



**Morgan Lewis**

GLOBAL PUBLIC COMPANY ACADEMY

# CYBERSECURITY AND RELATED DEVELOPMENTS

**Mark Krotoski**

**Emily Drazan Chapman**

March 27, 2019

# Overview

- I. Cyber Threat Environment**
- II. Significant Costs and Consequences**
- III. Recent Case Study**
- IV. Heightened Regulatory Enforcement**
- V. Morgan Lewis Guidance and Services**
- VI. Q&A**

# Preliminary Note

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

# CYBER THREAT ENVIRONMENT

# Cyber Landscape and Risks



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

# Business Email Compromise



**Public Service Announcement**  
FEDERAL BUREAU OF INVESTIGATION

**Jul 12, 2018**  
Alert Number  
**I-071218-PSA**

Questions regarding this PSA should be directed to your local **FBI Field Office**.  
Local Field Office Locations:  
[www.fbi.gov/contact-us/field](http://www.fbi.gov/contact-us/field)

**BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM**

This Public Service Announcement (PSA) is an update and companion to Business E-mail Compromise (BEC) PSA 1-050417-PSA posted on [www.ic3.gov](http://www.ic3.gov). This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data for the time frame October 2013 to May 2018.

**DEFINITION**

Business E-mail Compromise (BEC)/E-mail Account Compromise (EAC) is a sophisticated scam targeting both businesses and individuals performing wire transfer payments.

The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between **October 2013 and May 2018**:

Domestic and international incidents:	78,617
Domestic and international exposed dollar loss:	\$12,536,948,299

The following BEC/EAC statistics were reported in victim complaints where a country was identified to the IC3 from **October 2013 to May 2018**:

Total U.S. victims:	41,058
Total U.S. victims:	\$2,935,161,457
Total non-U.S. victims:	2,565
Total non-U.S. exposed dollar loss:	\$671,915,009

The following BEC/EAC statistics were reported by victims via the financial transaction component of the IC3 complaint form, which became available in June 2016<sup>3</sup>. The following statistics were reported in victim complaints to the IC3 from **June 2016 to May 2018**:

Total U.S. financial recipients:	19,335
Total U.S. financial recipients:	\$1,629,975,562
Total non-U.S. financial recipients:	11,452
Total non-U.S. financial recipients exposed dollar loss:	\$1,690,788,278

# Spear Phishing Attacks

- Target particular users to entice them into opening an attachment or clicking on a link which launches malware on the system
- Nearly “80% of all espionage-motivated attacks used either a link or attachment in a phishing email to gain access to their victim’s environment”

# Ransomware Demands

- 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.”





# Nation State Actors

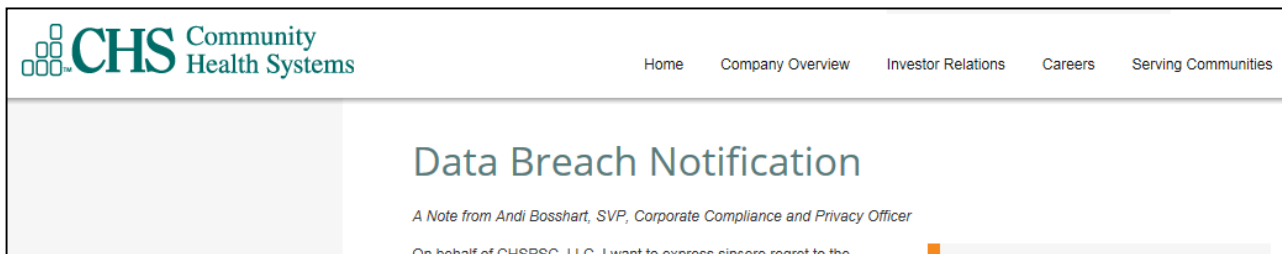


The screenshot shows the top portion of the FBI website. At the top left is the FBI logo with the text 'THE FBI FEDERAL BUREAU OF INVESTIGATION'. To the right is the official seal of the Department of Justice, Federal Bureau of Investigation. Below the logo and seal is a navigation bar with links for 'CONTACT US', 'ABOUT US', 'MOST WANTED', 'NEWS', and 'STATS'. The main heading is 'National Press Releases'. Below this is a breadcrumb trail: 'Home • News • Press Room • Press Releases • Update on Sony Investigation'. There are social media sharing options for Twitter (3,816), Facebook (3,008), and a 'Share' button. The title of the press release is 'Update on Sony Investigation'. The location is 'Washington, D.C.' and the date is 'December 19, 2014'. The contact information for the 'FBI National Press Office' is '(202) 324-3691'. The main text of the press release is as follows:

Today, the FBI would like to provide an update on the status of our investigation into the cyber attack targeting Sony Pictures Entertainment (SPE). In late November, SPE confirmed that it was the victim of a cyber attack that destroyed systems and stole large quantities of personal and commercial data. A group calling itself the "Guardians of Peace" claimed responsibility for the attack and subsequently issued threats against SPE, its employees, and theaters that distribute its movies.

The FBI has determined that the intrusion into SPE's network consisted of the deployment of destructive malware and the theft of proprietary information as well as employees' personally identifiable information and confidential communications. The attacks also rendered thousands of SPE's computers inoperable, forced SPE to take its entire computer network offline, and significantly disrupted the company's business operations.

# Foreign-Based Cyber Attacks



The screenshot shows the top portion of a website. On the left is the CHS Community Health Systems logo. On the right is a navigation menu with links for Home, Company Overview, Investor Relations, Careers, and Serving Communities. The main heading is "Data Breach Notification". Below the heading is a sub-heading: "A Note from Andi Bosshart, SVP, Corporate Compliance and Privacy Officer". The text below that is partially obscured by a callout box but begins with "On behalf of CHSPSC, LLC, I want to express sincere regret to the".

