Morgan Lewis

COMPUTER-SECURITY INCIDENT NOTIFICATION REQUIREMENTS FOR BANKS

March 15, 2022

Mark Krotoski
Charles Horn
Martin Hirschprung

Presenters

Mark L. Krotoski

Charles M. Horn

Martin Hirschprung

Morgan Lewis

Overview

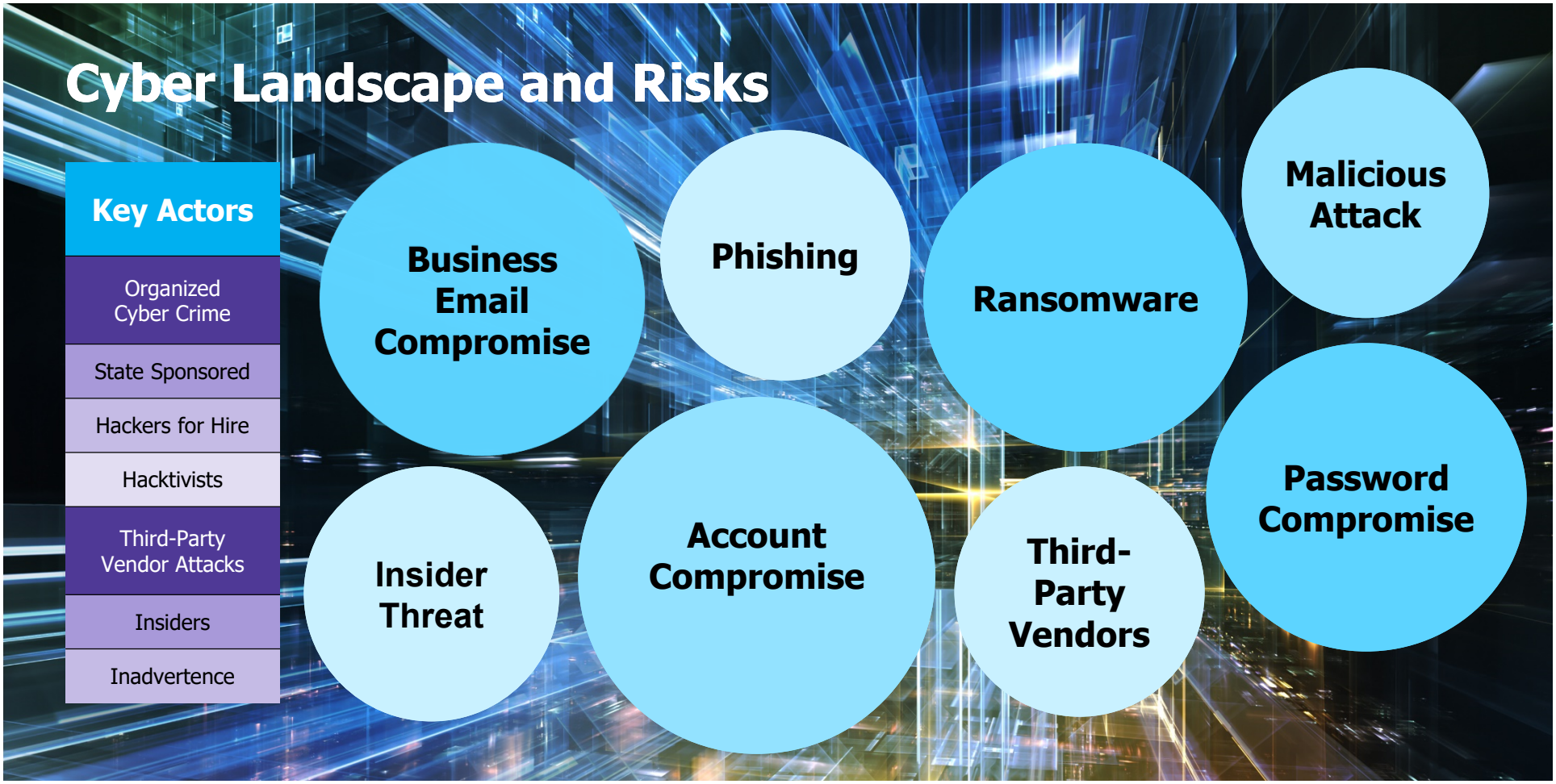
- Cyber Risk Landscape
- Financial Services Data Breach Examples
- Hypothetical Ransomware Attack
- Conducting a Cyber Investigation
- Notification Standards
- What Next and How to Prepare?

Preliminary Note

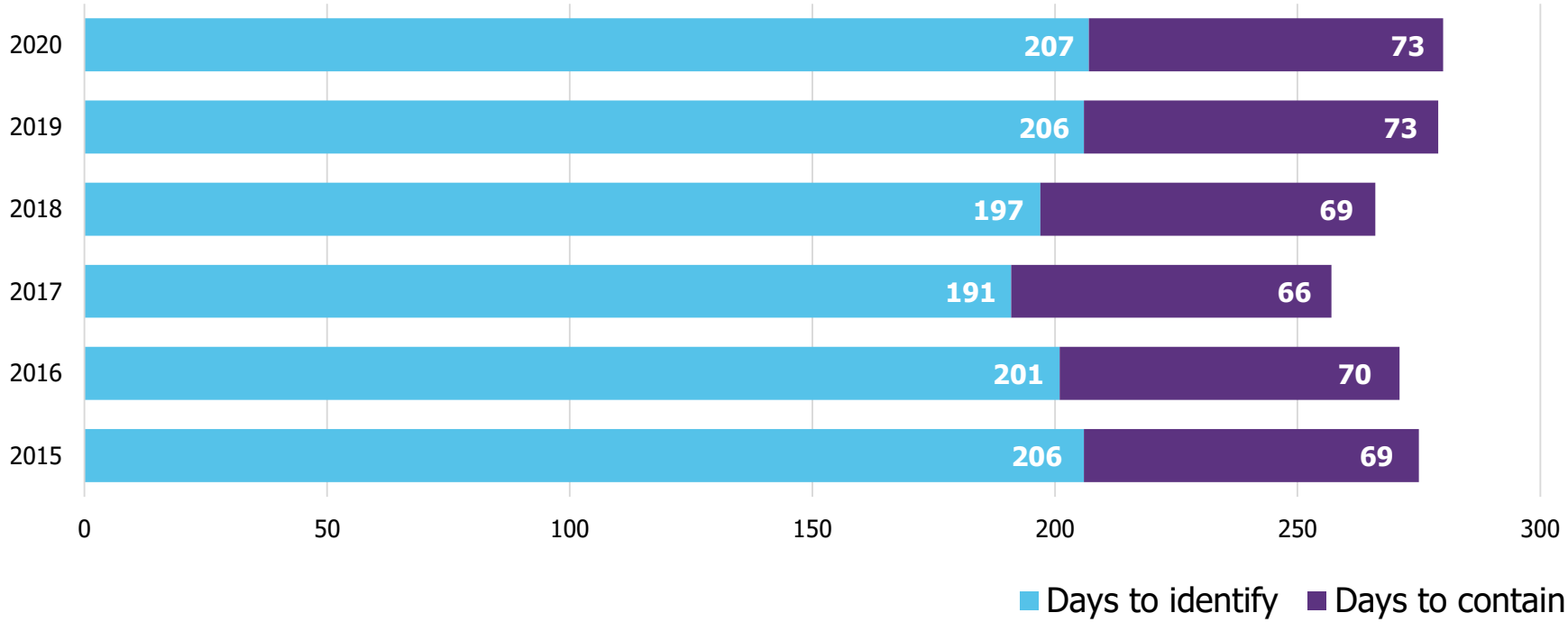
- Comments during this presentation are based upon:
  - Publicly available information;
  - General observations and experience; and
  - ***Not*** on any specific client case information.


