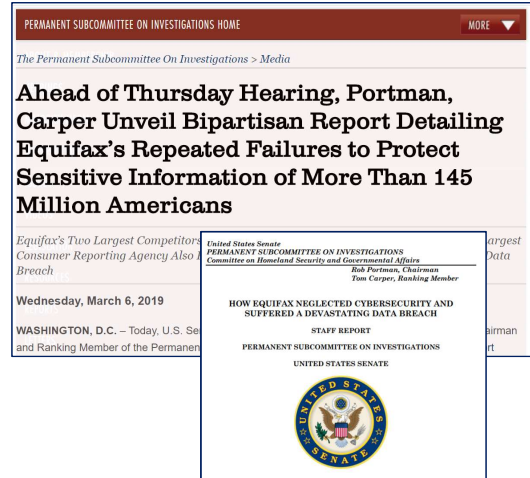
Morgan Lewis

32

Permanent Subcommittee on Investigations, Senate Homeland Security and Governmental Affairs Committee

“As a result of poor cybersecurity practices, Equifax failed to adequately protect the sensitive information of more than 145 million Americans, including information on driver’s licenses, passports and Social Security numbers.”

“Equifax allowed a key tool used to monitor IT assets for malicious web traffic to expire in November 2016. As a result, the hackers’ presence in the company’s network went entirely undetected for 78 days.”



Morgan Lewis

<https://www.hsgac.senate.gov/subcommittees/investigations/media/ahead-of-thursday-hearing-portman-carper-unveil-bipartisan-report-detailing-equifax-repeated-failures-to-protect-sensitive-information-of-more-than-145-million-americans>

33

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 on Oversight and Government Reform released a staff report after the Committee’s 14-month investigation of the largest data breaches in U.S. history. Through the investigation, the Committee reviewed documents and conducted transcribed interviews with three former Equifax employees.



Morgan Lewis

<https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf>
<https://republicans-oversight.house.gov/report/committee-releases-report-revealing-new-information-on-equifax-data-breach/>

34

Early Insider Trading Questions

Menu Q Search **Bloomberg**

Cybersecurity

Three Equifax Managers Sold Stock Before Cyber Hack Revealed

By [Anders Melin](#)
September 7, 2017, 2:59 PM PDT Updated on September 8, 2017, 6:17 AM PDT

- ▶ Trio didn't know about the intrusion when selling, firm says
- ▶ Shares tumbled in late trading after company disclosed breach

09-07-17 **FAST COMPANY**

Equifax execs dumped almost \$1.8 million in stock before revealing giant data breach

Three Equifax executives sold almost \$1.8 million worth of stock in the company shortly after the company discovered a security breach that could affect about 143 million U.S. consumers and an unspecified number of Canadian and U.K. customers, Bloomberg reports. The trades weren't part of a scheduled trading plan. The breach was discovered July 29 and believed ...

TECHNOLOGY NEWS
NOVEMBER 3, 2017 6:13 AM UPDATED 3 YEARS AGO

Equifax clears executives who sold shares after hack

By [John McCrank](#), [Anarajita Saxena](#)
3 MIN READ

(Reuters) - Equifax Inc. [EFX.N](#) said on Friday four of its executives who sold shares before the credit-reporting firm disclosed a massive data breach that wiped out billions from its market value were not aware of the incident when they made the trades.

FILE PHOTO: Credit reporting company Equifax Inc. corporate offices are pictured in Atlanta, Georgia, U.S., [September 8, 2017](#).

A special committee set up by Equifax's board to investigate the trades concluded that no insider trading took place and that pre-clearance for the trades was appropriately obtained.

Morgan Lewis

<https://www.reuters.com/article/us-equifax-cyber/equifax-clears-executives-who-sold-shares-after-hack-idUSKBN1D31EK>
<https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack>
<https://www.fastcompany.com/40464588/equifax-exec-sold-almost-1-8-million-in-stock-before-revealing-privacy-data-breach>

35

Equifax Inc.: SEC Action – Insider Trading Claims



- **Securities and Exchange Commission v. Jun Ying** – March 14, 2018
 - Jun Ying, a former chief information officer of a U.S. business unit of Equifax, who was next in line to be the company's global CIO, allegedly used confidential information entrusted to him to conclude that Equifax had suffered a serious breach.
 - Before Equifax's public disclosure of the data breach, Ying exercised all of his vested Equifax stock options and then sold the shares, resulting in proceeds of nearly \$1 million, and avoiding more than \$117,000 in losses.
- **Securities and Exchange Commission v. Sudhakar Reddy Bonthu** – June 28, 2018
 - Equifax software engineering manager Sudhakar Reddy Bonthu was charged with trading on confidential information he received while creating a website for consumers impacted by a data breach.
 - SEC alleged he traded on the non-public information by purchasing Equifax put options. Less than a week later, after Equifax publicly announced the data breach and its stock declined nearly 14 percent, Bonthu sold the put options and netted more than \$75,000, a return of more than 3,500 percent on his initial investment.
 - Bonthu, was terminated from Equifax after refusing to cooperate with an internal investigation into whether he had violated the company's insider trading policy.

Morgan Lewis

<https://www.sec.gov/litigation/complaints/2018/comp24073.pdf>
<https://www.sec.gov/litigation/complaints/2018/comp24183.pdf>

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

SECURITIES AND EXCHANGE COMMISSION,	Plaintiff,	Case No.
	v.	
JUN YING,	Defendant.	JURY TRIAL DEMANDED

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

SECURITIES AND EXCHANGE COMMISSION,	Plaintiff,	Case No.
	v.	
SUDHAKAR REDDY BONTHU,	Defendant.	JURY TRIAL DEMANDED

36

DOJ Prosecution



- October 16, 2018, Sudhakar Reddy Bonthu
 - Former manager at Equifax
 - Sentenced to eight months of home confinement, fined \$50,000, ordered to forfeit \$75,979.
- June 27, 2019, Jun Ying
 - Former chief information officer of a U.S. business unit of Equifax
 - Sentenced to four months in prison and one year of supervised release, ordered to pay restitution \$117,117.61, and fined \$55,000.

Department of Justice
U.S. Attorney's Office
Northern District of Georgia

SHARE

FOR IMMEDIATE RELEASE Thursday, June 27, 2019

Former Equifax employee sentenced for insider trading

ATLANTA - Jun Ying, the former Chief Information Officer of Equifax U.S. Information Solutions, has been sentenced to federal prison for insider trading.

"Ying thought of his own financial gain before the millions of people exposed in this data breach even knew they were victims," said U.S. Attorney Byung J. "BJay" Pak. "He abused the trust placed in him and the senior position he held to profit from inside information."

"If company insiders don't follow the rules that govern all investors, they will face the consequences for their actions. Otherwise the public's trust in the stock market will erode," said Chris Hacker, Special Agent in Charge of FBI Atlanta. "The FBI will do everything in its power to stop anyone who takes unfair advantage of their insider knowledge."

U.S. v. Jun Ying (N.D. Geo. 1:18-cr-00074)
U.S. v. Bonthu (N.D. Geo. 1:18-cr-00237)

Morgan Lewis <https://www.justice.gov/usao-ndga/pr/former-equifax-manager-sentenced-insider-trading>
<https://www.justice.gov/usao-ndga/pr/former-equifax-employee-sentenced-insider-trading>

Criminal Hacking Case



- On February 10, 2020, announced charges against four Chinese military-backed hackers for the 2017 cyberattack against Equifax.
- "The PLA hackers obtained names, birth dates, and social security numbers for approximately **145 million American citizens**, in addition to **driver's license numbers for at least 10 million Americans** stored in Equifax's databases. The hackers also collected **credit card numbers** and other personally identifiable information belonging to approximately **200,000 American consumers.**"
- "This data has economic value, and these thefts can feed China's development of artificial intelligence tools as well as the creation of intelligence-targeting packages," U.S. Attorney General William Barr said. "In addition to the thefts of sensitive personal data, our cases reveal a pattern of state-sponsored computer intrusions and thefts by China targeting trade secrets and confidential business information."



WANTED BY THE FBI

CHINESE PLA MEMBERS, 54TH RESEARCH INSTITUTE

Specialist Peng, Sergeant Major Wang, Corporal Li, Sergeant Peng, Specialist Peng, Sergeant Major Wang, Corporal Li, Sergeant Peng

Do not disseminate information about these individuals, please contact your local FBI office or the nearest FBI office.

READY TO CHALLENGE

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA, ATLANTA DIVISION

United States of America vs. **WU ZHENGLI, WANG QIANG, LI JIALI, LIU JIAN**

THE GRAND JURY CHARGES THAT:

INTRODUCTION

1. Equifax Inc. is a consumer credit reporting agency headquartered in Atlanta, Georgia ("Equifax"). It is the largest source of business, Equifax collects and stores a vast collection of consumer information, which it sells to other businesses and organizations looking to use the information to make credit decisions or verify identity. Equifax thus holds a critical repository of sensitive personally identifiable information, including full names, addresses, social security numbers, birth dates, and driver license numbers, belonging to hundreds of millions of individuals in the United States and abroad. This data compilation was confidential, proprietary business information for Equifax, and the company used the information on restricted, computer servers located in Alabama, Georgia and elsewhere.

Morgan Lewis

<https://www.justice.gov/pr/chinese-military-sponsored-computer-hack-economic-espionage-and-us-fraud-hacking>
<https://www.fbi.gov/newsroom/press-releases/2020/02/10/20-cv-00010>
<https://www.justice.gov/pr/2020-02-10>

“Under-Covered” for Cyber-Related Losses

- Equifax data breach (2017)
 - Only \$125 million was covered by insurance (at least 71% underinsurance rate).
 - Data breach costs substantially higher.



Morgan Lewis

<https://www.nytimes.com/2019/07/22/business/equifax-settlement.html>

<https://www.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUSKCN1GE257>

39

DATA PRIVACY AND PROTECTION BOOT CAMP

THREAT FOCUS: RANSOMWARE

Demand Note

DoppelPaymer

██████████ Your network has been penetrated.

This link and your decryption key will expire in 14 days after your systems were infected. Sharing this link or email will lead to the irreversible removal of the decryption keys.

NO TIME remains for special price.

All files on each host in the network have been encrypted with a strong algorithm. Backups were either encrypted or deleted or backup disks were formatted.

No any working decryption software is available from other sources.

Do not rename the encrypted or informational text files. Do not move the encrypted or informational text files. This may lead to the impossibility of recovery of the certain files.

Also, we have gathered all your private sensitive data. So if you decide not to pay, we would share it. It may harm your business reputation.