... a **foreign-based cyber-attack** of our computer network.... CHSPSC, LLC believes the attacker was an **“Advanced Persistent Threat” group originating from China**, which used **highly sophisticated malware technology** to attack CHSPSC, LLC’s systems. The intruder was able to bypass the company’s security measures and successfully copy and transfer some data existing on CHSPSC, LLC’s systems.

CHSPSC, LLC, a Tennessee company, provides management, consulting, and information technology services to certain clinics and hospital-based physicians in this area.

CHSPSC, LLC believes the attacker was an “Advanced Persistent Threat” group originating from China, which used highly sophisticated malware technology to attack CHSPSC, LLC’s systems. The intruder was able to bypass the company’s security measures and successfully copy and transfer some data existing on CHSPSC, LLC’s systems.

card information as a condition of receiving identity theft consultation or restoration services.

**PLEASE NOTE:** We will NOT call or email anyone requesting any personal information as a result of this situation. If you receive an unsolicited call or email that appears to be from CHSPSC, LLC,

# SIGNIFICANT COSTS AND CONSEQUENCES

COMPLEX, COSTLY, BURDENSOME

# 2018 Cost of Data Breach Study: Global Overview

## Global study at a glance

---

> Average total cost of a data breach:

**\$3.86 million**

> Average total one-year cost increase:

**6.4%**

> Average cost per lost or stolen record:

**\$148**

> One-year increase in per capita cost:

**4.8%**

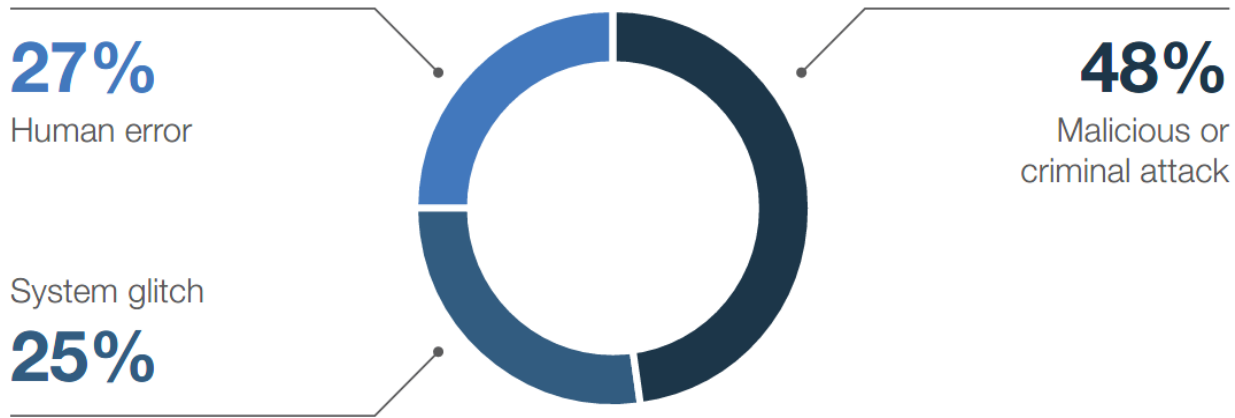
> Likelihood of a recurring material breach over the next two years:

**27.9%**

> Average cost savings with an Incident Response team:

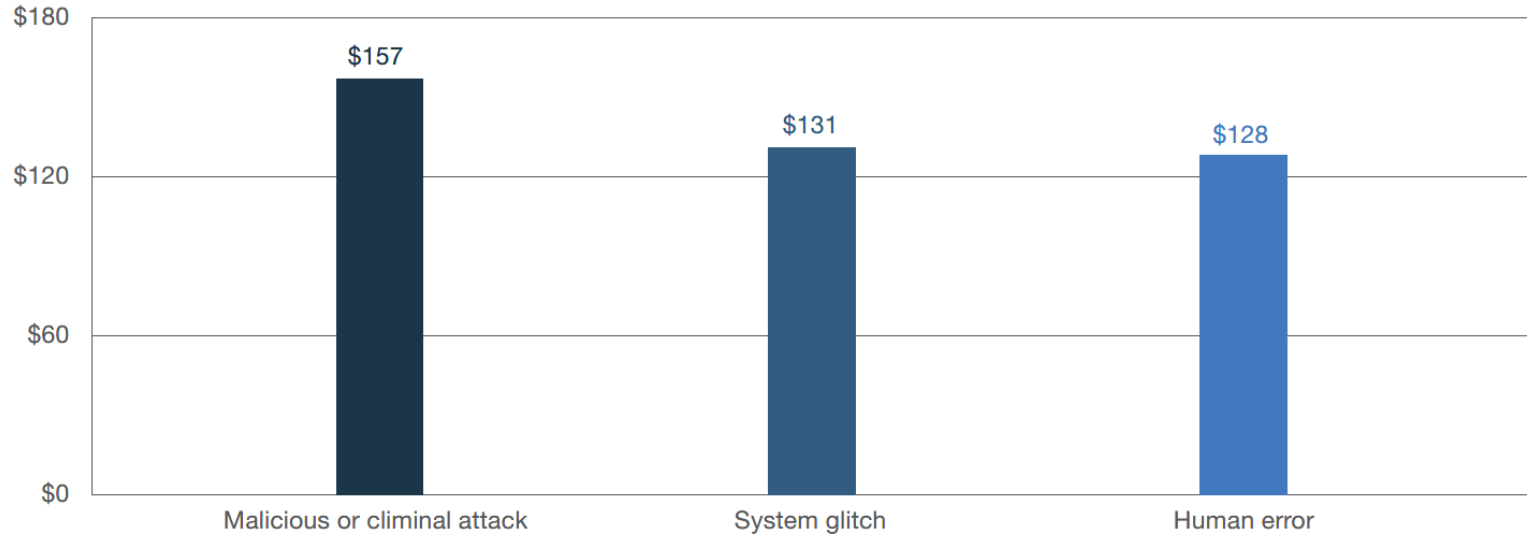
**\$14 per record**

# Root Cause of Data Breach



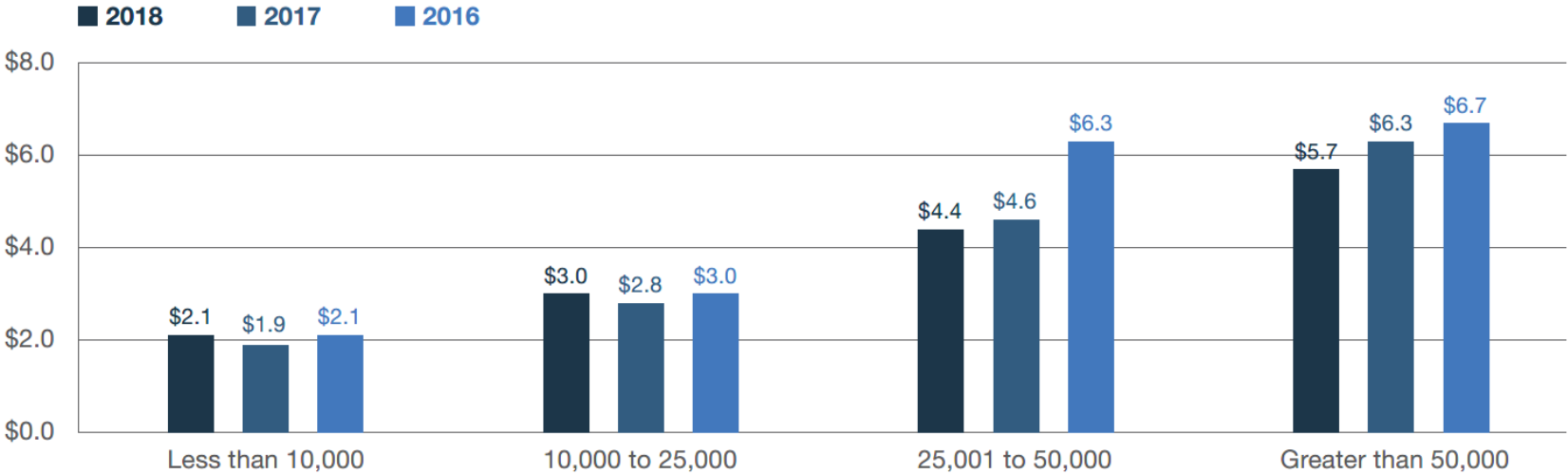
# Cost Per Capita Based on Cause of Data Breach

Measured in US\$



# Average Total Cost by Size

Measured in US\$ millions



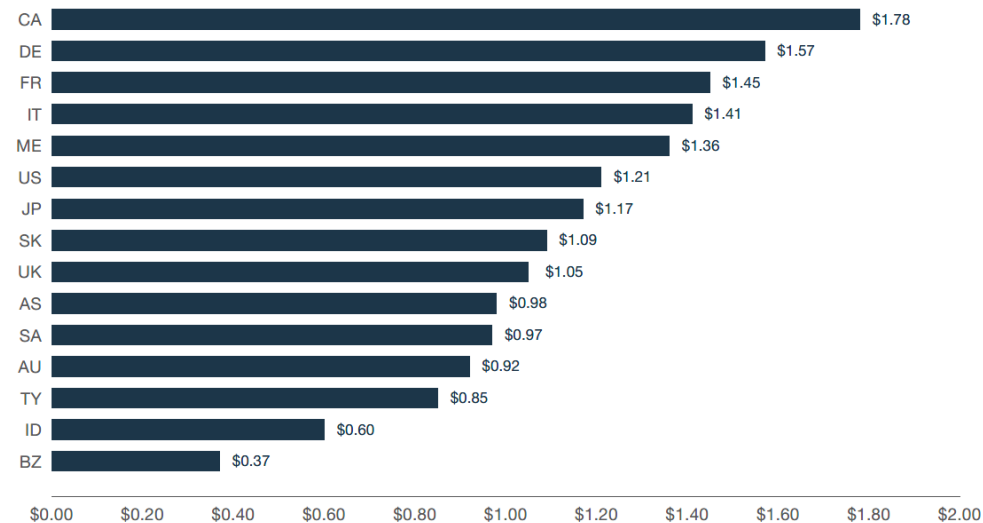
# Detection and Escalation Costs

Activities that enable a company to detect and report the breach to appropriate personnel within a specified time period.