Cyber Risk Landscape
Morgan Lewis

Cyber Landscape and Risks



Average Time to Identify and Contain a Data Breach

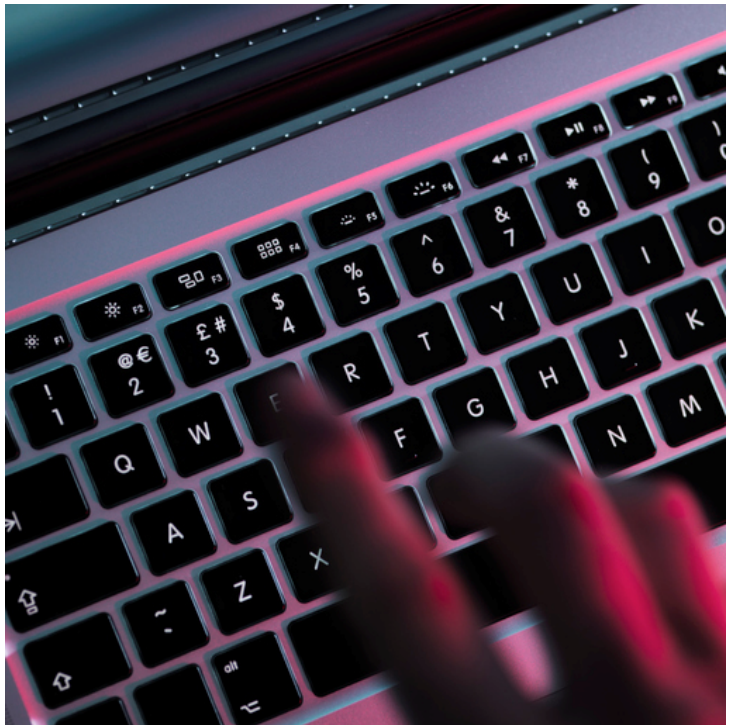


IBM Security | Cost of a Data Breach Report 2020

https://www.ibm.com/security/data-breach?mhsrc=ibmsearch_a&mhq=cost%20of%20a%20data%20breach%20report

Cybersecurity Costs

- Stolen Data
- Disruptions to Operations
- Reputational Harm
- Regulatory Risks



- The average cost of a data breach in 2020 was almost US $4 million.
- Cybersecurity Ventures estimates that Ransomware costs are expected to reach US $265 Billion by 2031.

Targeting Financial Institution Networks

- "Recent reports indicate that one or more **threat actors have orchestrated phishing and other campaigns designed to penetrate financial institution networks** to, among other objectives, access internal resources and deploy ransomware."
- "Ransomware is a type of malware designed to provide an unauthorized actor access to institutions' systems and to deny the institutions use of those systems until a ransom is paid."

RISK ALERT
OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS

July 10, 2020

CYBERSECURITY: RANSOMWARE ALERT

The Office of Compliance Inspections and Examinations (OCIE)* is committed to working with financial services market participants, federal, state and local authorities, and others, to monitor cybersecurity developments, improve operational resiliency, and effectively respond to cyber threats. Recent reports indicate that one or more threat actors have orchestrated phishing and other campaigns designed to penetrate financial institution networks to, among other objectives, access internal resources and deploy ransomware. Ransomware is a type of malware designed to provide an unauthorized actor access to institutions' systems and to deny the institutions use of those systems until a ransom is paid.

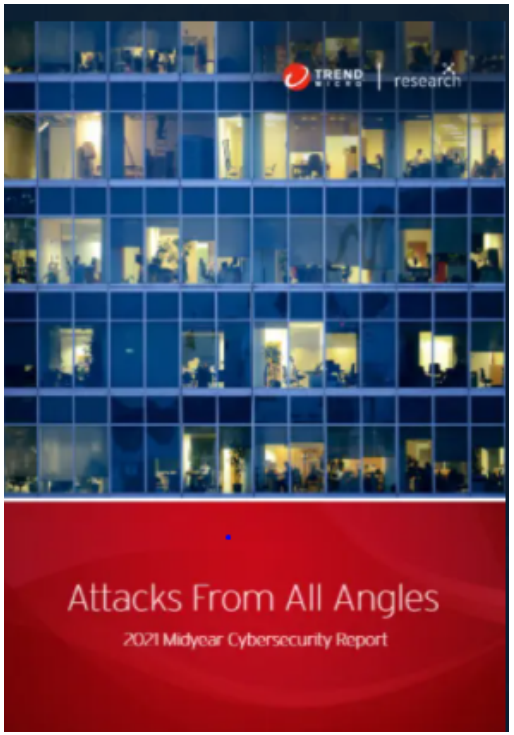
OCIE has also observed an apparent increase in sophistication of ransomware attacks on SEC registrants, which include broker-dealers, investment advisers, and investment companies. The perpetrators behind these attacks typically demand compensation (ransom) to maintain the integrity and/or confidentiality of customer data or for the return of control over registrant systems. In addition, OCIE has observed ransomware attacks impacting service providers to registrants.

In light of these threats, OCIE encourages registrants, as well as other financial services market participants, to monitor the cybersecurity alerts published by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), including the updated alert published on June 30, 2020 relating to recent ransomware attacks.[1] OCIE further encourages registrants to share this information with their third-party service providers, particularly with those that maintain client assets and records for registrants.

https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf

Targeting Financial Institution Networks

- "The banking industry was disproportionately affected, experiencing a **1,318% year-on-year increase in ransomware attacks** in the first half of 2021."



https://documents.trendmicro.com/assets/rpt/rpt-attacks-from-all-angles.pdf
https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats

Cyber-Incident Data for Financial Institutions

- The Federal banking agencies have stated that cyberattacks targeting the financial services industry have increased in frequency and severity in recent years.

See, e.g., Financial Crimes Enforcement Network, SAR Filings by Industry (Jan. 1, 2014-Dec. 31, 2020) (last accessed Oct. 11, 2021), https://www.fincen.gov/reports/sar-stats/sar-filings-industry. (Trend data may be found by downloading the Excel file "Depository Institution" and selecting the tab marked "Exhibit 5.")

