

Morgan Lewis

# TECHNOLOGY MARATHON

**New Cybersecurity Rules Impacting  
Financial Services Companies**

Elizabeth Goldberg, Mark Krotoski, Martin Hirschprung

**May 16** | 2:00-3:00 pm ET

# Presenters



**Elizabeth Goldberg**



**Mark Krotoski**



**Martin Hirschsprung**

**Morgan Lewis**

# Preliminary Note

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

# Overview: New Cybersecurity Rules Impacting Financial Services Companies

- Cyber Risk Landscape
- Conducting A Cyber Investigation
- Proposed Cybersecurity Incident Reporting for Investment Advisors and Broker-Dealers and Risk Management for Broker Dealers
- Notification Standards
- DOL Guidance DOL
- What Next and How to Prepare?

# Cyber Risk Landscape

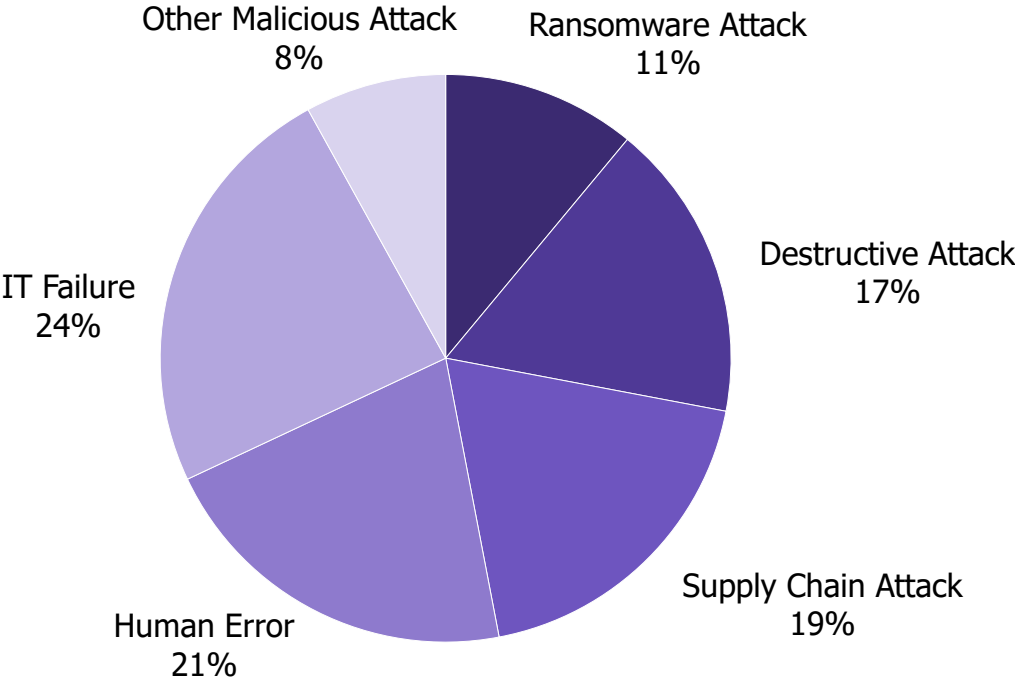
The background of the slide is a vibrant, abstract digital landscape. It features a dark blue and purple color palette with numerous glowing elements. Binary code (0s and 1s) is scattered throughout, some appearing as large, semi-transparent characters. There are also bright blue light streaks and lines that create a sense of motion and depth, suggesting a complex network or data flow. The overall aesthetic is high-tech and futuristic.