## Examples:

- Forensic and investigative activities
- Assessment and audit services
- Crisis team management
- Communications to executive management and board of directors

Measured in US\$ millions





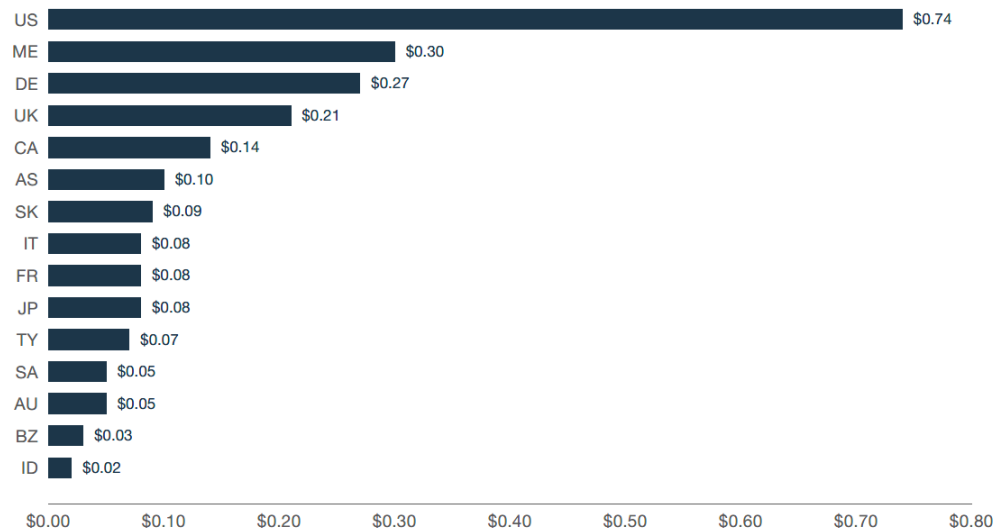
# Notification Costs

Activities that enable the company to notify individuals who had data compromised in the breach (data subjects) as regulatory activities and communications.

## Examples:

- Emails, letters, outbound telephone calls, or general notice that personal information was lost or stolen
- Communication with regulators; determination of all regulatory requirements, engagement of outside experts

Measured in US\$ millions



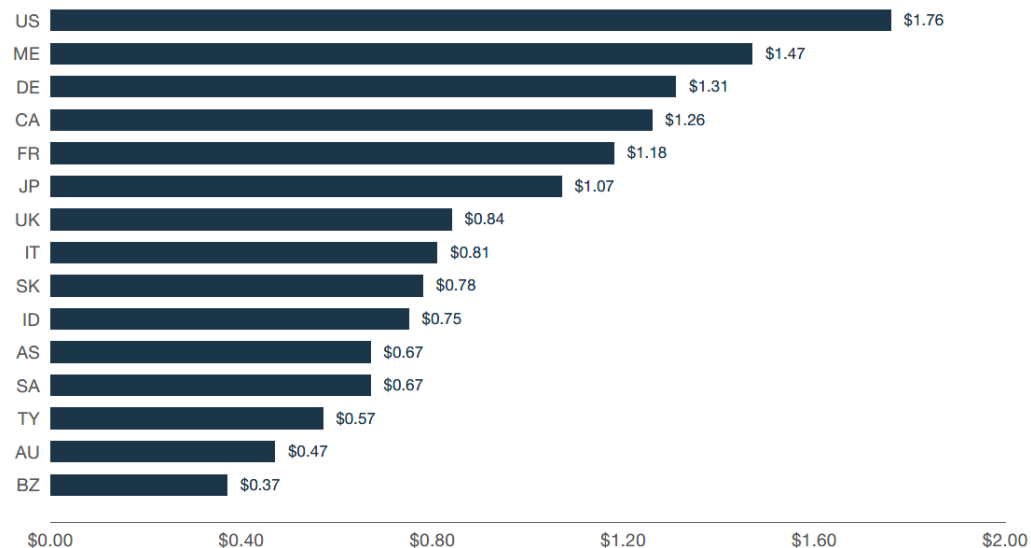
# Post Data Breach Response Costs

Processes set up to help individuals or customers affected by the breach to communicate with the company, as well as costs associated with redress activities and reparation with data subjects and regulators.

## Examples:

- Help desk activities/inbound communications
- Credit report monitoring and identity protection services
- Issuing new accounts or credit cards
- Legal expenditures
- Product discounts
- Regulatory interventions (fines)

Measured in US\$ millions



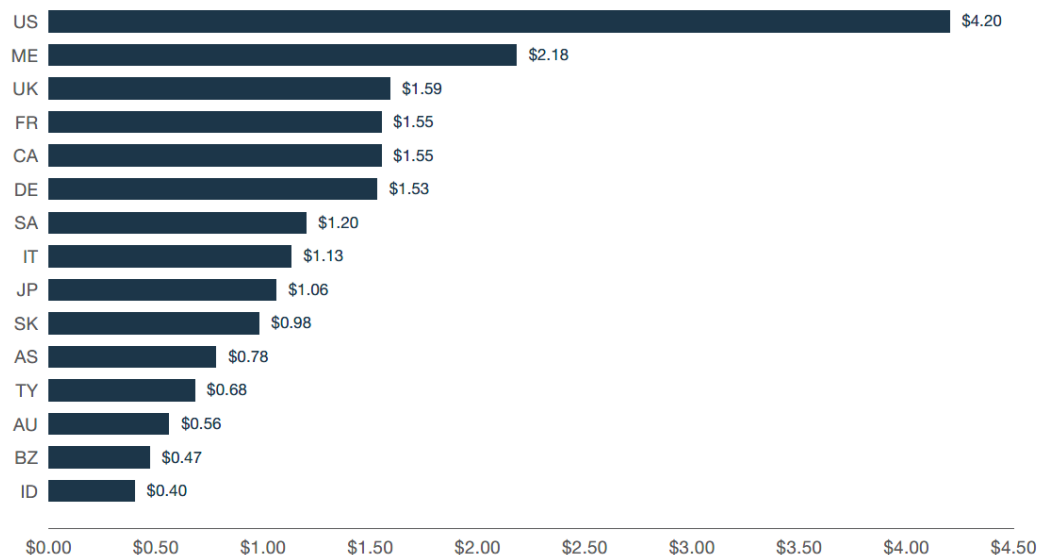
# Lost Business Costs

Activities associated with cost of lost business including customer churn, business disruption, and system downtime.