- Your reference ID: **135**
(we recommend to put the reference ID as the subject when contacting us)
- BTC wallet for payment:

Online chat



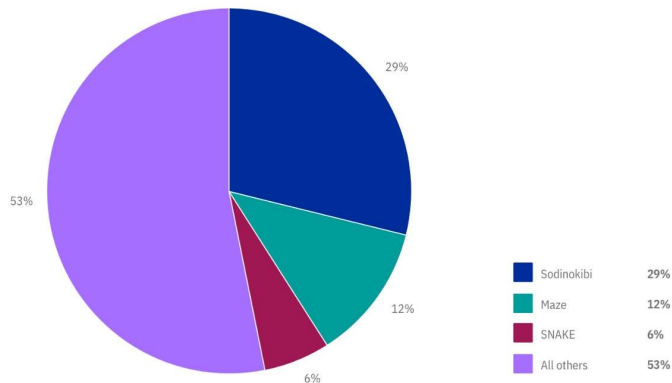
Morgan Lewis

<https://twitter.com/GrujaRS/status/1194405547145080832/photo/1>

41

Many Ransomware Families

Top ransomware families per attack volume



Source: IBM Security X-Force

Morgan Lewis

<https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/>

42

Common Initial Ransomware Steps

- Network Access
 - Phishing
 - Remote Desktop Protocol
 - Attachments
 - Surveillance, command and control
 - Disable anti-virus or other defenses
- Encrypt or Lock Computer Files
 - Usually search and encrypt file types
 - Normally does not search content
- Demand Payment
 - Usually in bitcoin
 - Urgency
 - Threats to release or destroy data



Morgan Lewis

43

New Exfiltration Trend

- “A hacker published documents containing Social Security numbers, student grades and other private information stolen from a large public-school district in Las Vegas **after officials refused a ransom** demanded in return for unlocking district computer servers.”
- “The illegal release late last week of sensitive information from the Clark County School District in Las Vegas, with about 320,000 students, demonstrates an escalation in tactics for hackers who have taken advantage of schools heavily reliant on online learning and technology to run operations during the coronavirus pandemic.”

♦ WSJ NEWS EXCLUSIVE | U.S.

Hacker Releases Information on Las Vegas-Area Students After Officials Don't Pay Ransom

Clark County in Nevada is largest known school district hit by hackers during Covid-19 pandemic



A classroom at Walter Johnson Junior High School in Las Vegas on Aug. 24. The Clark County School District in Las Vegas has about 320,000 students.

PHOTO: ETHAN MILLER/GETTY IMAGES

By [Tawnell D. Hobbs](#)




Updated Sept. 28, 2020 3:56 pm ET

Morgan Lewis

<https://www.wsj.com/articles/hacker-releases-information-on-las-vegas-area-students-after-officials-dont-pay-ransom-11601297930>


44

New Ransomware Demands

blackbaud® Who We Serve Solutions Training and Support Industry Insights Company More...    Sign in

Summary of Incident

In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system. Prior to our locking the cybercriminal out, the **cybercriminal removed a copy of a subset of data from our self-hosted environment.** The cybercriminal did not access credit card information, bank account information, or social security numbers. Because protecting our customers' data is our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. This incident did not involve solutions in our public cloud environment (Microsoft Azure, Amazon Web Services), nor did it involve the majority of our self-hosted environment. The subset of customers who were part of this incident have been notified and supplied with additional information and resources. We apologize that this happened and will continue to do our very best to supply help and support as we and our customers jointly navigate this cybercrime incident.



Morgan Lewis <https://www.blackbaud.com/securityincident>

45

Posting Exfiltrated Data

MAZE MAZE

Represented here companies dont wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news!

Morgan Lewis <https://krebsonsecurity.com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/#more-49994>

46

Larger Payments

CYBER RISK JULY 31, 2020 6:55 AM / UPDATED 19 HOURS AGO

'Payment sent' - travel giant CWT pays \$4.5 million ransom to cyber criminals

Jack Stubbs

4 MIN READ

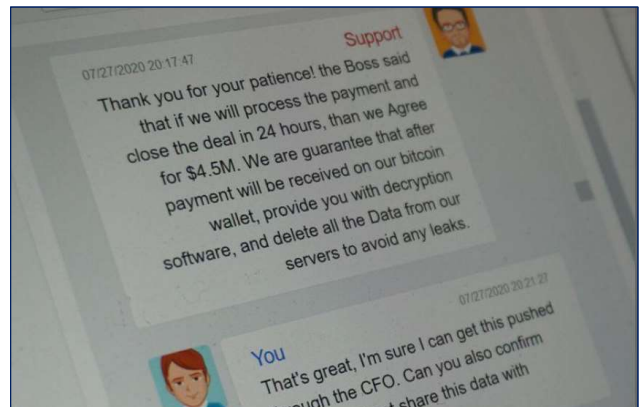
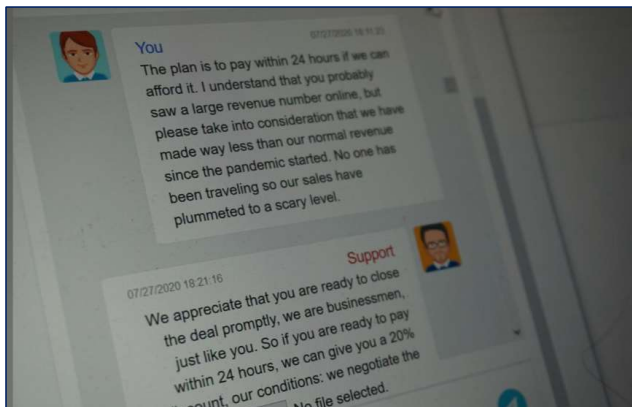


LONDON (Reuters) - U.S. travel management firm CWT paid \$4.5 million this week to hackers who stole reams of sensitive corporate files and said they had knocked 30,000 computers offline, according to a record of the ransom negotiations seen by Reuters.

Morgan Lewis <https://www.reuters.com/article/us-cyber-cwt-ransom/payment-sent-travel-giant-cwt-pays-45-million-ransom-to-cyber-criminals-idUSKCN24W25W>

47

Payment Negotiations



Morgan Lewis <https://www.reuters.com/article/us-cyber-cwt-ransom/payment-sent-travel-giant-cwt-pays-45-million-ransom-to-cyber-criminals-idUSKCN24W25W>

48

Payment?

WHAT IS RANSOMWARE?
Ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

HOW DO I RESPOND TO RANSOMWARE?
Implement your security incident response and business continuity plan. It may take time for your organization's IT professionals to isolate and remove the ransomware threat to your systems and restore data and normal operations. In the meantime, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

HOW DO I PROTECT MY NETWORKS?
A commitment to cyber hygiene and best practices is critical to protecting your networks. Here are some questions you may want to ask of your organization to help prevent ransomware attacks:

1. Backups: Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. Risk Analysis: Have we conducted a cybersecurity risk analysis of the organization?
3. Staff Training: Have we trained staff on cybersecurity best practices?
4. Vulnerability Patching: Have we implemented appropriate patching of known system vulnerabilities?
5. Application Whitelisting: Do we allow only approved programs to run on our networks?
6. Incident Response: Do we have an incident response plan and have we exercised it?
7. Business Continuity: Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. Penetration Testing: Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

CONTACT LAW ENFORCEMENT IMMEDIATELY. We encourage you to contact a local FBI or US&S field office immediately to report a ransomware event and request assistance.

There are serious risks to consider before paying the ransom. We understand that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. As you contemplate this choice, consider the following risks:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model.

"We do not encourage paying a ransom.

As you contemplate this choice, consider the following risks:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model."

Morgan Lewis

https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_OnePager_and_Technical_Document-FINAL.pdf

Second Ransomware Demand

Hackers demand ransom payment from Kansas Heart Hospital for files

WICHITA, Kan. A hospital held hostage by hackers and denied access to its files until it pays a ransom. It is a crime that's been committed across the country, and here in Kansas it's no exception. It's called "ransomware" — hackers "hack your computer" and hold the data until you pay.

The Kansas Heart Hospital is the latest victim of this attack. The hospital's president, Dr. Greg Druk, says the hackers never gave access to patient information, but the attack did cause serious problems.

Kansas Heart Hospital had a cyber attack (also been mentioned as being "Druk said." "We suspect, an attack on other parts of the country, this was an offshoot operation," he said.

Druk says hackers holding hospital files hostage is very common.

"Upwards of 40% of hospitals have received some kind of cyber attack. And multiple hospitals had additional attacks," he said.

About how "Wichitans," a hospital employee had access to files.

- Hackers "locked up the files, refusing to give back access unless the hospital paid up."
- "I'm not at liberty because it's an ongoing investigation, to say the actual exact amount. A small amount was made," the hospital president said.
- After payment, "the hackers didn't return full access to the files" and "**demanded another ransom.**"
- "The hospital says, it will not pay again."

Morgan Lewis

<http://www.kwch.com/content/news/Hackers-demand-ransom-payment-from-Kansas-Heart-Hospital-380342701.html>

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."

Morgan Lewis

https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

51



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments¹

Date: **October 1, 2020**

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 as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. This advisory describes these sanctions risks and provides information for contacting relevant U.S. government agencies, including OFAC, if there is a reason to believe the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.²

Ransomware Notification

- **Is it a HIPAA breach if ransomware infects a covered entity's or business associate's computer system?**
 - "Whether or not the presence of ransomware would be a breach under the HIPAA Rules is a fact-specific determination...."
 - "Unless the covered entity or business associate can demonstrate that there is a "...low probability that the PHI has been compromised," based on the factors set forth in the Breach Notification Rule, a breach of PHI is **presumed to have occurred.**"

Morgan Lewis <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>

52

FACT SHEET: Ransomware and HIPAA

A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015).¹ Ransomware exploits human and technical weaknesses to gain access to an organization's technical infrastructure in order to deny the organization access to its own data by encrypting that data. However, there are measures known to be effective to prevent the introduction of ransomware and to recover from a ransomware attack. This document describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack.

1. What is ransomware?

Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy ransomware that also destroys or exfiltrates² data, or ransomware in conjunction with other malware that does so.

Key Issues

- Initial cyber investigation under attorney client privilege
 - Determine scope of attack
 - Isolate and secure network
- Forensic analysis of incident
 - Forensic specialist with experience to address particular cyber incident
 - Facts make a difference
 - Functionality of malware
- Incident Response Plan
- Business continuity plans ready and tested
- Demand for payment
 - Usually bitcoin
- Whether and when to contact law enforcement
- Legal guidance and consequences
- Response to government inquiries and enforcement actions
- Mitigation steps



Morgan Lewis

53

Ransomware Protection and Prevention

- Offline, Secure and Regular Backups (different forms of media)
- Updated Operating Systems, Software, Patches and Antivirus Software
- Remote Desktop Protocol Connections limited to those needed
- Monitoring and Intrusion Detection
- Physical and logical segmentation and separate
 - Prevent Lateral Movement (e.g., by business units)
- Training and Awareness (Prevention)
 - Avoid Links or Phishing Schemes with Attachments Containing Malware
 - Strong Passwords, MFA
- Global awareness on new ransomware variants and trends
- Incident Response Plan that is tested
- Business Continuity Plan ready to implement

Morgan Lewis

54

DATA PRIVACY AND PROTECTION BOOT CAMP

EARLY CONSIDERATION OF THE SCOPE OF THE ATTORNEY CLIENT PRIVILEGE ON DATA BREACH CASES

Two Scenarios

SCENARIO ONE

Prepare in advance now

- Tailored cybersecurity program
- Consider new, emerging legal standards
- **Legal guidance under attorney client privilege**
- Risk assessments, compliance issues
- Training
- Safeguard third party vendor information
- Address unique issues, consider safeguards

• LATER CYBER INCIDENT

- **Cyber investigation under attorney client privilege / work product doctrine**
 - Determine scope of incident
- Reputational harm
- Assess litigation exposure and risk
- Federal and state regulators

Morgan Lewis

SCENARIO TWO

Respond to incident now

• CYBER INCIDENT

- Ransomware, business email compromise, phishing scheme, account takeover, etc.
- **Cyber investigation under attorney client privilege / work product doctrine**
 - Determine scope of incident
 - Are prior vulnerabilities exposed?
 - Failure to patch
 - Lack of controls to prevent incident
 - Training issues (e.g., recurring phishing)
- Reputational harm
- Training
- Assess litigation exposure
- Federal and state regulators