- They also estimate that approximately 150 notification incidents occurred annually.

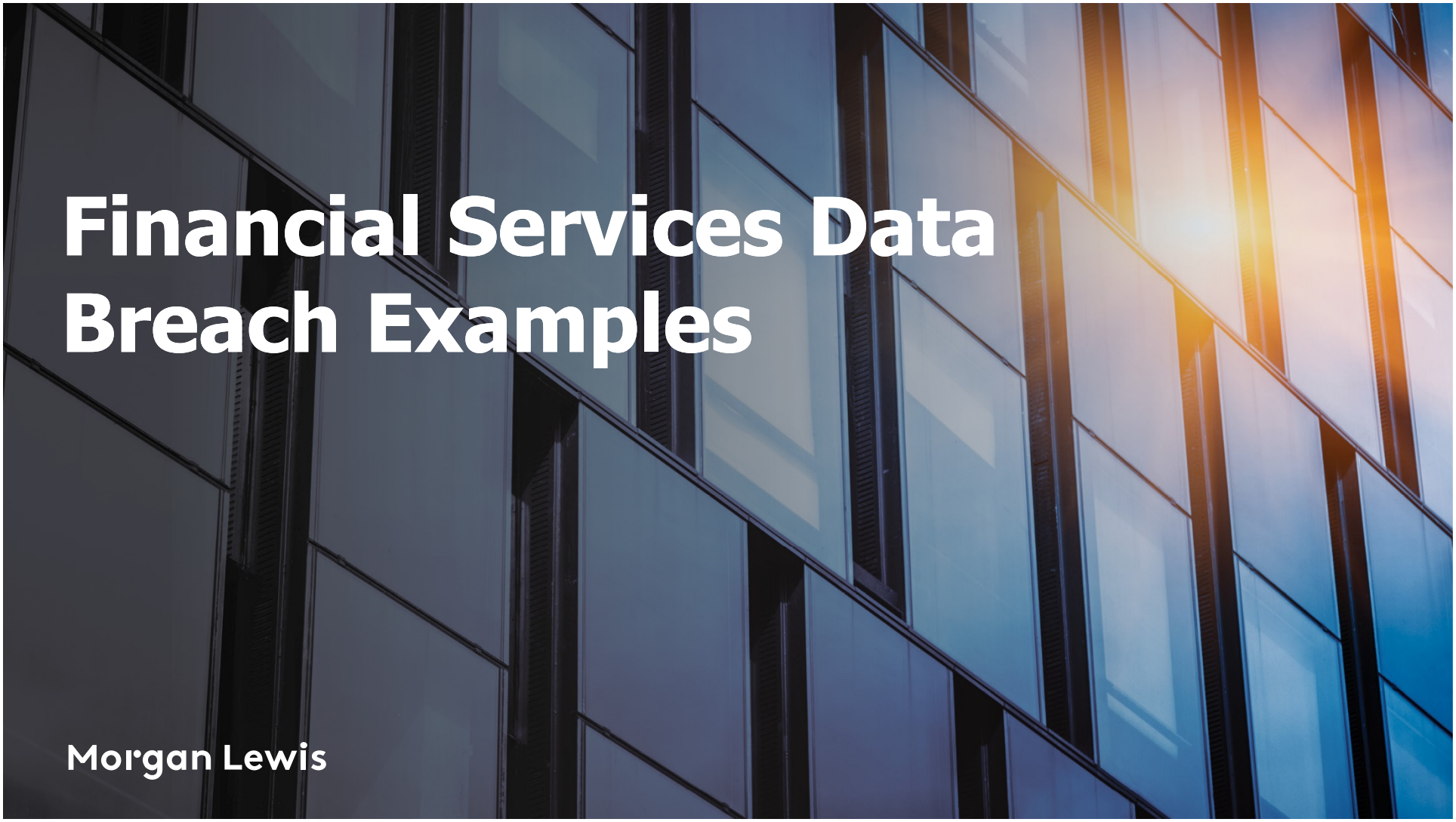
https://www.occ.gov/news-issuances/news-releases/2021/2021-119a.pdf

- FinCEN reported that, based on information it has gathered from financial institutions, the total value of suspicious activity reported in ransomware-related SARs during the first six months of 2021 was $590 million, which exceeds the value reported for the entirety of 2020 ($416 million).
- It also noted that financial institutions play an important role in protecting the US financial system from ransomware, related threats through compliance with BSA obligations.

https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

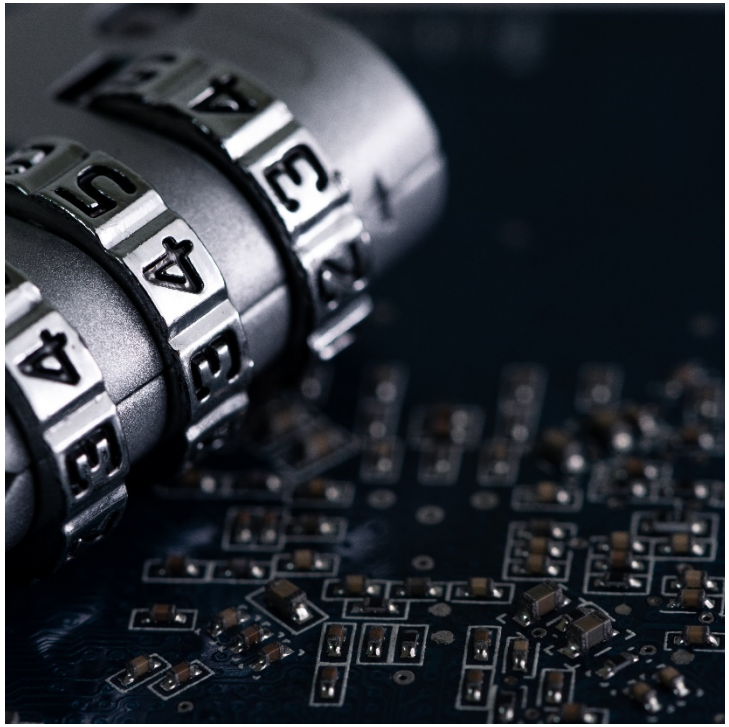
Department of Homeland Security Reporting

- As of last week, critical infrastructure owners and operators are required to report cyber incidents to the DHS Cybersecurity and Infrastructure Security Agency.
- The requirement was enacted as part of the fiscal 2022 spending bill.
- Expressly included is the reporting of ransomware attacks.
- https://homeland.house.gov/news/press-releases/thompson-katko-clarke-garbarino-laud-cyber-incident-reporting-passage


Financial Services Data
Breach Examples
Morgan Lewis

Financial Services Data Breach Examples

- Equifax
- Capital One
- Heartland Payment Systems Data
- Experian



Other examples: https://www.upguard.com/blog/biggest-data-breaches-financial-services

Equifax Inc. – Public Disclosure (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

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.