## Examples:

- Cost of business disruption and revenue losses from system downtime
- Cost of lost customers and acquiring new customers
- Reputation losses and diminished goodwill

Measured in US\$ millions



# “Under-Covered” for Cyber-Related Losses

- Equifax data breach (2017)
  - Cost approximately \$439 million to address
  - Only \$125 million was covered by insurance (71% underinsurance rate).



[Home](#) [About](#) [Packages](#)

In fact, **Target's costs related to the data breach have reached \$252M in total, of which \$90M has been covered by cyber insurance.** This is because the costs related to a data breach (and covered by cyber liability insurance) far exceed those of a settlement with effected customers. Those costs include:

- Defending various lawsuits from [banks](#) and [customers](#) alike
- Forensic / investigative costs to determine the cause of the breach
- Data and network infrastructure restoration and costs
- Compliance with [breach notification laws](#)
- [Business interruption](#) costs for downtime while fixing the POS systems
- Hiring marketing/PR firms to repair the reputational damage from such a disaster

In fact, Advisen's research has revealed that the Target data breach was the largest data breach incident in the [last 8 years](#). Keep in mind that the claims are still rolling in! Though the company still had to pay over \$160M out of pocket, cyber insurance kicked in to cover a sizable portion of each of the above costs.

# Preliminary Questions

- Did a “data breach” occur?
- Determining scope of data breach or incident.
- When was cyber compromise/incident discovered?
  - How was cyber compromise/incident discovered?
- How did cyber compromise/incident occur?
- When did the cyber compromise/incident occur?
  - Early assessments can be revised
- Who caused cyber compromise/incident?
  - Attribution analysis
- What security risks?
- Which regulators?
- Notification issues
- Public relations
- Cyber Insurance coverage

# RECENT CASE STUDY

# Yahoo!, Inc.

- All information pursuant to SEC Order and Yahoo public filings:
  - Multiple data breaches over multiple years
  - On-going litigation
  - No insurance coverage

UNITED STATES OF AMERICA  
Before the  
SECURITIES AND EXCHANGE COMMISSION

SECURITIES ACT OF 1933  
Release No. 10485 / April 24, 2018

SECURITIES EXCHANGE ACT OF 1934  
Release No. 83096 / April 24, 2018

ACCOUNTING AND AUDITING ENFORCEMENT  
Release No. 3937 / April 24, 2018

ADMINISTRATIVE PROCEEDING  
File No. 3-18448

In the Matter of

ALTABA INC., f/d/b/a  
YAHOO! INC.,

Respondent.

ORDER INSTITUTING CEASE-AND-  
DESIST PROCEEDINGS PURSUANT TO  
SECTION 8A OF THE SECURITIES ACT  
OF 1933 AND SECTION 21C OF THE  
SECURITIES EXCHANGE ACT OF 1934,  
MAKING FINDINGS, AND IMPOSING A  
CEASE-AND-DESIST ORDER

I.

The Securities and Exchange Commission ("Commission") deems it appropriate that cease-and-desist proceedings be, and hereby are, instituted pursuant to Section 8A of the Securities Act of 1933 (the "Securities Act") and Section 21C of the Securities Exchange Act of 1934 ("Exchange Act"), against Altaba Inc., f/d/b/a Yahoo! Inc. ("Yahoo" or "Respondent").

II.

# Yahoo!, Inc. – Incidents and Response Timeline

- **August 2013**

- Hackers steal data from 1 billion Yahoo users.

- **December 2014**

- Yahoo's security team discovered that Russian hackers had obtained its "crown jewels"—the usernames, email addresses, phone numbers, birthdates, passwords and security questions/answers for at least 500 million Yahoo accounts.

- **2015 – Early 2016**

- Yahoo's internal security team was aware that the same hackers were continuously targeting Yahoo's user database and also received reports that Yahoo user credentials were for sale on the dark web.

- **Summer 2016**

- Yahoo negotiates with Verizon to sell its operating business.
- In response to due diligence questions about its history of data breaches, Yahoo gave Verizon a spreadsheet falsely representing that it was aware of only four minor breaches involving users' personal information. A new Yahoo CISO (hired in October 2015) concluded that Yahoo's entire database, including the personal data of its users, had likely been stolen by nation-state hackers and could be exposed on the dark web in the immediate future.



# Yahoo!, Inc. – Disclosures

- **September 2016**

- Yahoo discloses the 2014 data breach to Verizon and in a press release attached to a Form 8-K. Yahoo's disclosure pegged the number of affected Yahoo users at 500 million.

- **December 2016**

- Yahoo discloses the August 2013 data breach, and that hackers had forged cookies that would allow an intruder to access user accounts without supplying a valid password in 2015 and 2016.

# Yahoo, Inc. – Public Disclosures

## Yahoo 2013 Account Security Update FAQs

Yahoo is providing notice to additional user accounts affected by an August 2013 theft of user data [previously announced by the company in December 2016](#). This is not a new security issue. In 2016, Yahoo previously took action to protect all user accounts.

Below are updated FAQs containing details about the issue Yahoo announced in December 2016, what was done to secure user accounts, and additional account security recommendations.