56

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

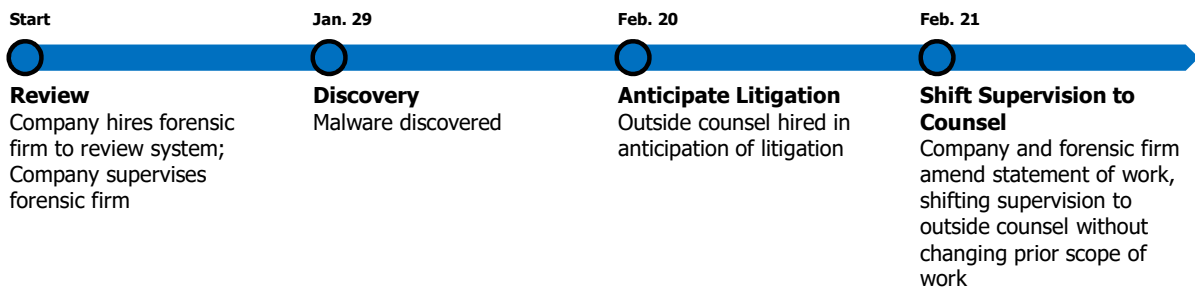
- Work prepared in anticipation of litigation by attorneys or representatives
 - Mental impressions, conclusions, legal theories, opinions.
- Fed. R. Civ. P. 26(b)(3)(A)(ii)
 - May be disclosed if “party shows that it has substantial need for the materials to prepare its case and cannot, without undue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

Morgan Lewis

57

Attorney Client Privilege Common Facts

Forensic Report:



Morgan Lewis

58

Consider Range of Incident Communications

- Incident Response Team
- Forensics Specialist
 - Analysis
 - Remediation
- Board of Directors
 - Discussion about legal advice?
 - Or updates concerning incident?
- Management
- Public Relations Team
- Auditor
- Customer and Business Relations
- Other Third Parties?



Morgan Lewis

59

Capital One Case (May 26, 2020)

LAW360

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.

Morgan Lewis

LAW360

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.

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

60

Capital One Case

Forensic Report:

Nov. 30, 2015



Master Services Agreement & SOW
"[Q]uickly respond to a cybersecurity incident should one occur."

Jan., Feb. 2019



SOW & Retainer
"Business Critical" expense for incident response services if necessary including "computer security incident response support; digital forensics, log, and malware analysis support; and incident remediation assistance" and detailed report.

March 2019



Data Breach
Incident response services commence.

July 2019



Counsel Retained

- July 20, 2019, counsel retained.
- July 24, letter agreement with forensic firm for "same service" under "same terms as the SOW and MSA" at the direction of counsel.
- July 29, public announcement on data breach.
- July 30, first lawsuit followed by others.

Morgan Lewis

61

Privilege / Work Product Considerations

- Ensure Attorney Client Privilege / Work Product Doctrine is properly in place before services commence.
 - Fact specific inquiry.
 - Engagement "at the direction of counsel".
 - The burden ultimately is on the proponent of the privilege and work product.
 - Can you survive a challenge?
 - What record is established to support the privilege and work product doctrine?
- Challenge may come many months later; address scope at the front end.
 - Confirm legal guidance and role and anticipation of litigation.
 - Mark communications and documents
 - Avoid business purposes.
- Carefully consider what information is covered and what documents are created.
 - What is the purpose of the report? (e.g., expert testimony, legal guidance, etc.)
 - Consider the nature and scope of the forensic work. (e.g., determine exfiltration, access, acquisition, etc.)
 - ACP / WP applies on a document-by-document basis.

Confidential Document
Attorney-Client Privilege









Morgan Lewis

62

DATA PRIVACY AND PROTECTION BOOT CAMP

ANTICIPATING AND ADDRESSING REGULATORY ENFORCEMENT ISSUES

**Cybersecurity Landscape
Growing Patchwork of Laws – Many Regulators**

	<p>Data Breach Notification Statutes</p> <ul style="list-style-type: none"> • First: California Data Breach Notification Statute (2002) • Now: 54 US Jurisdictions (DC, Puerto Rico, Guam and Virgin Islands) 		<p>Federal Trade Commission</p> <ul style="list-style-type: none"> • Section 5: “unfair or deceptive acts or practices in or affecting commerce”
	<p>California Consumer Privacy Act of 2018</p>		<p>Securities and Exchange Commission (SEC) Statement and Guidance on Public Company Cybersecurity Disclosures</p>
	<p>Special Focus Statutes: South Carolina Insurance Data Security Act (H. 4655)</p>		<p>Health Insurance Portability and Accountability Act (HIPAA) of 1996</p>
	<p>New York Department of Financial Services (NYDFS) Cybersecurity Rule (March 2017)</p>		<p>European Union (EU) General Data Protection Regulation (GDPR) (May 2018)</p>

Two Scenarios

SCENARIO ONE

Prepare in advance now

- Tailored cybersecurity program
- Consider new, emerging legal standards
- Legal guidance under attorney client privilege
- Risk assessments, compliance issues
- Training
- Safeguard third party vendor information
- Address unique issues, consider safeguards

• LATER CYBER INCIDENT

- Cyber investigation under attorney client privilege / work product doctrine
 - Determine scope of incident
- Reputational harm
- Assess litigation exposure and risk
- **Federal and state regulators**

Morgan Lewis

SCENARIO TWO

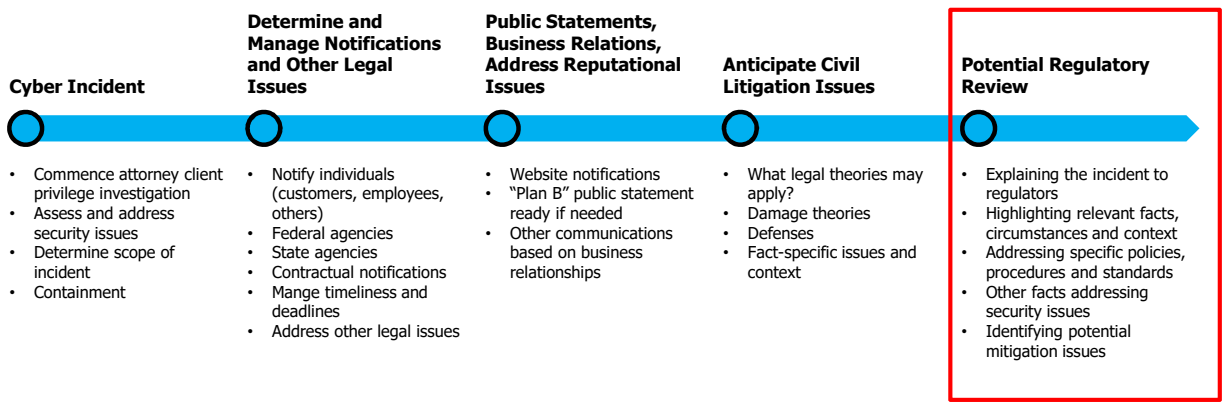
Respond to incident now

• CYBER INCIDENT

- Ransomware, business email compromise, phishing scheme, account takeover, etc.
- Cyber investigation under attorney client privilege / work product doctrine
 - Determine scope of incident
 - Are prior vulnerabilities exposed?
 - Failure to patch
 - Lack of controls to prevent incident
 - Training issues (e.g., recurring phishing)
- Reputational harm
- Training
- Assess litigation exposure
- **Federal and state regulators**

65

Incident Response Timeline Key Phases



Morgan Lewis

66

Regulatory Issues

- Preliminary regulator questions
- Government agency enforcement actions key consequences and penalties
- Trend to reasonable cybersecurity standards
- Specific cybersecurity standards and requirements
- Consider START approach

Morgan Lewis

67

Preliminary Regulator Questions

- How did incident occur?
 - Phishing
 - Ransomware
 - Business email compromise
 - What context and facts?
- Focus on company:
 - What was company's role?
 - Was reasonable cybersecurity in place?
 - What controls and policies?
 - Review governance
 - Training
 - What could company have done to prevent incident, if at all?

Morgan Lewis



Preliminary Regulator Questions

- Scope of incident
 - Harm to others
 - What type of damages?
 - Mitigation
- Was any notification timely?
 - Were notification requirements met?
- What other issues may be exposed during review process?
 - Finding other cybersecurity issues
- Other specific regulatory requirements for the jurisdiction
 - NYDFS Cybersecurity Rule
 - Written Information Security Program



Morgan Lewis

69

Regulatory Issues

- Preliminary regulator questions
- **Government agency enforcement actions key consequences and penalties**
- Trend to reasonable cybersecurity standards
- Specific standards and requirements
- Consider START approach

Morgan Lewis

70

Recent Office for Civil Rights HHS Enforcement

- Phishing email installed malware providing access to network
- APT undetected for nearly 9 months
- Disclosure of 10.4 million PHI
 - Names, addresses, dates of birth, email addresses, Social Security numbers, bank account information, and health plan clinical information
- HHS concluded “**systemic noncompliance** with the HIPAA Rules including failure to conduct an enterprise-wide risk analysis, and failures to implement risk management, and audit controls”

HHS.gov

U.S. Department of Health & Human Services

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

Premiera 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 individuals' protected health information including their names, addresses, dates of birth, email addresses, Social Security numbers, bank account information, and health plan clinical information.

Morgan Lewis <https://www.hhs.gov/about/news/2020/09/25/health-insurer-pays-6-85-million-settle-data-breach-affecting-over-10-4-million-people.html>

71

Government Agency Enforcement Actions Key Consequences and Penalties



Morgan Lewis <https://www.law360.com/articles/1251633/navigating-new-federal-state-data-privacy-compliance-duties>

72

NYDFS: Equifax (June 27, 2018)

CONSENT ORDER

The purpose of this Consent Order (ORDER) is to require certain corrective actions in response to criticisms noted in the Multi-State Regulatory Agencies' Examination that are outlined below. The following terms are used in this ORDER:

Company: Equifax Inc.
Board: The Board of Directors of Equifax Inc.
Multi-State Regulatory Agencies: Includes the Alabama State Banking Department, California Department of Business Oversight, Georgia Department of Banking and Finance, Maine Bureau of Consumer Credit Protection, Massachusetts Division of Banks, New York State Department of Financial Services, North Carolina Office of Commissioner of Banks, and Texas Department of Banking.

The Company, by and through its duly elected and acting Board, has consented to the issuance of this ORDER without admitting or denying any charges of unsafe or unsound information security practices.

NOW, THEREFORE, The Multi-State Regulatory Agencies, acting under statutory authority and with consent of the Company, hereby order that the undersigned representatives take, on behalf of the Company, the following steps in furtherance of alleviating the regulatory concerns of the Multi-State Regulatory Agencies.

INFORMATION SECURITY

- 1) Within 90 days from the effective date of this ORDER, the Board shall review and approve the written risk assessment that identifies:
 - (a) foreseeable threats and vulnerabilities to the confidentiality of personally identifiable information (PII);
 - (b) the likelihood of threats;
 - (c) the potential damage to the Company's business operations; and
 - (d) the safeguards and mitigating controls that address each threat and vulnerability.