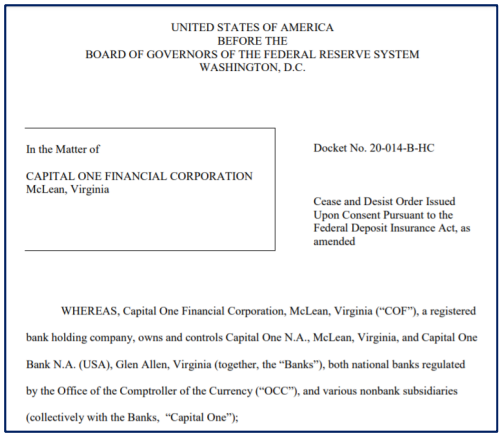
Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately **143 million U.S. consumers**. Criminals exploited a U.S. website application vulnerability to gain access to certain files.

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

Board of Governors of the Federal Reserve System

- **Background**:
  - "[O]n July 19, 2019, Capital One determined that, in March 2019, an outside individual gained unauthorized access and obtained certain types of personal information about Capital One credit card customers and individuals who had applied for Capital One credit card products affecting approximately 100 million individuals in the United States and approximately 6 million individuals in Canada."

- Cease and Desist Order Issued Upon Consent Pursuant to the Federal Deposit Insurance Act



UNITED STATES OF AMERICA
BEFORE THE
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, D.C.

In the Matter of

CAPITAL ONE FINANCIAL CORPORATION
McLean, Virginia

Docket No. 20-014-B-HC

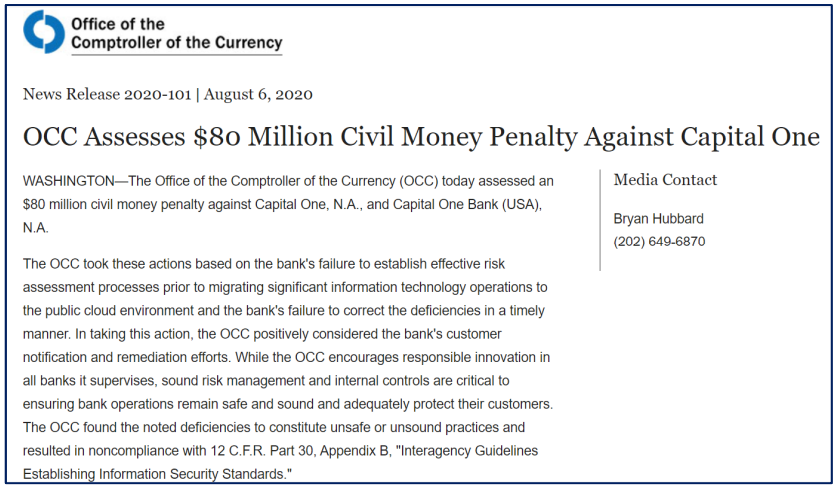
Cease and Desist Order Issued Upon Consent Pursuant to the Federal Deposit Insurance Act, as amended

WHEREAS, Capital One Financial Corporation, McLean, Virginia ("COF"), a registered bank holding company, owns and controls Capital One N.A., McLean, Virginia, and Capital One Bank N.A. (USA), Glen Allen, Virginia (together, the "Banks"), both national banks regulated by the Office of the Comptroller of the Currency ("OCC"), and various nonbank subsidiaries (collectively with the Banks, "Capital One");

file:///C:/Users/mp074242/Documents/Cybersecurity%20Financial%20Institutions/Federal%20Reserve%20Enforcement%20Capital%20One.pdf

OCC Enforcement Action Example

- $80 million civil penalty
- Comptroller findings:
  - In 2015, the Bank **failed to establish effective risk assessment processes** prior to migrating its information technology operations to the cloud operating environment.
  - Bank's **internal audit failed to identify numerous control weaknesses and gaps** in the cloud operating environment.
  - On internal audit, **Board failed to take effective actions to hold management accountable**, particularly in addressing concerns regarding certain internal control gaps and weaknesses.
  - Bank was in **noncompliance with "Interagency Guidelines Establishing Information Security Standards,"** and engaged in unsafe or unsound practices that were part of a pattern of misconduct.
  - Bank has begun addressing the identified corrective action and has committed to providing resources to remedy the deficiencies.



Office of the Comptroller of the Currency

News Release 2020-101 | August 6, 2020

OCC Assesses $80 Million Civil Money Penalty Against Capital One

WASHINGTON—The Office of the Comptroller of the Currency (OCC) today assessed an $80 million civil money penalty against Capital One, N.A., and Capital One Bank (USA), N.A.

The OCC took these actions based on the bank's failure to establish effective risk assessment processes prior to migrating significant information technology operations to the public cloud environment and the bank's failure to correct the deficiencies in a timely manner. In taking this action, the OCC positively considered the bank's customer notification and remediation efforts. While the OCC encourages responsible innovation in all banks it supervises, sound risk management and internal controls are critical to ensuring bank operations remain safe and sound and adequately protect their customers. The OCC found the noted deficiencies to constitute unsafe or unsound practices and resulted in noncompliance with 12 C.F.R. Part 30, Appendix B, "Interagency Guidelines Establishing Information Security Standards."

Media Contact

Bryan Hubbard
(202) 649-6870

https://occ.gov/news-issuances/news-releases/2020/nr-occ-2020-101.html#

Board of Governors of the Federal Reserve System

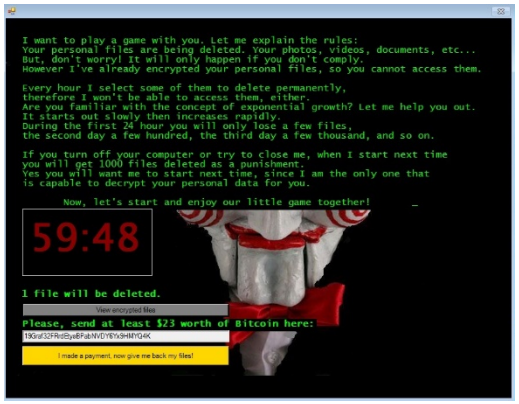
- **Board Oversight**:
  - Within 90 days, board shall submit a written plan to strengthen oversight of risk management program acceptable to the Reserve Bank.
- **Risk Management Program**:
  - Within 90 days, COF's senior management shall submit a written plan to improve risk management program, acceptable to the Reserve Bank.
- **Internal Audit**:
  - Within 90 days, COF shall jointly submit written revisions to COF's internal audit program with respect to auditing COF's risk management program, including technology risk management, acceptable to the Reserve Bank.
- **Source of Strength**:
  - Board shall take appropriate steps to fully utilize COF's financial and managerial resources to serve as a source of strength.
- **Progress Reports**:
  - Within 45 days after the end of each calendar quarter, board shall submit to the Reserve Bank written progress reports detailing the form and manner of all actions taken to secure compliance with this Order, a timetable and schedule to implement specific remedial actions to be taken, and the results thereof.
- **Approval and Implementation of Plans and Programs**:
  - COF shall submit written plans and program that are acceptable to the Reserve Bank.
  - Each plan and program shall contain a timeline for full implementation of the plan or program with specific deadlines for the completion of each component of the plan or program.