- + [What happened?](#)
- + [Was my account affected by the August 2013 incident?](#)
- + [What information was taken in the August 2013 incident?](#)
- + [Is this October 2017 notification related to the data theft that Yahoo announced on December 14, 2016?](#)

# Yahoo!, Inc. – Disclosures

- **March 1, 2017**

- Yahoo files its 2016 Form 10-K, describing the 2014 hacking incident as having been committed by a “state-sponsored actor,” and the August 2013 hacking incident by an “unauthorized third party.” As to the August 2013 incident, Yahoo stated that “we have not been able to identify the intrusion associated with this theft.” Yahoo disclosed security incident expenses of \$16 million (\$5 million for forensics and \$11 million for lawyers), and flatly stated: “The Company does not have cybersecurity liability insurance.”

- **October 3, 2017**

- Yahoo discloses that all of its users (3 billion accounts) have likely been affected by the hacking activity that traces back to August 2013.

# Yahoo!, Inc. Litigation

- SEC Action – April 2018
- Securities Class Action – Santa Clara County
- Derivative Lawsuit – Northern District of California
- Individual Class Action – Northern District of California
- DOJ Prosecution Against Hackers

# Yahoo, Inc.: Enforcement Action



- **Fine: \$35 million;** SEC Order (April 24, 2018)
- **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

## 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

# Yahoo!, Inc.: Securities Class Action and Derivative Lawsuit

- Securities Class Action – September 7, 2018
  - **\$80 million settlement**
- Derivative Lawsuit – Jan. 4, 2019
  - **\$29 million settlement**
  - The derivative complaint asserted claims against Yahoo's board for breach of fiduciary duty, insider trading, unjust enrichment, and waste.
  - The plaintiffs also asserted claims against Verizon for aiding and abetting.
  - The complaint alleged that Yahoo officials knew about the data breaches long before they were disclosed to the public and that instead of disclosing that the data breaches had taken place the defendants sought to cover up the breaches.
  - The complaint also alleged that several of the individual defendants sold stock from their personal holding of Yahoo stock after becoming aware of the data breaches and before the breaches were made public.

# Yahoo!, Inc.:

## Individual Class Action – Northern District of California

- **\$50 million settlement rejected** by Judge Koh in January 2019
  - Nationwide litigation brought on behalf of well over 1 billion users whose personal information was compromised in three massive data breaches.
  - “All plaintiffs have alleged a risk of future identity theft, in addition to loss of value of their personal identification information” - Judge Lucy Koh

7	
8	
9	UNITED STATES DISTRICT COURT
10	NORTHERN DISTRICT OF CALIFORNIA
11	SAN JOSE DIVISION
12	IN RE: YAHOO! INC. CUSTOMER
13	DATA SECURITY BREACH
14	LITIGATION
15	Case No. 16-MD-02752-LHK
16	<b>ORDER DENYING MOTION FOR</b>
17	<b>PRELIMINARY APPROVAL OF</b>
18	<b>CLASS ACTION SETTLEMENT</b>
19	Re: Dkt. No. 330
20	
21	Plaintiffs Kimberly Heines, Hashmatullah Essar, Paul Dugas, Matthew Ridolfo, Deana
22	Ridolfo, Yaniv Rivlin, Mali Granot, Brian Neff, and Andrew Mortensen (collectively, “Plaintiffs”)
23	bring a putative class action against Defendant Yahoo! Inc. (“Yahoo”). Plaintiff Brian Neff also
24	brings a putative class action against Defendant Aabaco Small Business, LLC (“Aabaco”)
25	(collectively with Yahoo, “Defendants”). Before the Court is Plaintiffs’ motion for preliminary
26	approval of class action settlement. ECF No. 330 (“Mot.”). Having considered the parties’
	motion and supplemental filings, arguments of counsel at the November 29, 2018 hearing, the
	relevant law, and the record in this Case, the Court DENIES Plaintiffs’ motion for preliminary
	approval of class action settlement.

# Yahoo!, Inc.: DOJ Prosecution

- On March 15, 2017, DOJ charged two officers of the Russian Federal Security Service and two hackers in connection with the breach in late 2014.
  - Nov. 2017, Karim Baratov, a 23-year-old hacker-for-hire, pled guilty
    - Conspiracy to commit computer fraud and aggravated identity theft.
  - Admitted that, between 2010 and 2017, he hacked into the webmail accounts of more than 11,000 victims, stole and sold the information contained in their email accounts, and provided his customers with ongoing access to those accounts.
  - May 2018, Sentenced to **5 years in prison**.

**JUSTICE NEWS**

Department of Justice  
Office of Public Affairs

---

FOR IMMEDIATE RELEASE Tuesday, May 29, 2018

**International Hacker-For-Hire Who Conspired With and Aided Russian FSB Officers Sentenced to 60 Months in Prison**

**Russian Officers Tasked Prolific Hacker-for-Hire to Target Webmail Accounts**

Karim Baratov, aka Kay, aka Karim Taloverov, aka Karim Akehmek Tokbergenov, 23, was sentenced to five years in prison and ordered to pay a fine, which encompasses all of his remaining assets.

Assistant Attorney General for National Security John C. Demers, Acting U.S. Attorney Alex G. Tse for the Northern District of California, and Special Agent in Charge John F. Bennett of the FBI's San Francisco Field Office made the announcement. The sentence was handed down today by U.S. District Judge the Honorable Vince Chhabria.

"Criminal hackers and the countries that sponsor them make a grave mistake when they target American companies and citizens. We will identify them wherever they are and bring them to justice," said Assistant Attorney General Demers. "I would like to thank Canadian law enforcement authorities for their tremendous assistance in bringing Baratov to justice. We will continue to work with our foreign partners to find and prosecute those who would violate our laws."