- **Written Risk Assessment :** Board review and approval
- **Audit:** Improve the oversight of the audit function.
- **Board and Management Oversight:** Improve the oversight of the Information Security Program:
 - Approve Written Information Security Program and Information Security Policy annually
 - Review management annual report on the adequacy of the Security Program
 - Enhance the level of detail within the Technology Committee and board minutes, documenting relevant internal management reports
 - Review and approve IT and information security policies and ensure they are up-to-date
 - Security Incident Handling Procedure Guide includes up-to-date incident-related procedures and clarifies the roles and relationships of the groups involved in the incident response.

Morgan Lewis <https://www.dfs.ny.gov/about/ea/ea180627.pdf>

NYDFS: Equifax (June 27, 2018)

CONSENT ORDER

The purpose of this Consent Order (ORDER) is to require certain corrective actions in response to criticisms noted in the Multi-State Regulatory Agencies' Examination that are outlined below. The following terms are used in this ORDER:

Company: Equifax Inc.
Board: The Board of Directors of Equifax Inc.
Multi-State Regulatory Agencies: Includes the Alabama State Banking Department, California Department of Business Oversight, Georgia Department of Banking and Finance, Maine Bureau of Consumer Credit Protection, Massachusetts Division of Banks, New York State Department of Financial Services, North Carolina Office of Commissioner of Banks, and Texas Department of Banking.

The Company, by and through its duly elected and acting Board, has consented to the issuance of this ORDER without admitting or denying any charges of unsafe or unsound information security practices.

NOW, THEREFORE, The Multi-State Regulatory Agencies, acting under statutory authority and with consent of the Company, hereby order that the undersigned representatives take, on behalf of the Company, the following steps in furtherance of alleviating the regulatory concerns of the Multi-State Regulatory Agencies.

INFORMATION SECURITY

- 1) Within 90 days from the effective date of this ORDER, the Board shall review and approve the written risk assessment that identifies:
 - (a) foreseeable threats and vulnerabilities to the confidentiality of personally identifiable information (PII);
 - (b) the likelihood of threats;
 - (c) the potential damage to the Company's business operations; and
 - (d) the safeguards and mitigating controls that address each threat and vulnerability.

- **Vendor Management:** Improve oversight and documentation of critical vendors and ensure that sufficient controls are developed to safeguard information.
- **Patch Management:** Improve standards and controls for supporting the patch management function.
- **Information Technology Operations:** Enhance oversight of IT operations concerning disaster recovery and business continuity function.

Alabama State Banking Department, the California Department of Business Oversight, Georgia Department of Banking and Finance, Maine Bureau of Consumer Credit Protection, Massachusetts Division of Banks, New York Department of Financial Services, North Carolina Office of Commissioner of Banks, and Texas Department of Banking.

Morgan Lewis <https://www.dfs.ny.gov/about/ea/ea180627.pdf>

Regulatory Issues

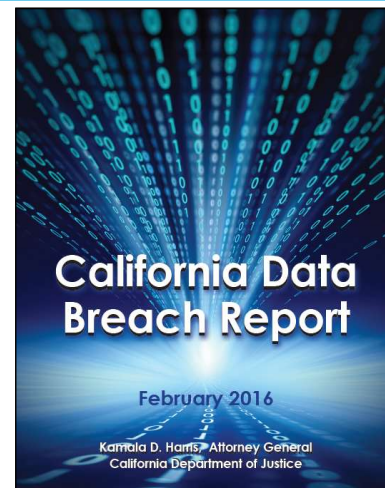
- Preliminary regulator questions
- Government agency enforcement actions key consequences and penalties
- **Trend to reasonable cybersecurity standards**
- Specific cybersecurity standards and requirements
- Consider START approach

Morgan Lewis

75

Government Perspective and Premise

- “Securing data is no doubt challenging, with sophisticated cyber criminals – including some nation states – waging an escalating battle.”
- “But many of the **breaches reported to us could have been prevented by taking reasonable security measures**, and an organization that voluntarily chooses to collect and retain personal information takes on a **legal obligation to adopt appropriate security controls.**”
- Other federal and state agencies share this view
 - SEC, FTC, Other State AGs



Morgan Lewis

<https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>

76

SEC Investigative Report (Oct. 16, 2018)



SEC Investigative Report

- Nine public companies were victims of cyber-related frauds
- Issue: Whether these companies violated federal securities laws by failing to have a sufficient system of internal accounting controls
- Public companies could still be liable for federal securities violations if they do not have sufficient internal accounting controls that specifically take into account these new threats
- Focus on internal accounting controls that reasonably safeguard company and investor assets from cyber-related frauds
 - "Devise and maintain a system of **internal accounting controls sufficient to provide reasonable assurances** that (i) transactions are executed in accordance with management's general or specific authorization" and that "(iii) access to assets is permitted only in accordance with management's general or specific authorization." Section 13(b)(2)(B)(i) and (iii) of the Securities Exchange Act

Press Release

SEC Investigative Report: Public Companies Should Consider Cyber Threats When Implementing Internal Accounting Controls

FOR IMMEDIATE RELEASE
2018-236

Washington D.C., Oct. 16, 2018 — The Securities and Exchange Commission today issued an investigative report cautioning that public companies should consider cyber threats when implementing internal accounting controls. The report is based on the SEC Enforcement Division's investigations of nine public companies that fell victim to cyber fraud, losing millions of dollars in the process.

The SEC's investigations focused on "business email compromises" (BECs) in which perpetrators posed as company executives or vendors and used emails to dupe company personnel into sending large sums to bank accounts controlled by the perpetrators. The frauds in some instances lasted months and often were detected only after intervention by law enforcement or other third parties. Each of the companies lost at least \$1 million, two lost more than \$30 million, and one lost more than \$45 million. In total, the nine companies wired nearly \$100 million as a result of the frauds, most of which was unrecoverable. No charges were brought against the companies or their personnel.

Morgan Lewis

<https://www.sec.gov/news/press-release/2018-236> **77**

"Reasonable and Appropriate" Procedures



"[F]ailed to implement **reasonable and appropriate procedures** for handling personal information about customers and employees, in violation of federal laws.... did **not implement reasonable policies and procedures** to dispose securely of personal information, did **not adequately train employees**, did **not use reasonable measures** to assess compliance with its policies and procedures for disposing of personal information, and **did not employ a reasonable process** for discovering and remedying risks to personal information."

Morgan Lewis

<https://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial> **78**

Uses California Customer Records Act



- "A business that owns, licenses, or maintains **personal information*** about a California resident shall implement and maintain **reasonable security procedures and practices** appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."
 - Enacted 2004 (AB 1950)
 - Note: Comparable reasonable security statutes in about half the states.

Morgan Lewis

- * **"Personal information"**
 - Not encrypted or redacted
 - (A) First name or first initial and his or her last name plus another data element
 - Social security number
 - Driver's license number or California identification card number
 - Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
 - Medical information
 - Health insurance information
 - (B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

[Cal. Civil Code § 1798.81.5] **79**

New York SHIELD Act



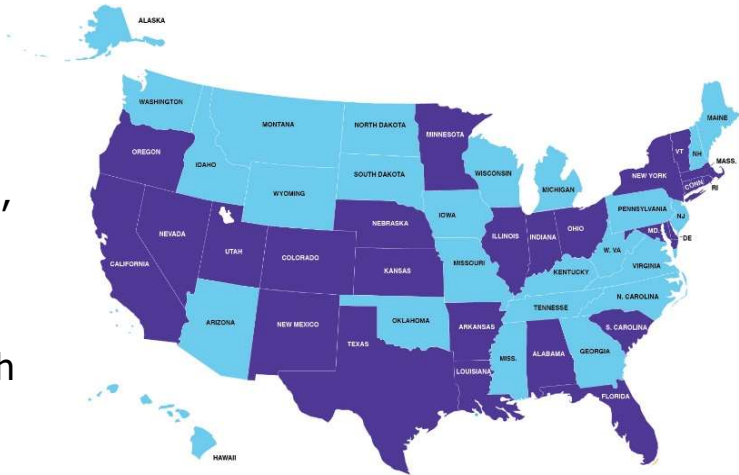
- New reasonable security requirement for companies to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of" private information of New York residents.
- Effective March 23, 2020.
- Reasonable safeguards include
 - Focus: Administrative, Technical and Physical Safeguard
 - Risk assessments, employee training, selecting vendors capable of maintaining appropriate safeguards and implementing contractual obligations for those vendors, and disposal of private information within a reasonable time.

Morgan Lewis

80

States with Reasonable Security Standards

- Alabama, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Illinois, Indiana, Kansas, Louisiana, Maryland, Massachusetts, Minnesota, Nebraska, Nevada, New Mexico, New York, Ohio, Oregon, Rhode Island, South Carolina, Texas, Utah, and Vermont

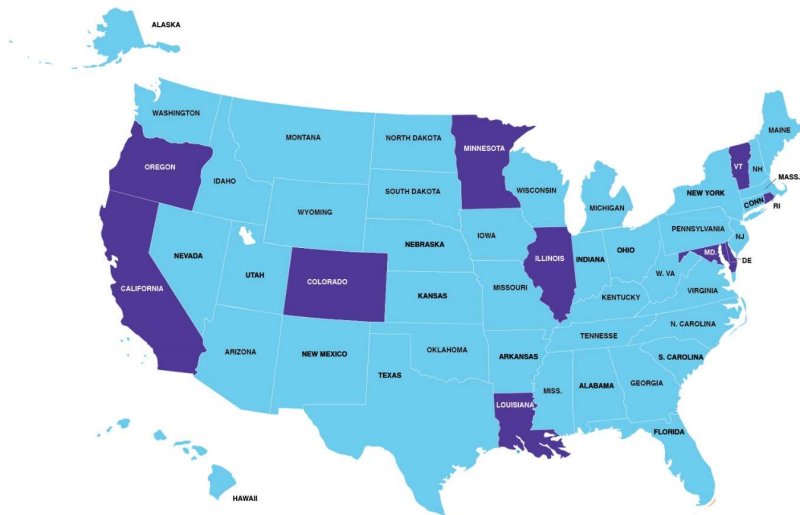


Morgan Lewis

81

Other States with a Private Right of Action

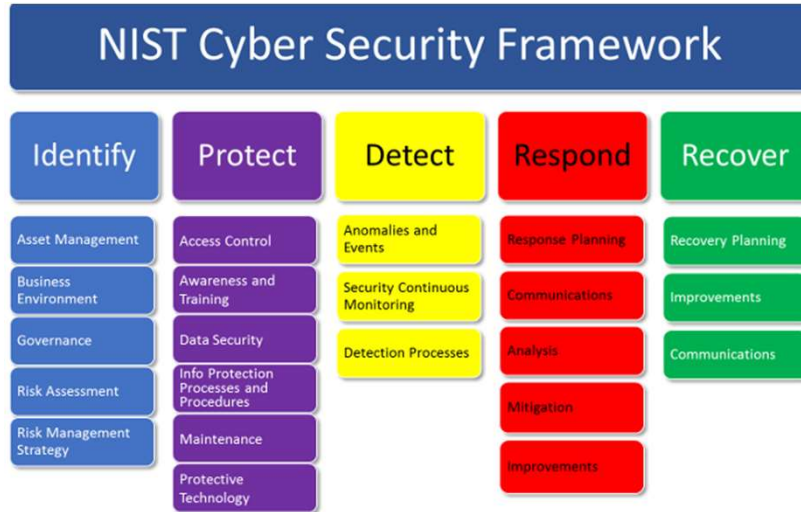
- California, Colorado, Delaware, Illinois, Louisiana, Maryland, Minnesota, Oregon, Rhode Island and Vermont.