file:///C:/Users/mp074242/Documents/Cybersecurity%20Financial%20Institutions/Federal%20Reserve%20Enforcement%20Capital%20One.pdf


Hypothetical
Ransomware Attack
Morgan Lewis

Hypothetical Ransomware Attack

- A large international banking company experiences a ransomware attack.
  - Threat Actor Identifies/Exploits Vulnerability
    - Phishing, Remote Desktop Protocol (RDP), compromised passwords, software vulnerabilities
  - Deploys tools, lateral movement, escalate privileges
    - Cobalt Strike, Emotet, Trickbot
    - Credential harvesting
  - Exfiltrates data
    - PII
    - Sensitive or proprietary information
  - Encrypts files
  - Ransom demand
    - Threat to leak or destroy data
    - Urgent deadline or clock




Conducting A Cyber Investigation
Morgan Lewis

Legal Issues During Incident Response Phases

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

- Whether and when to contact law enforcement
- Legal guidance and consequences
- Response to government inquiries and enforcement actions
- Mitigation steps

Range of Legal and Forensic Issues

- Was data "exfiltrated" or "accessed" or "acquired"?
- What data?
  - PII, PHI, Contractual Information?
- Did a data "breach" occur?
- What notification requirements may be triggered?
- How to mitigate loss or damages?
- Conducting a risk assessment
- Compliance issues
- Obligations during third party vendor attack
- Issues to anticipate in a regulatory inquiry or investigation
- Issues for anticipated litigation

Are Legal Protections in Place?

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 U.S. 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."

Caution Concerning Changed Business and Legal Relationships

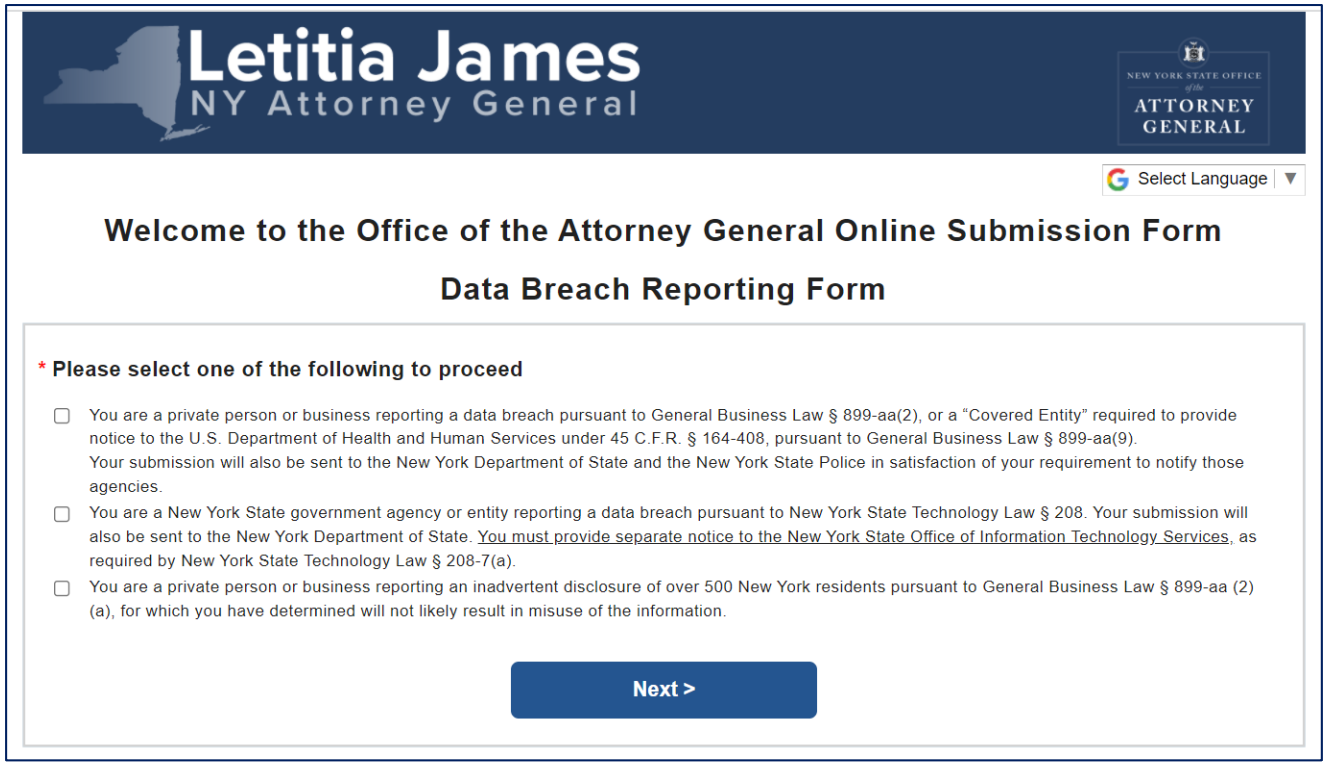
- "In sum, Capital One had determined that it had a **business critical need** for certain information in connection with a data breach incident, it had contracted with [a forensic provider] to provide that information directly to it in the event of a data breach incident, and after the data breach incident at issue in this action, Capital One then arranged to receive through **[a law firm] the information** it already had contracted to receive directly from [the forensic firm]. The Magistrate Judge, after considering the totality of the evidence, properly concluded that Capital One had **not established that the Report was protected work product**; and the Order was neither clearly erroneous nor contrary to law."
- Memorandum Opinion and Order, *In re Capital One Consumer Data Security Breach Litigation*, 2020 WL 3470261 (ED.Va. June 25, 2022).


Notification Standards
Morgan Lewis

Triggers or Is This a Cybersecurity Event?

- Federal Banking Agencies Notification Requirement
  - any "computer-security incident" that rises to the level of a "notification incident."
- New York State Law
  - unauthorized access to or acquisition of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business. The law enumerates ways in which businesses can make the determination that a breach of the security system has occurred.
- GDPR
  - a personal information data breach.
- NYDFS
  - a "cybersecurity event" has occurred that is either of the following:
  - (1) cybersecurity events impacting the covered entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or
  - (2) cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity.