"The sentence imposed reflects the seriousness of hacking for hire," said Acting U.S. Attorney Tse. "Hackers such as Baratov ply their trade without regard for the criminal objectives of the people who hire and pay them. These hackers are not minor players; they are a critical tool used by criminals to obtain and exploit personal information illegally. In sentencing Baratov











# HEIGHTENED REGULATORY ENFORCEMENT

# Regulatory Landscape



# Cybersecurity Landscape

## Growing Patchwork of Laws

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

# 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**

# Government Agency Enforcement Actions



# 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

# SEC Investigative Report (Oct. 16, 2018)



- **SEC Investigative Report**

- Nine public companies 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.

# Cybersecurity Focus during Examinations



- 2017 Risk Report
- Examination of 75 Firms
  - Governance and Risk Assessment
  - Access Rights and Controls
  - Data Loss Prevention
  - Vendor Management
  - Training
  - Incident Response

The image shows the cover of a document titled "NATIONAL EXAM PROGRAM RISK ALERT". The cover is dark blue with a gold border. At the top left is the SEC logo. The title "NATIONAL EXAM PROGRAM" is in large white letters, and "RISK ALERT" is in smaller white letters below it. Below the title, it says "By the Office of Compliance Inspections and Examinations ('OCIE')". The volume and issue information "Volume VI, Issue 5" and the date "August 7, 2017" are on the right. The main title "OBSERVATIONS FROM CYBERSECURITY EXAMINATIONS" is in large white letters. Below that is the section "I. Introduction". The text describes the OCIE's Cybersecurity 2 Initiative, which examined 75 firms to assess industry practices and legal and compliance issues. It mentions that the initiative built upon prior cybersecurity examinations and involved more validation and testing of procedures and controls. A summary of the staff's observations is provided at the bottom.

**NATIONAL EXAM PROGRAM**  
RISK ALERT

By the Office of Compliance Inspections and Examinations ("OCIE")<sup>1</sup>

Volume VI, Issue 5 August 7, 2017

**OBSERVATIONS FROM  
CYBERSECURITY EXAMINATIONS**

**I. Introduction**

In OCIE's Cybersecurity 2 Initiative, National Examination Program staff examined 75 firms, including broker-dealers, investment advisers, and investment companies ("funds") registered with the SEC to assess industry practices and legal and compliance issues associated with cybersecurity preparedness.<sup>2</sup> The Cybersecurity 2 Initiative built upon prior cybersecurity examinations, particularly OCIE's 2014 Cybersecurity 1 Initiative.<sup>3</sup> However, the Cybersecurity 2 Initiative examinations involved more validation and testing of procedures and controls surrounding cybersecurity preparedness than was previously performed.

The examinations focused on the firms' written policies and procedures regarding cybersecurity, including validating and testing that such policies and procedures were implemented and followed. In addition, the staff sought to better understand how firms managed their cybersecurity preparedness by focusing on the following areas: (1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response.

In general, the staff observed increased cybersecurity preparedness since our 2014 Cybersecurity 1 Initiative. However, the staff also observed areas where compliance and oversight could be improved. This Risk Alert provides a summary of the staff's observations from the Cybersecurity 2 Initiative



# Cybersecurity Focus during Examinations



- OCIE 2019 Priorities

“Cybersecurity protection is critical to the operation of the financial markets. The impact of a successful cyber-attack may have consequences that extend beyond the firm compromised to other market participants and retail investors, who may not be well informed of these risks and consequences. OCIE is working with firms to identify and manage cybersecurity risks and to encourage market participants to actively and effectively engage in this effort. **OCIE will continue to prioritize cybersecurity in each of its five examination programs.**

Examinations will focus on, among other things, **proper configuration of network storage devices, information security governance generally, and policies and procedures related to retail trading information security.**

Specific to investment advisers, OCIE will emphasize cybersecurity practices at investment advisers with multiple branch offices, including those that have recently merged with other investment advisers, and continue to focus on, among other areas, governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.”

# 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

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



- A specialized unit dedicated to targeting cyber-related misconduct in the US markets.
- The SEC Cyber Unit has focused on alleged misconduct involving:
  - Issuer disclosure
  - Market oversight
  - Intrusions into retail brokerage accounts
  - The submission of false regulatory filings
  - Hacking to obtain material non-public information.

# SEC Cyber Unit – Hacking / Insider Trading



- SEC v. Ieremenko, Oleksandr, et al.
  - The Commission filed a district court action alleging that Ieremenko, working with others, hacked into the SEC's EDGAR system and extracted test files containing nonpublic information about upcoming quarterly earnings announcement to use for illegal trading.
- SEC v. Hong, Iat, et al.
  - Overseas traders hacked into two U.S. law firms to obtain nonpublic information on which they traded.

# SEC Cyber Unit – Protecting Customer Accounts



- SEC v. Joseph P. Willner
  - Day trader hacked into over 100 online customer brokerage accounts to manipulate the price of securities generating at least \$700,000 in illicit profits

# SEC Cyber Unit – Safeguarding Information



- **Voya Financial Advisors**
  - The Commission filed settled administrative proceedings against an Iowa-based broker-dealer and investment adviser related to its failures in cybersecurity policies and procedures surrounding a cyber intrusion that compromised personal information of thousands of its customers, in violation of Reg S-P and Reg S-ID.

# SEC Cyber Unit – Safeguarding Information



- Morgan Stanley Smith Barney LLC
  - Failure to safeguard customer data from cyber-breaches in violation of Reg S-P stemming from a Morgan Stanley employee transferring confidential customer data to a personal server that was eventually hacked.



- RT Jones Capital Equities Management, Inc.
  - Failure to safeguard customer data from cyber-breaches in violation of Reg S-P as a result of an investment adviser's storage of sensitive customer information on a third-party hosted web server that was eventually hacked and its failure to adopt written policies and procedures reasonably designed to safeguard such customer information.