Morgan Lewis

82

NIST Cyber Security Framework



Morgan Lewis

83

CIS Critical Security Controls

Basic CIS Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational CIS Controls

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/cis-controls-list/>

Morgan Lewis

84

Rule 30 of Regulation S-P (the "Safeguard Rule")



- Requires registered broker-dealers, investment advisers and investment companies to establish **written policies and procedures** that are reasonably designed to **safeguard customer information**.
- The Safeguard Rule requires firms to:
 - address the administrative, technical, and physical safeguards for the protection of nonpublic personal information;
 - insure the security and confidentiality of customer records and information;
 - protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
 - protect against any unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer

Morgan Lewis

Regulation S-P, Privacy of Consumer Financial Information. 17 C.F.R. Part 248; SEC Release No. IC-24543 (Jun. 22, 2000)

85

SEC Enforcement Action: Safeguard Rule



R.T. Jones Failed to Adopt Written Policies and Procedures Reasonably Designed to Safeguard Customer Information

7. The Safeguards Rule, which the Commission adopted in 2000, requires that every investment adviser registered with the Commission adopt policies and procedures reasonably designed to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. The Commission adopted amendments to the Safeguards Rule, effective January 2005, to require that the policies and procedures adopted thereunder be in writing.

8. During the relevant period, R.T. Jones maintained client PII on its third party-hosted web server. However, the firm failed to adopt any written policies and procedures reasonably designed to safeguard its clients' PII as required by the Safeguards Rule. R.T. Jones's policies and procedures for protecting its clients' information did not include, for example: conducting periodic risk assessments, employing a firewall to protect the web server containing client PII, encrypting client PII stored on that server, or establishing procedures for responding to a cybersecurity incident. Taken as a whole, R.T. Jones's policies and procedures for protecting customer records and information were not reasonable to safeguard customer information.

- Reg S-P violated by failure to safeguard customer data on a third-party hosted web server that was hacked
- Failure to adopt written policies and procedures reasonably designed to safeguard personal information of "approximately 100,000 individuals, including thousands of the firm's clients."
- Failure "to conduct periodic risk assessments, implement a firewall, encrypt PII stored on its server, or maintain a response plan for cybersecurity incidents."

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

86

Safeguarding Customer Data



- Failure to safeguard customer data from cyber-breaches in violation of Reg S-P stemming from a registered broker-dealer and investment adviser employee transferring “the data regarding approximately 730,000 accounts to his personal server, which was ultimately hacked by third parties.”
- Firm “policies and procedures were not reasonable, however, for two internal web applications or ‘portals’ that allowed its employees to access customers’ confidential account information.” Failure to restrict access based on business need and failure to audit or test and monitor or analyze “access to and use of the portals.”

The screenshot shows the SEC's press release page for the case. The main heading is "SEC: Morgan Stanley Fined for Failure to Safeguard Customer Data". The release is dated June 8, 2016, and is categorized as an administrative proceeding. The subject is the failure of Morgan Stanley Smith Barney LLC to protect customer information, which was hacked and offered for sale online. The release includes the SEC's order instituting administrative proceedings against the firm.

Morgan Lewis

<https://www.sec.gov/news/pressrelease/2016-112.html>

87

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**

Morgan Lewis

88

NY Department of Financial Services Cybersecurity Regulation Requirement Phases



6 MONTHS

- Cybersecurity Program
- Cybersecurity Policy
- Appointment of CISO
- Access Privileges
- Performance of Risk Assessment
- Training of Cybersecurity Personnel
- Preparation/Update of Incident Response Plan
- Notification to Superintendent of Breach

1 YEAR

- CISO reports to Board of Directors
- Penetration Testing and Vulnerability Assessments
- Risk Assessments
- Multi-Factor Authentication
- Cybersecurity Awareness Training

18 MONTHS

- Audit Trails
- Application Security
- Data Retention
- Policies and Procedures to Monitor the Activity of Authorized Users
- Encryption

2 YEARS

- Third-Party Service Provider Security Policy

Effective: Mar. 1, 2017

First certification: Feb. 15, 2018

<https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dsfr500txt.pdf>

Morgan Lewis

89

Annual Compliance Certification



- Annual Certification Requirement
 - February 15 (Normally)
 - June 1, 2020 (COVID-19)
- “[C]ertifying that the Covered Entity is in compliance with the requirements set forth in this Part.”

APPENDIX A (Part 500)

(Covered Entity Name)
February 15, 20____

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of _____(date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended____(year for which Board Resolution or Compliance Finding is provided) complies with Part _____.

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name) _____ Date: _____

[DFS Portal Filing Instructions]

Morgan Lewis

[Section 500.17(b)]

90

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

Morgan Lewis

91

Insider Trading Prevention



SEC Requirement for Registered Entities:

- Required to establish, maintain, and enforce written policies reasonably designed to prevent securities law violations (including insider trading)
 - SEC has charged a number of broker-dealers, investment advisers, and hedge funds for violating these rules

SEC's 2018 Guidance for All Companies:

- They should "take steps to prevent directors and officers (and other corporate insiders. . .) from trading its securities until investors have been appropriately informed about the incident or risk"
- Companies should have "well designed policies and procedures to prevent trading on the basis of all types of material nonpublic information, including information relating to cybersecurity risks and incidents"

Morgan Lewis

92

Massachusetts WISP Since 2010

New 2019 reporting requirement to Massachusetts Attorney General and Office of Consumer Affairs and Business Regulation:

- Whether the company maintains a written information security program
- All the steps the company has taken or plans to take relating to the incident, including updating the written information security program

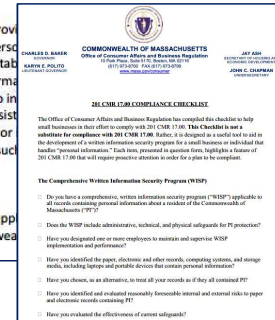
201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH

- Section:
 17.01: Purpose and Scope
 17.02: Definitions
 17.03: Duty to Protect and Standards for Protecting Personal Information
 17.04: Computer System Security Requirements
 17.05: Compliance Deadline

17.01 Purpose and Scope

(1) Purpose
 This regulation implements the provisions of Chapter 93A, Section 17B, of the Massachusetts General Laws, which requires that persons who own or license personal information in the Commonwealth take appropriate steps to safeguard the personal information in their possession, custody, or control. The objectives of this regulation are to ensure that the safeguarding of personal information is done in a manner that fully consists with the public interest and that the threats or hazards to the security or confidentiality of such information or unauthorized access to or use of such information do not result in a substantial inconvenience to any consumer.

(2) Scope
 The provisions of this regulation apply to any person who owns or licenses personal information about a resident of the Commonwealth.



to be met
 onwealth of
 ion with
 rds. The
 r
 ticipated
 st
 m or
 formation

Morgan Lewis <https://www.mass.gov/service-details/reporting-data-breaches-to-the-attorney-generals-office>

New York SHIELD ACT



DATA SECURITY PROGRAM

Reasonable Administrative Safeguards

- One or more employees to coordinate the security program
- Identifies reasonably foreseeable internal and external risks
- Assesses the sufficiency of safeguards in place to control the identified risks
- Trains and manages employees in the security program practices and procedures
- Selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and
- Adjusts the security program in light of business changes or new circumstances

Morgan Lewis

N.Y. Gen. Bus. Law § 899-bb 94

New York SHIELD ACT



DATA SECURITY PROGRAM

Reasonable Technical Safeguards

- Assesses risks in network and software design
- Assesses risks in information processing, transmission and storage
- Detects, prevents and responds to attacks or system failures
- Regularly tests and monitors the effectiveness of key controls, systems and procedures

Morgan Lewis

N.Y. Gen. Bus. Law § 899-bb **95**

New York SHIELD ACT



DATA SECURITY PROGRAM

Reasonable Physical Safeguards

- Assesses risks of information storage and disposal
- Detects, prevents and responds to intrusions
- Protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information

Morgan Lewis

N.Y. Gen. Bus. Law § 899-bb **96**

Regulatory Issues

- Preliminary regulator questions
- Key consequences and penalties from regulatory investigation and inquiry
- Trend to reasonable cybersecurity standards
- Specific cybersecurity standards and requirements
- **Consider START approach**

Morgan Lewis

97

Consider START Approach

- **S** Specific policies, procedures and standards tailored to the Co.
- **T** Testing (e.g., Penetration Testing, Vulnerability Assessments, etc.)
- **A** Assess policies and security
- **R** Reasonable Security and Red Flags, address them
- **T** Training

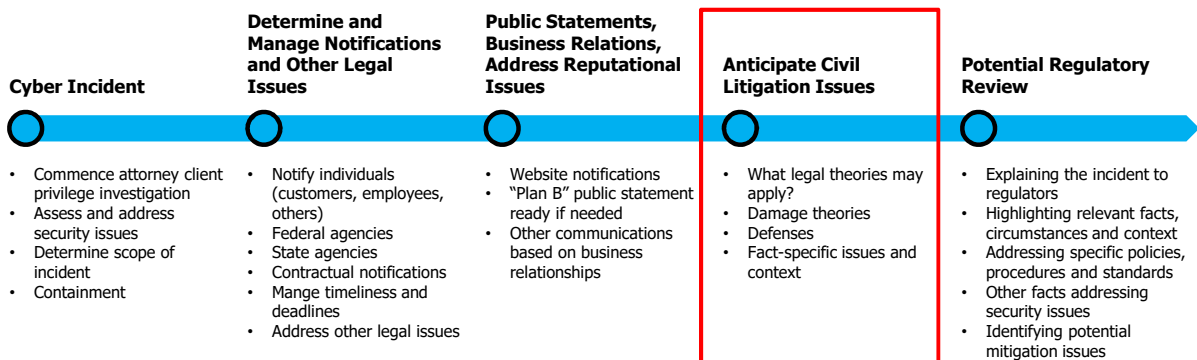
Morgan Lewis

98

DATA PRIVACY AND PROTECTION BOOT CAMP

LITIGATION DEFENSE ISSUES

Incident Response Timeline Key Phases



Anticipate Litigation Defenses

- What legal theories may apply to the facts?
 - Response will depend on possible claims
- What defenses are available?
- Damages or injury
 - Economic damages?
 - Statutory damages?
 - Containing and mitigating damages
- Fact-specific issues and context
 - Business email compromise
 - Ransomware
 - Third party vendor attack



Morgan Lewis

101

Article III Standing

- **Article III "Cases" and "Controversies"**
 - To meet the burden to establish standing, "The plaintiff must have
 - 1) suffered **an injury in fact**,
 - 2) that is fairly traceable to the challenged conduct of the defendant, and
 - 3) that is likely to be redressed by a favorable judicial decision."

Spokeo, 136 S.Ct. at 1547.
- **US Supreme Court**
 - *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540 (2016)
 - "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical"
 - *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013)
 - Holding lack of standing "because they cannot demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm."
 - "[W]e have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." n.5

Morgan Lewis

102

Private Rights of Action

State Statute Examples

North Carolina	South Carolina	Washington
<ul style="list-style-type: none"> "No private right of action may be brought by an individual for a violation of this section unless such individual is injured as a result of the violation." N.C. Gen. Stat. § 75-65(i). 	<ul style="list-style-type: none"> "A resident of this State who is injured by a violation of this section, in addition to and cumulative of all other rights and remedies available at law, may: (1) institute a civil action to recover damages in case of a willful and knowing violation; (2) institute a civil action that must be limited to actual damages resulting from a violation in case of a negligent violation of this section; (3) seek an injunction to enforce compliance; and (4) recover attorney's fees and court costs, if successful." S.C. Code Ann. § 39-1-90(G) 	<ul style="list-style-type: none"> "Any consumer injured by a violation of this section may institute a civil action to recover damages." Wash. Rev. Code § 19.255.010(13)(a).