Reporting Forms



Letitia James
NY Attorney General

NEW YORK STATE OFFICE of the ATTORNEY GENERAL

Select Language

Welcome to the Office of the Attorney General Online Submission Form

Data Breach Reporting Form

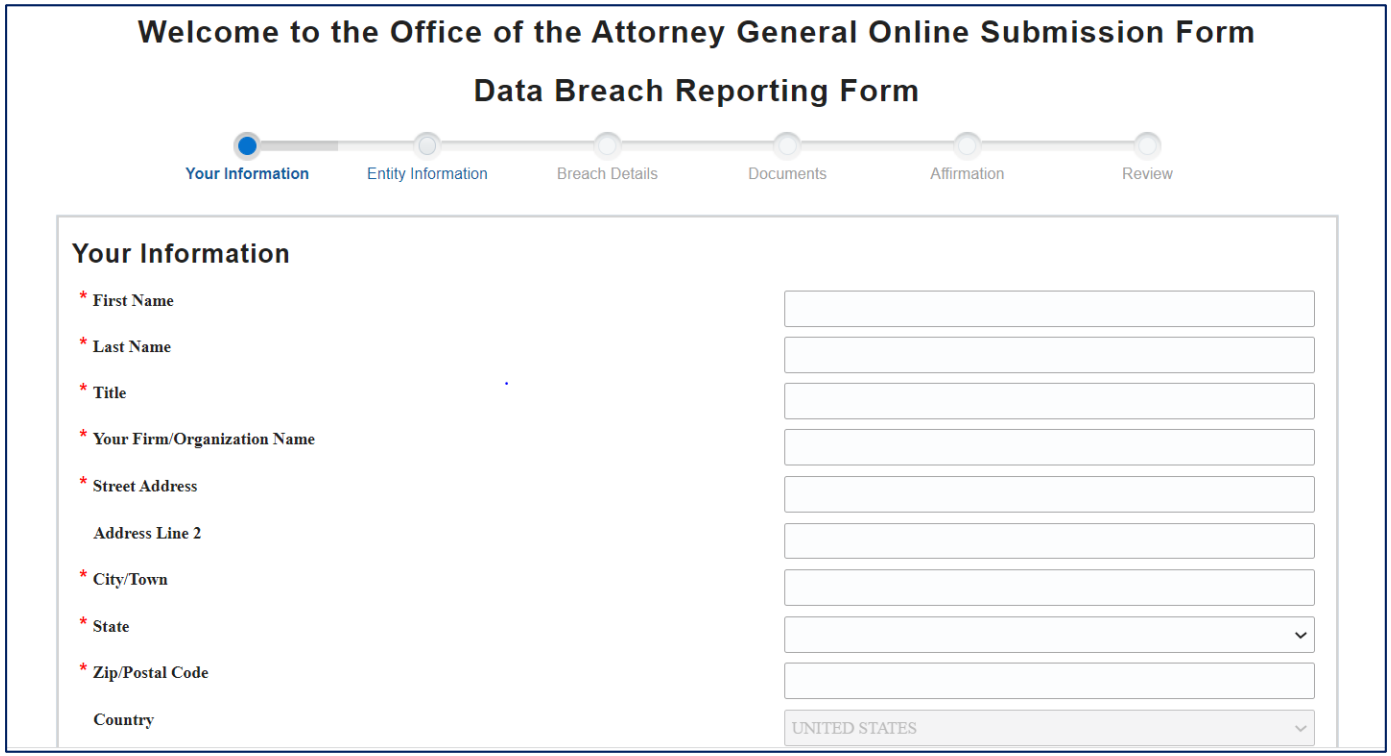
* **Please select one of the following to proceed**

- ☐ You are a private person or business reporting a data breach pursuant to General Business Law § 899-aa(2), or a "Covered Entity" required to provide notice to the U.S. Department of Health and Human Services under 45 C.F.R. § 164-408, pursuant to General Business Law § 899-aa(9). Your submission will also be sent to the New York Department of State and the New York State Police in satisfaction of your requirement to notify those agencies.
- ☐ You are a New York State government agency or entity reporting a data breach pursuant to New York State Technology Law § 208. Your submission will also be sent to the New York Department of State. You must provide separate notice to the New York State Office of Information Technology Services, as required by New York State Technology Law § 208-7(a).
- ☐ You are a private person or business reporting an inadvertent disclosure of over 500 New York residents pursuant to General Business Law § 899-aa (2)(a), for which you have determined will not likely result in misuse of the information.

Next >

https://formsnym.ag.ny.gov/OAGOnlineSubmissionForm/faces/OAGSBHome;jsessionid=M2KIbeUyp69u02tD0rwtqhH4CvWXW7uFYIEsUVHI9RMfd0Z6jYcR!828131627

Reporting Forms



Welcome to the Office of the Attorney General Online Submission Form

Data Breach Reporting Form

Your Information | Entity Information | Breach Details | Documents | Affirmation | Review

Your Information

* First Name
* Last Name
* Title
* Your Firm/Organization Name
* Street Address
  Address Line 2
* City/Town
* State
* Zip/Postal Code
  Country — UNITED STATES

https://formsnym.ag.ny.gov/OAGOnlineSubmissionForm/faces/OAGSBHome;jsessionid=M2KIbeUyp69u02tD0rwtqhH4CvWXW7uFYIEsUVHI9RMfd0Z6jYcR!828131627

Timing

- Federal Banking Agencies Notification Requirement
  - As soon as possible and no later than **36 hours** after the banking organization determines that a notification incident has occurred.
- New York State Law
  - Notification is required to be made in the most expedient time possible and without unreasonable delay.
  - Several states have more specific deadlines ranging from **30 to 45 days**.
- GDPR
  - Within **72 hours** after having become aware of the data breach.
- NYDFS
  - As promptly as possible but in no event later than **72 hours** from a determination that a "cybersecurity event" has occurred.

Other Regulatory Notification Requirements

- Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
  - When a financial organization becomes aware of an incident of unauthorized access to sensitive customer information, the organization should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the organization determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible.
  - The banking agencies adopted a new rule, since they believe that this standard does not include all computer-security incidents of which the agencies, as supervisors, need to be alerted and would not always result in timely notification to the agencies.
- Regulation SCI (Systems Compliance and Integrity)
  - Applies to financial market utilities or FMUs, which is "any person that manages or operates a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and the person."
  - Notification is to the SEC or CFTC, as applicable.

Proposed FTC Notification Rule (as part of the Safeguards Rule)

Applicability: The rule would apply to "financial institutions" which means all businesses, regardless of size, that are "significantly engaged" in providing financial products or services. This includes, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, and courier services. The rule would also apply to companies like credit reporting agencies and ATM operators that receive information about the customers of other financial institutions.

Trigger: a security event where the financial institution determines misuse of customer information has occurred or is reasonably likely, and where at least 1,000 consumers have been affected or reasonably may be affected.

Timing: as soon as possible, and **no later than 30 days** after discovery of the event.

Form of Notification: Financial institutions would be required to promptly provide the FTC (1) The name and contact information of the reporting financial institution; (2) a description of the types of information involved in the security event; (3) if the information is possible to determine, the date or date range of the security event; and (4) a general description of the security event. The notice would be provided electronically through a form located on the FTC's website.