**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.



# Compliance – EU Considerations

- The EU's General Data Protection Regulation has a strict 72-hour reporting obligation if you collect personal data or behavioral information from someone in an EU country.
  - U.S. companies that have no direct business operations in any one of the 28 member states of the European Union are still subject to the rule if they have a web presence and market their products over the web.
  - The law only applies if the data subjects are in the EU when the data is collected. For EU citizens outside the EU when the data is collected, the GDPR would *not* apply.

# MORGAN LEWIS GUIDANCE AND SERVICES

# The Best Offense is a Good Defense

- **Governance**

- Board cyber risk management
- Cybersecurity risk oversight and personnel
- Cyber-risk management practices
- Preparedness for cyber incident or attack

- **Internal Controls and Policies**

- “[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

- **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**

- Insider Trading Programs
- Internal Control Programs

# The Best Offense is a Good Defense

- **Training**

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

- **Managing Cyber Incident**

- Multiple regulators
- Incident Response Plans and Testing
- Attorney-Client Privilege Cyber Investigations

- **Address Disclosure Issues**

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

# 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 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.

Q&A

# Mark L. Krotoski



**Partner**

**Morgan Lewis**

[mark.krotoski@morganlewis.com](mailto:mark.krotoski@morganlewis.com)

+1.650.843.7212

- Litigation Partner, Privacy and Cybersecurity and Antitrust practices with more than 20 years' experience handling cybersecurity cases and issues.
- Advises clients on 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.
- Experience handling complex and novel cyber investigations and high-profile 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, in addition to other DOJ leadership positions.

# Emily Drazan Chapman



**Associate**  
**Morgan Lewis**

[emily.chapman@morganlewis.com](mailto:emily.chapman@morganlewis.com)

+1.202.739.5699

Emily Drazan Chapman counsels companies with respect to the federal securities laws, corporate governance matters, and responding to activist shareholder campaigns. Prior to joining Morgan Lewis, Emily was an attorney-adviser with the US Securities and Exchange Commission (SEC) in the Division of Corporation Finance where she reviewed transactional filings under the Securities Act of 1933 and periodic reports and proxy statements under the Securities Exchange Act of 1934.

Emily also served in the SEC's Division of Corporation Finance's Office of Small Business Policy, where she provided interpretative guidance on exemptions to SEC registration and reviewed applications for bad actor waivers.

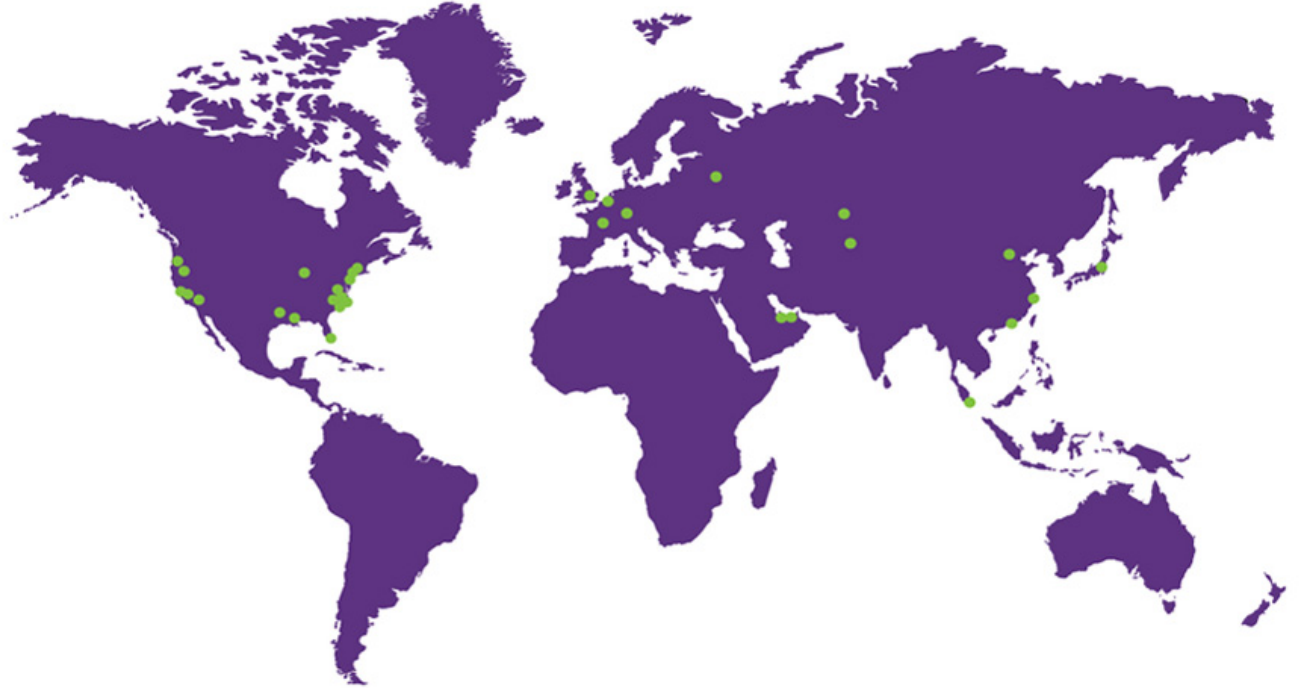


## Our Global Reach

Africa  
Asia Pacific  
Europe  
Latin America  
Middle East  
North America

## Our Locations

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



**Morgan Lewis**

\*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis 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

© 2019 Morgan, Lewis & Bockius LLP  
© 2019 Morgan Lewis Stamford LLC  
© 2019 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.