Morgan Lewis



California Consumer Privacy Act



- Enacted June 28, 2018
- Effective Jan. 1, 2020
- New Privacy Rights
- **The right to know the categories of information** that a business collects, sells, or discloses about the consumer, and to whom information was sold or disclosed, as well as the right to prevent the business from selling or disclosing the consumer's personal information
- **The right to access a copy** of the "specific pieces of personal information that the business has collected about that consumer," to be delivered free of charge within 45 days in a portable manner by mail or electronically
- **The right to be forgotten** by requesting that a business delete, and direct any third-party service providers to delete, any personal information collected about the consumer
- **The right to opt out of the sale of personal information** to third parties by requiring a business to post a "clear and conspicuous link" titled "Do Not Sell My Personal Information" on its website's home page
- **The right to equal service and price**, which prohibits a business from discriminating against consumers who exercise their rights under the CCPA

AB 375 Signed - Californians for Consumer Privacy Applauds Successful Passage of Groundbreaking Legislation—WINS CALIFORNIA'S SOME OF THE STRONGEST CONSUMER PRIVACY PROTECTIONS IN THE WORLD.

June 28, 2018

Californians for Consumer Privacy Applauds Successful Passage of Groundbreaking Legislation—WINS CALIFORNIA'S SOME OF THE STRONGEST CONSUMER PRIVACY PROTECTIONS IN THE WORLD.

June 28, 2018

Successes, Calif. – Californians for Consumer Privacy applauds the Senate's final passage of the landmark passage of AB 375, the California Consumer Privacy Act, which will provide consumers with unprecedented control over their personal information. As a result of the bill's passage, Californians for Consumer Privacy will now welcome the California Consumer Privacy Act, through the California Secretary of State's office.

The passage of AB 375 has become law. This is a monumental achievement for consumers, with California leading the way in creating comprehensive consumer privacy legislation. The bill, introduced by Assemblymember Matt Hagman, Chairman of California's Consumer Privacy Act, and signed by Governor Jerry Brown and California Assemblymember Matt Hagman, will give consumers the right to know, access, delete, and opt out of the sale of their personal information. Californians for Consumer Privacy is proud to have led a group's battle against the forces that stand in the way of the most comprehensive consumer privacy legislation in the world. The bill, which will give consumers the right to know, access, delete, and opt out of the sale of their personal information, is a landmark achievement for consumers. It is the strong belief that these new California rights will have a positive impact on the world's privacy laws.




Morgan Lewis

<https://www.caprivacy.org/post/ab-375-signed-californians-for-consumer-privacy-applauds-successful-passage-of-groundbreaking-legislation>

104

California Consumer Privacy Act



- **Limited Consumer Private Right of Action**

- Individual consumer or class actions

- 1) Nonencrypted or nonredacted **personal information***
- 2) “subject to an unauthorized access and **exfiltration, theft, or disclosure**
- 3) as a result of the business’s violation of the duty to implement and maintain **reasonable security procedures and practices** appropriate to the nature of the information to protect the personal information”

Morgan Lewis

[Cal. Civil Code § § 1798.100 - 1798.199] **105**

California Consumer Privacy Act Statutory Damages Range



- Court imposes the **greater** of **statutory or actual damages**

- No actual harm is required

- **Statutory Damage Range**

- Statutory damages are “not less than” \$100 and “not greater than” \$750 “per consumer per incident”

- **Other Remedies**

- Injunctive or declaratory relief
- “Any other relief the court deems proper”

Statutory Damages Factors

- Nature and seriousness of the misconduct
- Number of violations
- Persistence of the misconduct
- Length of time over which the misconduct occurred
- Willfulness of the defendant’s misconduct
- Defendant’s assets, liabilities, and net worth
- Other “relevant circumstances presented by any of the parties”

Morgan Lewis

[Cal. Civil Code § 1798.150(a)(2)] **106**

CCPA New Era in Cybersecurity Litigation



- **Key Questions**

- What measures are in place to protect personal information?
- Can you redact and encrypt where possible?
- Can you demonstrate there are reasonable security procedures and practices appropriate to the nature of the information to protect the personal information?
- Are you prepared to respond to an incident?

Morgan Lewis

107

Reasonable Security Statute



- “A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain **reasonable security procedures and practices appropriate to the nature of the information**, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”
- Tailored to the circumstances.
 - Consider examples based on incident and vulnerabilities.

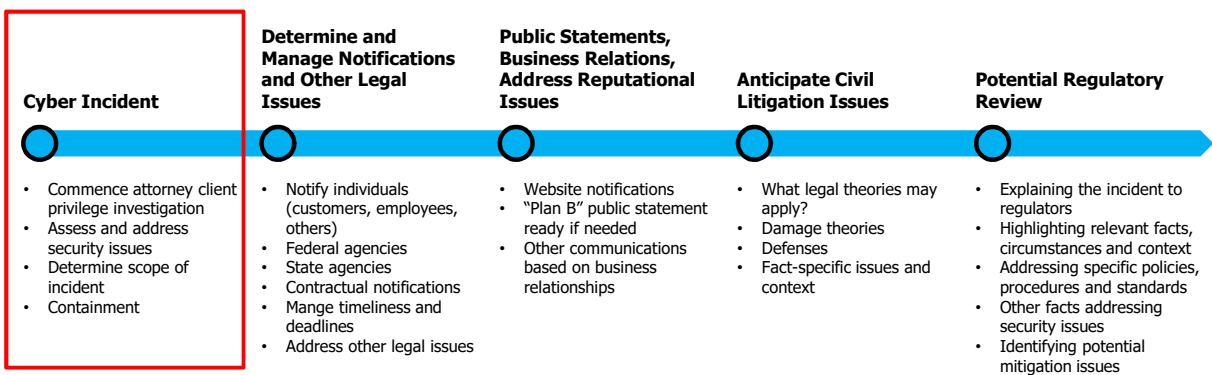
Morgan Lewis

[Cal. Civil Code § 1798.81.5] 108

DATA PRIVACY AND PROTECTION BOOT CAMP

INCIDENT RESPONSE

Incident Response Timeline Key Phases



Overseeing Internal Cyber Investigation



Initial call

- How was the cyber compromise / incident discovered?
- Launch Incident Response Plan



Determine Scope and Nature of Breach

- Did a "data breach" occur?
- Assess and address security issues
- Containment



Attorney Client Privilege

- Is the privilege effectively in place?



Assess Legal Consequences

- What notification obligations?
- What regulatory agencies?
- Was information accessed, acquired or exfiltrated?
- Which customers?
- What legal standards apply?



Coordination Issues / Coverage Obligations

Morgan Lewis



Determining the Scope of the Incident

- Did a "data breach" occur?
- When was cyber compromise/incident discovered?
- How was cyber compromise/incident discovered?
- How did cyber compromise/incident occur?
- When did the cyber incident occur?
 - Early assessments can be revised
- Who caused cyber compromise/incident?
 - Attribution analysis
- What security risks to contain?
- Which regulators?
- Managing notification issues
- Public relations
- Cyber Insurance coverage

Morgan Lewis

112

Incident Response Team



Morgan Lewis

113

Effective Public Relations Plan Prepared

- Addressing reputational damage issues
- Effectively communicating with customers
 - Will website and FAQ be appropriate?
- How quickly can you implement strategy to address and respond to customer questions and concerns?
- Whether to include credit monitoring
- Have “Plan B” PR Plan ready if needed



Morgan Lewis

114

Role of Attorney Client Privilege

- For the purpose of seeking or providing legal advice
 - Aids in the careful evaluation of any threats/intrusions and responsive action for investigation, legal obligations, and litigation
 - Early in the process
 - Risks if not properly used/protected
- Company counsel working with outside counsel
- Role of counsel with vendors
 - At the direction of counsel

Confidential Document
Attorney-Client Privilege

Morgan Lewis

115

DATA PRIVACY AND PROTECTION BOOT CAMP

MANAGING NOTIFICATION ISSUES

Disclosure Issues

- Timeliness
 - Managing different deadlines in different jurisdictions
- Notification triggers
 - Different definitions of breach and personal information
- Who to notify?
 - SEC, FTC
 - State Agencies
- Periodic Reports
 - Form 10-K
 - Management’s Discussion and Analysis (MD&A) section
 - Materiality Standard
 - Cybersecurity Risk Factors



Morgan Lewis

117

Differing Standards

- Vary by state and circumstances of the breach
 - Definition of “personal information”
 - Notification trigger
 - Notification to AG or other state agency
 - Manner of notification
 - Data format: hard copy files vs. electronic only
 - Safe harbor for encryption



Morgan Lewis

118

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.”

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

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

119

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

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

120

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.

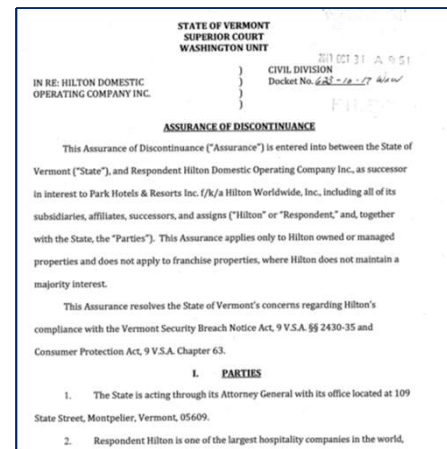
Morgan Lewis

<https://www.hhs.gov/about/news/2017/01/09/first-hipaa-enforcement-action-lack-timely-breach-notification-settles-475000.html>

121

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



In Re Hilton Domestic Operating Company, Inc.

Morgan Lewis

<http://ago.vermont.gov/blog/2017/10/31/vermont-attorney-general-resolves-security-breach-hilton-company-pay-300000-penalty/>

122

Notification Enforcement

- **June 15, 2017**
- NY Attorney General
 - **\$130,000**
- “Waiting **over a year** to provide notice is unacceptable.”
- Intruder downloaded records for 221,178 patients
 - Name, gender, date of birth, address, phone number, and medical insurance card information

A.G. Schneiderman Announces Settlement With Healthcare Services Company That Illegally Deferred Notice Of Breach Of More Than 220,000 Patient Records

Company Violated General Business Law That Requires Companies To Provide Notice Of A Breach As Soon As Possible

CoPilot Provider Support Services, Inc. Must Pay \$130,000 In Penalties And Reform Its Legal Compliance Program

Schneiderman: Healthcare Services Providers Have A Duty To Protect Patient Records As Securely As Possible And To Provide Notice When A Breach Occurs

NEW YORK – Attorney General Eric T. Schneiderman today announced a settlement with CoPilot Provider Support Services, Inc. (“CoPilot”), a New York corporation that provides support services to the health industry, after the company violated General Business Law by waiting over a year to provide notice of a data breach that exposed 221,178 patient records. CoPilot has agreed to pay

In Re CoPilot Provider Support Services, Inc.

Morgan Lewis

<https://ag.ny.gov/press-release/ag-schneiderman-announces-settlement-healthcare-services-company-illegally-deferred>

123

Defining “Breach”

California

- “[B]reach of the security of the system’ means **unauthorized acquisition** of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.”