More to Note: In its proposal, the FTC stated that even if state law already requires notification to consumers or state regulators, notice would still be required to the FTC. Many of the aspects of the rule may be subject to change, as the FTC has requested input from commentators.

Proposed SEC Notification Rule

Applicability: The rule would apply to SEC-registered investment advisers and investment companies.

Trigger: a cybersecurity incident, or a group of related incidents, that significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in (1) substantial harm to the adviser, or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed. Similarly, an adviser would have to report significant fund cybersecurity incidents for its registered fund and business development company clients.

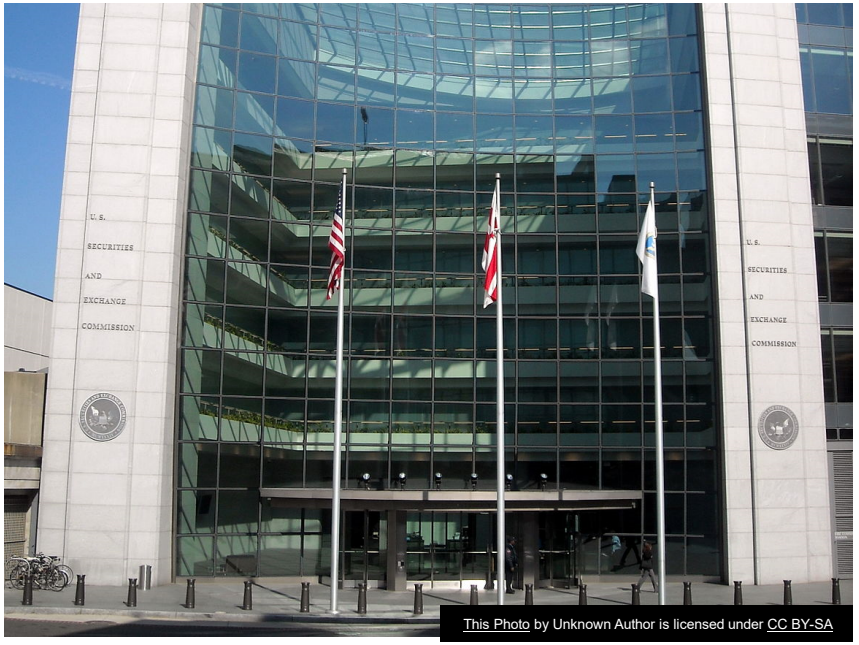
Timing: promptly, but in no event more than **48 hours**, after having a reasonable basis to conclude (there is no requirement to know definitively) that a significant adviser cybersecurity incident or a significant fund cybersecurity incident had occurred or is occurring.

Form of notification: newly proposed Form ADV-C to be filed via the Investment Adviser Registration Depository platform. The confidential form contains 16 detailed items for the advisers to disclose.

More to note: Advisers are also required to amend any previously filed Form ADV-C promptly, but in no event more than 48 hours, (1) after information reported on the form becomes materially inaccurate, (2) if new material information about a previously reported incident is discovered, and (3) after resolving a previously reported incident or closing an internal investigation pertaining to a previously disclosed incident. The Proposal states that the SEC or its staff could issue analyses and reports that are based on aggregated, nonidentifying Form ADV-C data.

More Regulatory Actions on the Horizon

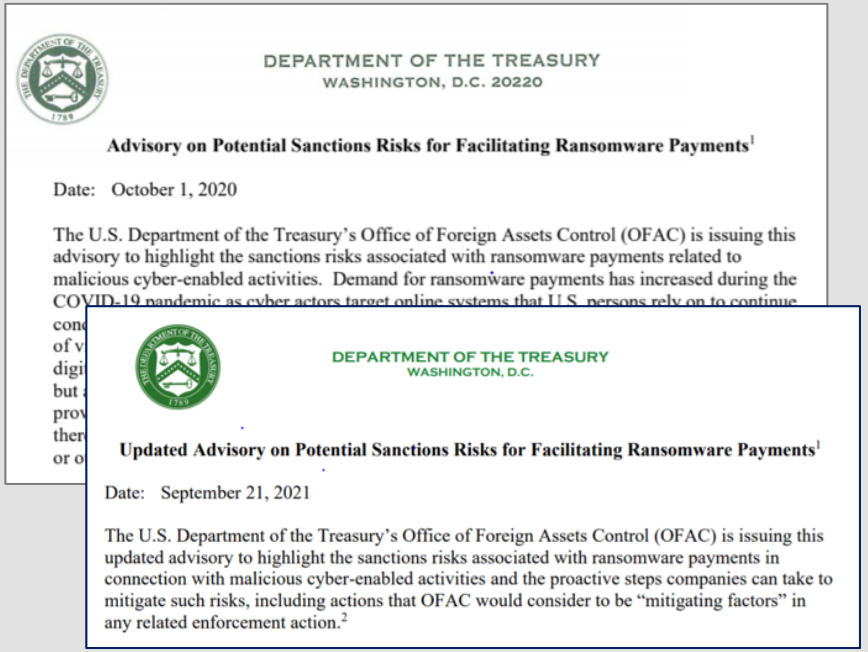
- The SEC has proposed enhanced cybersecurity disclosures for registered investment advisers, registered funds, and public companies focused on cybersecurity incidents (and often within a short time frame following such an incident) and governance and controls for preventing such incidents.
- SEC Chair Gary Gensler indicated that further regulatory proposals should be expected regarding cybersecurity disclosures for broker-dealers, Regulation SCI, and intermediaries' requirements regarding customer notices (Regulation S-P).



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

- US 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."



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

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

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: September 21, 2021

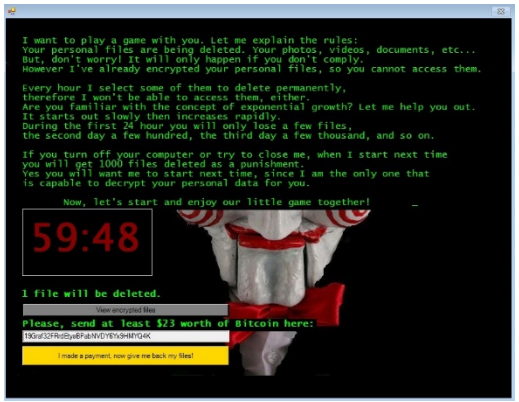
The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be "mitigating factors" in any related enforcement action.[2]

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


Hypothetical
Ransomware Attack
Morgan Lewis

Hypothetical Ransomware Attack

- A large international banking company experiences a ransomware attack
- Key Issues
  - When was incident discovered?
  - What was the scope of the incident?
  - Has a notification incident occurred?
  - What can you report in 36 or 72 hours?
  - Who to notify?
    - Which federal regulators?
    - Which state regulators?
    - Customers and individuals
  - What is the substance of the notification?