Cal. Civ. Code § 1798.82(g)



Morgan Lewis

New York

- “Breach of the security of the system’ shall mean **unauthorized access to or acquisition of**, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business.”
- Note: “access to” added in 2019 under the SHIELD Act.



NY GBL § 899-aa(1)(c)

124

NY Factors



- **Accessed:**

Without valid authorization or by an unauthorized person:

- Indications that the information was:
 - viewed,
 - communicated with,
 - used, or
 - altered by a person.
- Among other factors

NY GBL § 899-aa(1)(c)

Morgan Lewis

- **Acquired:**

Indications that the information:

- (1) is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
- (2) has been downloaded or copied; or
- (3) was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.
- Among other factors

125

Has a “Breach” Occurred?

Variable	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

Morgan Lewis

126

Has a “Breach” Occurred?

Variable	State Examples
Risk of Harm	Alaska, Arkansas, Delaware, District of Columbia, Hawaii, Louisiana, Oregon, South Dakota, Washington
Material risk of harm to the resident	North Carolina, South Carolina
Reasonably likely to cause substantial harm to the individuals to whom the information relates	Alabama
No reasonable likelihood of financial harm ... has resulted or will result from the breach	Iowa
Material risk of identity theft or other fraud to the person or property of a resident of this state	Ohio, Wisconsin
Substantial risk of identity theft or fraud against a resident of the commonwealth	Massachusetts

Morgan Lewis

127

Compromising Personal Information

California

- “[B]reach of the security of the system’ means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of **personal information** maintained by the person or business.”

Cal. Civ. Code § 1798.82(g)



Morgan Lewis

New York

- “Breach of the security of the system’ shall mean unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of **private information** maintained by a business.”
- Note: “access to” added in 2019 under the SHIELD Act.

NY GBL § 899-aa(1)(c)



128

California Consumer Privacy Act



- Personal Information
 - **Broad definition**
 - PI includes “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a **particular consumer or household.**”
 - Including but not limited to:
 - “Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.”
 - Biometric information, Geolocation data, Professional or employment-related information.
 - “Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement.”
 - Inferences drawn from any of the information identified in this subdivision to create a **profile about a consumer** reflecting the consumer’s preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Morgan Lewis

129

Expanding Personal Information Data Elements



“Personal Information”

- Not encrypted or redacted
 - (A) First name or first initial and his or her last name plus another data element
 - Social security number
 - Driver’s license number or California identification card number
 - Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account

Morgan Lewis

[Cal. Civil Code § 1798.81.5] 130

Expanding Personal Information Data Elements



“Personal Information”

- Not encrypted or redacted
 - (A) First name or first initial and his or her last name plus another data element
 - o Social security number
 - o Driver’s license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
 - o Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account
 - o Medical information
 - o Health insurance information
 - o Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.
 - (B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

Morgan Lewis

[Cal. Civil Code § 1798.81.5] 131

Expanding Personal Information Data Elements

DATA ELEMENT	JURISDICTION
Birth certificate	South Dakota and Wyoming
Marriage certificate	Wyoming
Challenge questions	South Dakota
Date of birth	North Dakota, Texas, and Washington
Digital signature	North Carolina and North Dakota
DNA profile	Delaware and Wisconsin
Password	Georgia, Maine, North Carolina, and South Dakota
Financial account password	Alaska
Mother’s maiden name	North Dakota and Texas
Information or data collected through the use or operation of an automated license plate recognition system	California

<https://www.law360.com/articles/1210779/next-steps-for-cos-in-light-of-new-calif-privacy-laws>

Morgan Lewis

132

Expanding Personal Information Data Elements (cont.)

DATA ELEMENT	JURISDICTION
Employer identification card "in combination with any required security code, access code, or password"	North Dakota
State identification number	Alabama, Alaska, California, Connecticut, Georgia, Hawaii, Maine, Maryland, Oregon, Utah, Virginia, Washington, Wyoming, among other states
Student identification number	Colorado and Washington
Tribal identification number	Rhode Island, South Dakota, and Wyoming
Voter's identification	Puerto Rico
Security tokens used for data based authentication	Wyoming
Telecommunication for access device	Texas
Unique electronic identification number, address, or routing code	Texas
Work related evaluations	Puerto Rico

<https://www.law360.com/articles/1210779/next-steps-for-cos-in-light-of-new-calif-privacy-laws>

Morgan Lewis

133

Notification Issues

- What form of notice is required?
 - Email notification
 - Substitute notice
- What consequences and penalties?
 - Private right of action
 - Enforcement action
- Any there any industry-specific requirements?
 - Insurance (GA, KS, ME, MT)
 - Medical records (CA, LA)
 - Financial institutions (MN)
- Public utilities (MI)
- Who must be notified?
 - Customers
 - Public Agencies
- When must they be notified?
 - Reasonable notice
 - Delayed notification
- What data (PII) triggers notification?
 - What constitutes a "data breach"?
 - What exemptions?
 - Any reasonable likelihood of harm?

Morgan Lewis

134

Compare Notification Standards

California

• “The disclosure shall be made 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.” Cal. Civ. Code §1798.82(a).

Colorado

• “Notice shall be made in the most expedient time possible and **without unreasonable delay**, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to **determine the scope of the breach** and to restore the reasonable integrity of the computerized data system.” Colo. Rev. Stat. Ann. § 6-1-716(2)(a).



Morgan Lewis

135

Data Breach Notification Deadlines

Jurisdiction	Time for Notification
NY Department of Financial Services	72 hours
Florida, Washington	30 days
Alabama, Arizona, Arkansas, Illinois, Maryland, New Mexico, Ohio, Oregon, Rhode Island, Tennessee, Vermont, Wisconsin	45 days
Delaware, South Dakota, Texas	60 days
Connecticut	90 days

Morgan Lewis

136

Public Agency Notifications

Jurisdiction	Trigger
New Jersey	Division of State Police in the Department of Law and Public Safety For a single data breach and prior to notifying customers
New York	Attorney General State Police Division of Consumer Protection For a single data breach
Vermont	Attorney General "provide a preliminary description of the breach within 14 business days ... of the data collector's discovery of the security breach or when the data collector provides notice to consumers"
North Dakota, Oregon, South Dakota, Texas	Attorney General More than 250 residents
California, Colorado, Delaware, Florida, Illinois, Iowa, Rhode Island, Washington	Attorney General More than 500 residents

Morgan Lewis

137

California AG Notification

State of California Department of Justice

 **XAVIER BECERRA**
Attorney General

HOME ABOUT MEDIA CAREERS REGULATIONS RESOURCES PROGRAMS CONTACT

Search Data Security Breaches

Home / Privacy / Search Data Security Breaches

California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. (You can read the law here: California Civil Code s. 1798.29(a) for state agencies and California Civ. Code s. 1798.82(a) for businesses).

The law also requires that a sample copy of a breach notice sent to more than 500 California residents must be provided to the California Attorney General. Below is a list of those sample breach notices. (Note that in some cases the organization that sent the notice is not the one that experienced the breach. For example, a bank may notify of a credit card number breach that occurred not at the bank, but at a merchant.)

You can search by the name of the organization that sent the notice, or simply scroll through the list. To read a notice, click on the name of the organization in the list. Then click on the link titled "Sample Notification."

Organization Name: Date of Breach Range:

Organization Name	Date(s) of Breach	Reported Date ▼
RadNet, Inc.	07/18/2020	09/18/2020
FabFitFun, Inc.	04/26/2020, 05/22/2020	09/18/2020
Joslin Diabetes Center, Inc.	05/14/2020, 05/20/2020	09/18/2020
Rocklin Unified School District	n/a	09/18/2020
U.S. Bank, N.A.	07/30/2020	09/18/2020
Greenworks Tools	07/14/2019, 06/30/2020	09/17/2020
Episcopal Community Services	02/07/2020	09/17/2020
California Dialysis Management Services, Inc.	n/a	09/16/2020
BMB Associates	n/a	09/15/2020
Inova Health System	02/07/2020, 05/20/2020	09/15/2020
Baylor Genetics	09/24/2019, 11/14/2019	09/14/2020

Morgan Lewis

<https://oag.ca.gov/privacy/databreach/list>

138

Delaware AG Notification

Data Security Breaches:

Show 10 entries

Search:

Organization Name	Date(s) of Breach	Reported Date	Number of Potentially Affected Delaware Residents	Sample of Notice
Filters Fast LLC	7/15/19 - 7/10/20	8/27/20	1,492	View
Heifer Project International	5/14/20	8/21/20	1,225	View
Dave Inc.	6/23/20 - 7/1/20	8/21/20	7,299	View
Arbiter Sports	6/3/20 - 7/14/20	8/24/20	1,790	View
Westcor Land Title Insurance	1/10/20	8/25/20	1,114	View
Delaware Nature Society	5/20/20	8/21/20	624	View
Med-Delaware Imaging	1/24/20 - 1/30/20	7/14/20	8,784	View

Morgan Lewis <https://attorneygeneral.delaware.gov/fraud/cpu/securitybreachnotification/database/>

139

Texas AG Notification



Data Security Breach Report

(Be aware that information you submit on this form may become a public record and disclosed to third parties outside of the Office of the Texas Attorney General.)

PART A - IDENTIFYING INFORMATION OF ENTITY THAT EXPERIENCED THE BREACH

1. Name of Entity or Individual That Owns or Licenses the Data Subject to the Breach

* Entity or Individual Name

Entity or Individual Name is required

* Entity or Individual Address

* Entity or Individual City

* Entity or Individual State

* Entity or Individual Zip Code

Entity or Individual Website

2. Entity Type

* Entity Type

Morgan Lewis

<https://oagtx.force.com/datasecuritybreachreport/s/>

140

HIPAA Protected Health Information

**U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information**



Please Note: The Breach Notification Portal will be offline for maintenance from Fri Sep 25 10:00 PM EDT to Sat Sep 26 06:00 AM EDT. Any information being entered when the Portal is taken off-line will be lost.

Form Approved: OMB No. 0945-0001

Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

This site is available as we continuously work to make improvements to better serve the public. Should you need assistance with this site or have any questions, please email ocrprivacy@hhs.gov or call us toll-free: (800) 368-1019, TDD toll-free: (800) 537-7697.

To file a breach report, please enter information in the wizard pages below. A field with an asterisk (*) before it is a required field. [Download Sample Form \(PDF\)](#)

General Contact Breach Notice of Breach and Actions Taken Attestation Summary

General: Please supply the required general information for the breach.