Complex Challenges for Hypothetical Bank

- Initial Questions
  - How is the incident discovered?
  - How long has the Threat Actor been in the network?
  - Has any data been compromised?
  - What is the impact on operations?
  - What is the scope of the incident?
- Timely Notifications
  - Review Notification Triggers
- Substance of Notifications
  - What do you know?
  - What to report?


What Next and How to Prepare?
Morgan Lewis

What Next and How to Prepare?

- Financial institutions should review policies, procedures, and contracts with service providers to ensure compliance with new requirements
- Conduct risk assessments
- Vulnerability management plan
- Identity and Access management
- Data classification program to identify sensitive and critical data
- Management and board role and oversight of cybersecurity risks
- Identify primary federal and state regulators
- Refresh their information security programs to ensure consistent with regulatory expectations
- Encrypt or tokenize sensitive and critical data in transit and at rest

What Next and How to Prepare?

- Maintain, update, and test Incident Response and Business Continuity Plans
- Back up and secure data
  - Offline or segregated
- Conduct regular employee trainings on key risk areas
- Keep security software up to date
- Review cybersecurity insurance policies
- Consider risks associated with remote work
- Address third party vendor issues and risks
- Address privilege and legal protection issues
- Consult with counsel for legal guidance—the earlier the better!

Questions

MARK L. KROTOSKI

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

Litigation Partner, Privacy and Cybersecurity and Antitrust practices

- Co-Head of Privacy and Cybersecurity Practice
- Litigates, responds to a data breach, directs confidential cybersecurity investigations, responds to federal and state regulatory investigations, coordinates with law enforcement on cybercrime issues, mitigates and addresses cyber risks, and develops cybersecurity protection plans.
- 25 years' experience handling a broad range of complex and novel cyber cases and investigations under the Computer Fraud and Abuse Act, Economic Espionage Act, Defend Trade Secrets Act, and other statutes.
- 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.

CHARLES M. HORN

Charles M. Horn
Washington, DC
charles.horn@morganlewis.com
+1.202.739.5951

Charles M. Horn counsels US and international banks and other financial institutions on corporate, regulatory, supervisory, enforcement, and compliance matters before all major federal and state financial regulatory agencies. He advises clients on major federal financial services statutes and regulations, as well as on US and international financial reform developments. Charles also counsels banks and other financial services firms on issues affecting their governance, structure, management, and operations.

He also counsels clients on financial institutions laws that include the National Bank Act, the Bank Holding Company Act, the Federal Reserve Act, the Federal Deposit Insurance Act, the International Banking Act, and the Dodd–Frank Wall Street Reform and Consumer Protection Act. Additionally, he guides clients on global regulatory capital requirements and key state banking law requirements.

MARTIN HIRSCHPRUNG

Martin Hirschprung
New York
martin.hirschprung@morganlewis.com
+1.212.309.6837

Martin Hirschprung's practice involves counseling US and international banks and non-bank financial services companies on corporate, regulatory, and compliance matters. He advises clients on major state and federal financial services statutes and regulations, including data protection, anti-money laundering, fiduciary duties, consumer lending, licensing, and transactional matters. Martin is a member of the firm's Privacy and Cybersecurity practice and a Certified Information Privacy Professional/United States (CIPP/US).

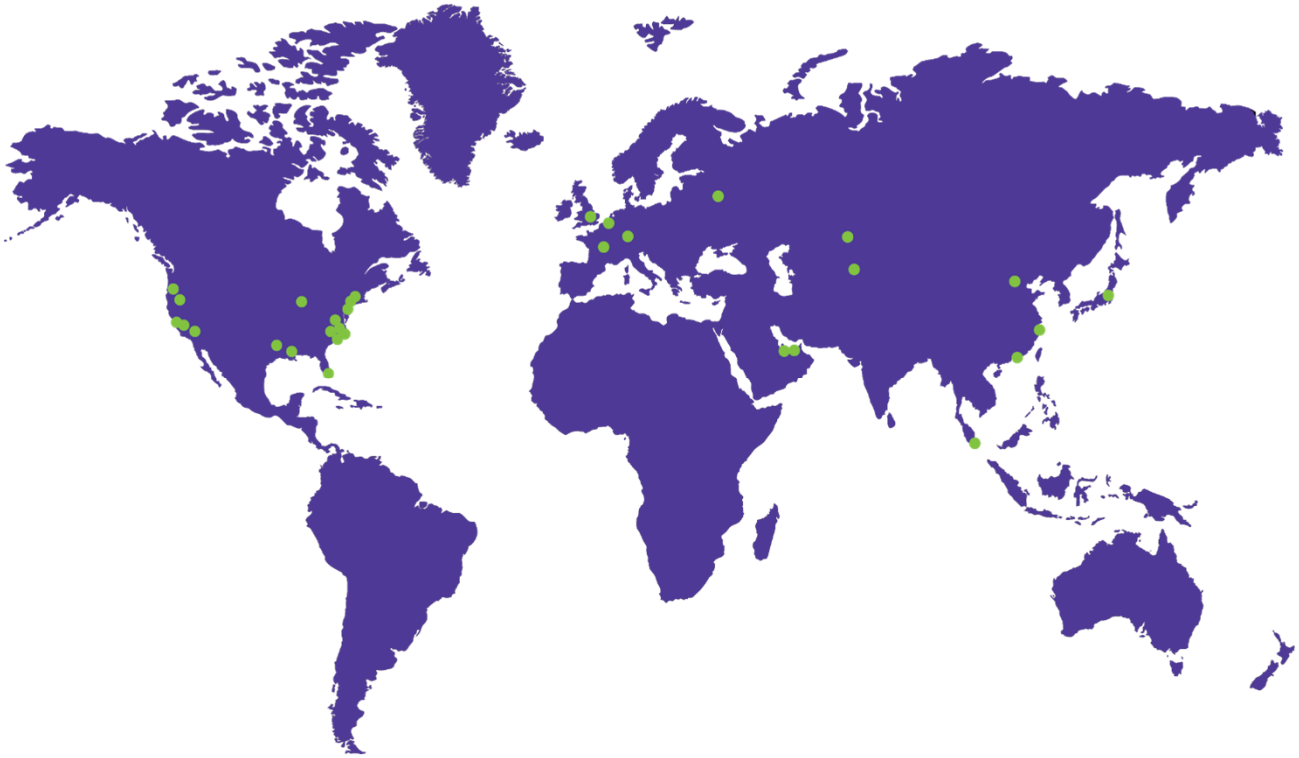
He works with companies on designing and building aspects of their privacy programs, including internal policies, procedures, and guidelines that incorporate best practices and legal requirements. Martin also represents mutual fund complexes, their independent trustees and investment advisers in a number of areas, including SEC filings, and regulatory and compliance issues.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

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



Morgan Lewis

THANK YOU