* Report Type: What type of breach report are you filing? Initial Breach Report Addendum to Previous Report

Morgan Lewis https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true

141

Form of Notice



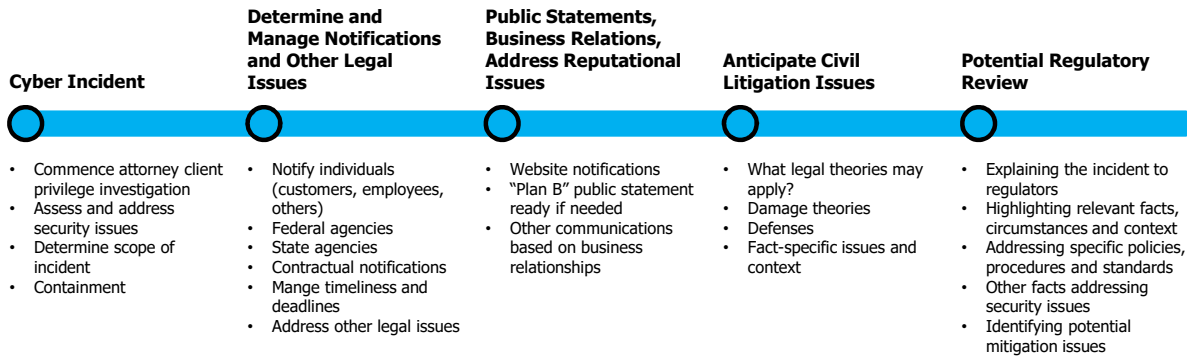
[NAME OF INSTITUTION / LOGO] _____ Date: (insert date)	
NOTICE OF DATA BREACH	
What Happened?	
What Information Was Involved?	
What We Are Doing.	
What You Can Do.	
Other Important Information. [insert other important information]	
For More Information.	Call [telephone number] or go to [Internet Web site]

- Some jurisdictions impose specific notice requirements
 - Plain language, titled "Notice of Data Breach"
 - Use "the following headings":
 - "What Happened"
 - "What Information Was Involved"
 - "What We Are Doing"
 - "What You Can Do"
 - "For More Information"
 - Format "designed to call attention to the nature and significance of the information"
 - Title and headings "clearly and conspicuously displayed"
 - Text "no smaller than 10-point type"

Morgan Lewis

142

Incident Response Timeline Key Phases



Morgan Lewis

143

DATA PRIVACY AND PROTECTION BOOT CAMP

BEST PRACTICES, NEXT STEPS

Two Scenarios

SCENARIO ONE

Prepare in advance now

- Tailored cybersecurity program
- Consider new, emerging legal standards
- Legal guidance under attorney client privilege
- Risk assessments, compliance issues
- Training
- Safeguard third party vendor information
- Address unique issues, consider safeguards

• LATER CYBER INCIDENT

- Cyber investigation under attorney client privilege / work product doctrine
 - Determine scope of incident
- Reputational harm
- Assess litigation exposure and risk
- Federal and state regulators

Morgan Lewis

SCENARIO TWO

Respond to incident now

• CYBER INCIDENT

- Ransomware, business email compromise, phishing scheme, account takeover, etc.
- Cyber investigation under attorney client privilege / work product doctrine
 - Determine scope of incident
 - Are prior vulnerabilities exposed?
 - Failure to patch
 - Lack of controls to prevent incident
 - Training issues (e.g., recurring phishing)
- Reputational harm
- Training
- Assess litigation exposure
- Federal and state regulators

145

The Best Offense is a Good Defense

• Governance

- Board cyber risk management
- Board oversight of corporate cybersecurity assessments, policies, and procedures
- Board reports
- Engagement with management
- Preparedness for cyber incident or attack
- Who is responsible for managing cyber program?

• Internal Controls, Policies, Procedures and Standards

- “[M]aintain[] comprehensive policies and procedures related to cybersecurity risks and incidents”
- Tailored to your cyber security needs
- Identify, Protect, Detect, Respond and Recover
- Review controls to prevent and detect cybercrime (Section 21(a) Report)
- Emerging Reasonable Cybersecurity Standard

Morgan Lewis

146

The Best Offense is a Good Defense

- **Risk Assessment and Management Program**

- Risk assessment process
- Identify and address cyber risks
- Safeguard key assets and information
- Testing and monitoring
- Patch management
- Network segmentation
- Assess controls policies, procedures and standards
- Address red flags

- **Access Management**

- Appropriate restrictions
- Password policies
- MFA
- Consider termination policies
- Monitoring access issues
- Insider threat issues

Morgan Lewis

147

The Best Offense is a Good Defense

- **Training**

- Prepared for cyber risks
- Prevention
- Assess effectiveness
- Responding to cyber risks
 - Phishing and Business Email Compromise

- **Third Party Vendors**

- Contractual obligations
- Notification requirements
- Security measures
- Encryption
- Independent audits

- **Address Disclosure Issues**

- Timeliness
- Periodic Reports
 - Form 10-K
 - Management's Discussion and Analysis (MD&A) section
- Materiality Standard
- Cybersecurity Risk Factors

- **Managing Cyber Incident**

- Multiple regulators
- Incident Response Plans
- Business Continuity Plans
- Test Plans for preparedness
- Attorney-Client Privilege

Morgan Lewis

148

The Best Offense is a Good Defense

- **Address Unique Jurisdiction Standards and Requirements**
 - Mandatory WISP
 - Disposal standards
 - NYDFS Annual Certification Requirement
- **Insider Trading**
 - Insider Trading Policies and Procedures Related to Cyber Risks and Incidents
 - “[P]olicies and procedures to prevent trading on the basis of all types of material nonpublic information, including information relating to cybersecurity risks and incidents.”
- **Legal Review**
 - Compliance standards and issues
 - Insider Trading Programs
 - Internal Control Programs

Morgan Lewis

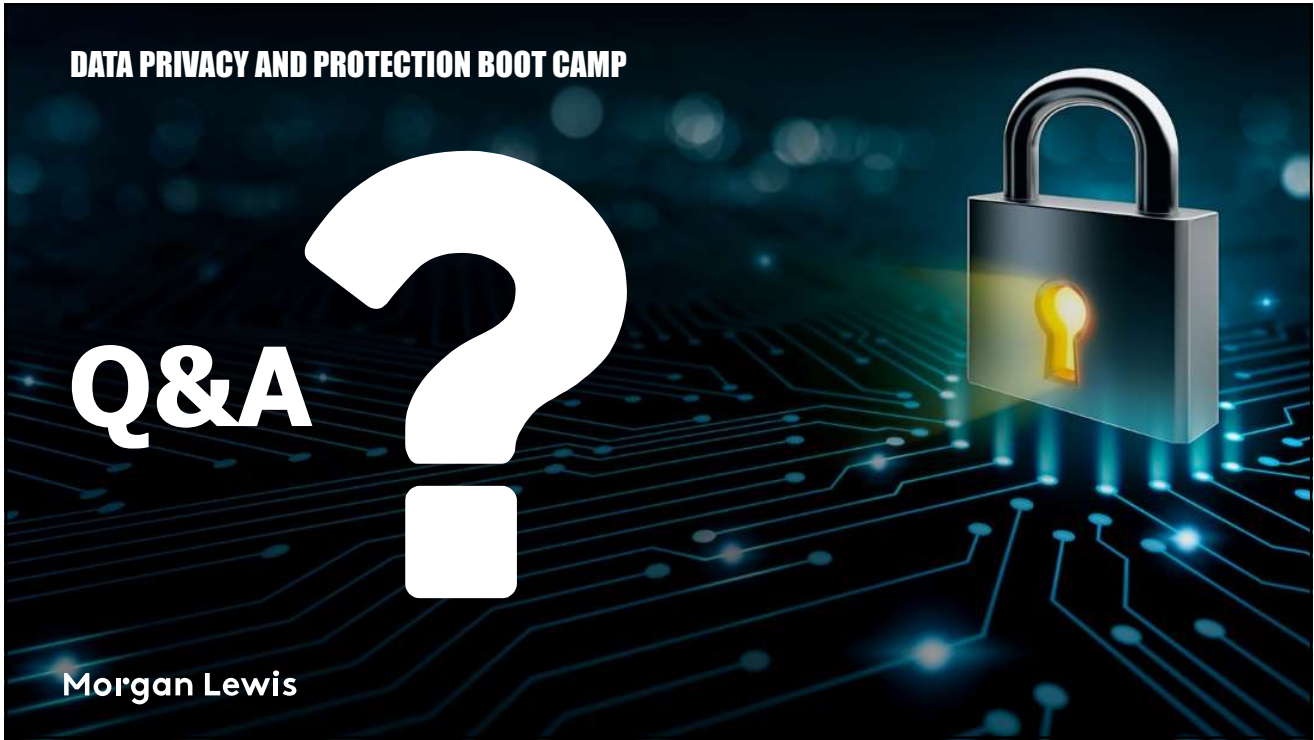
149

Prepared for All Cyber Incident Phases

- Assist 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.
- Assist on enforcement investigations and actions by federal and state regulators
- Assist on 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.

Morgan Lewis

150



Biography



Andrew J. Gray IV
Silicon Valley
+1.650.843.7575
andrew.gray@morganlewis.com

Serving as the leader of Morgan Lewis's semiconductor practice and as a member of the firm's fintech and technology practices, Andrew J. Gray IV concentrates his practice on intellectual property (IP) litigation and prosecution and on strategic IP counseling. Andrew advises both established companies and startups on Blockchain, cryptocurrency, computer, and Internet law issues, financing and transactional matters that involve technology firms, and the sale and licensing of technology. He represents clients in patent, trademark, copyright, and trade secret cases before state and federal trial and appellate courts throughout the United States, before the US Patent and Trademark Office's Patent Trial and Appeal Board, and before the US International Trade Commission.

Morgan Lewis

153

Biography



Mark L. Krotoski
Silicon Valley
+1.650.843.7212
Washington, DC
+1.202.739.5024
mark.krotoski@morganlewis.com

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 regulatory investigations, and coordinating with law enforcement on cybercrime issues.
- Variety of complex and novel cyber investigations and cases
 - 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, and as a cybercrime prosecutor in Silicon Valley, among other DOJ leadership positions.

Morgan Lewis

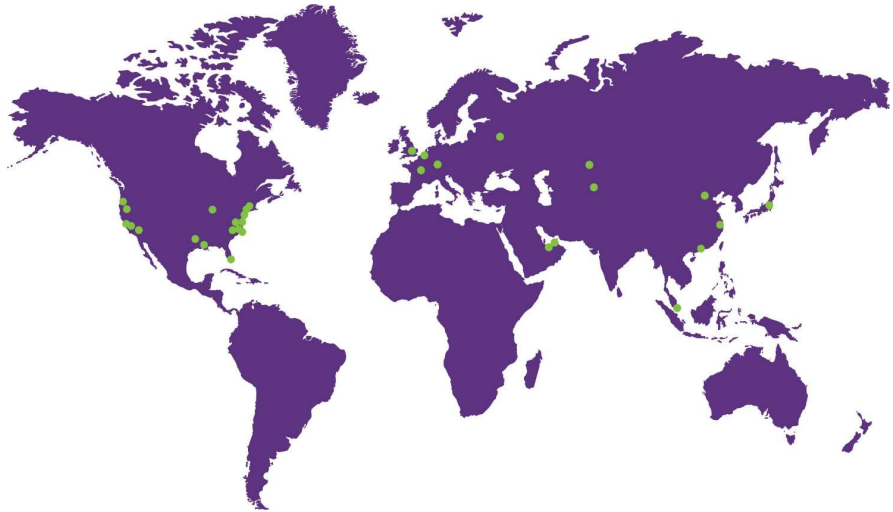
154

Our Global Reach

Africa	Latin America
Asia Pacific	Middle East
Europe	North America

Our Locations

Abu Dhabi	Moscow
Almaty	New York
Beijing*	Nur-Sultan
Boston	Orange County
Brussels	Paris
Century City	Philadelphia
Chicago	Pittsburgh
Dallas	Princeton
Dubai	San Francisco
Frankfurt	Shanghai*
Hartford	Silicon Valley
Hong Kong*	Singapore*
Houston	Tokyo
London	Washington, DC
Los Angeles	Wilmington
Miami	



*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.



**THANK
YOU**

© 2020 Morgan, Lewis & Bockius LLP
 © 2020 Morgan Lewis Stamford LLC
 © 2020 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 operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. 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.