Morgan Lewis

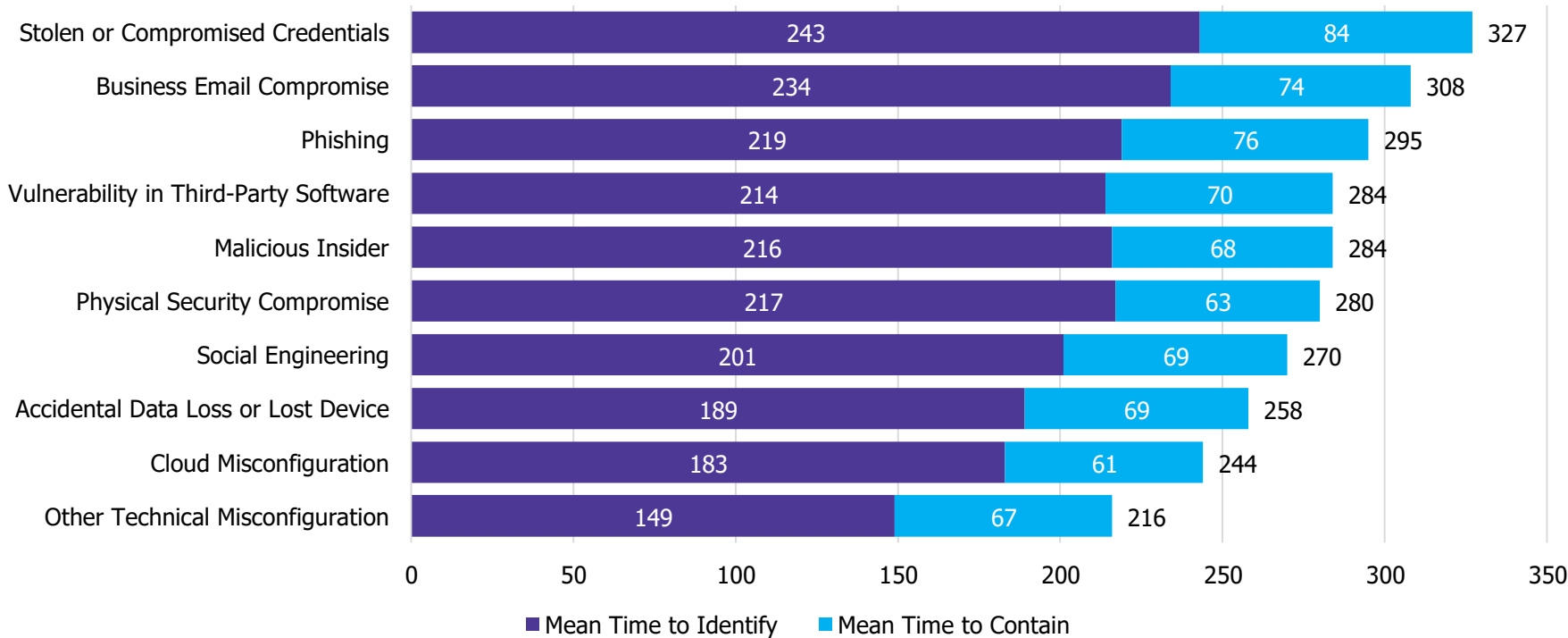
# Cyber Landscape and Risks



# Types of Breaches Experienced by Organizations



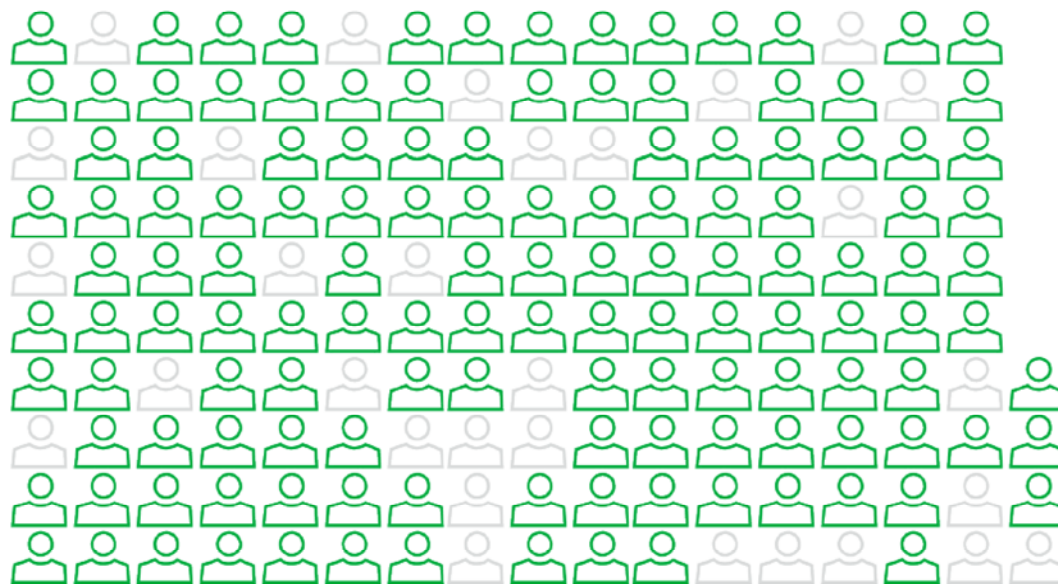
# Average Time to Identify and Contain a Data Breach by Initial Attack Vector





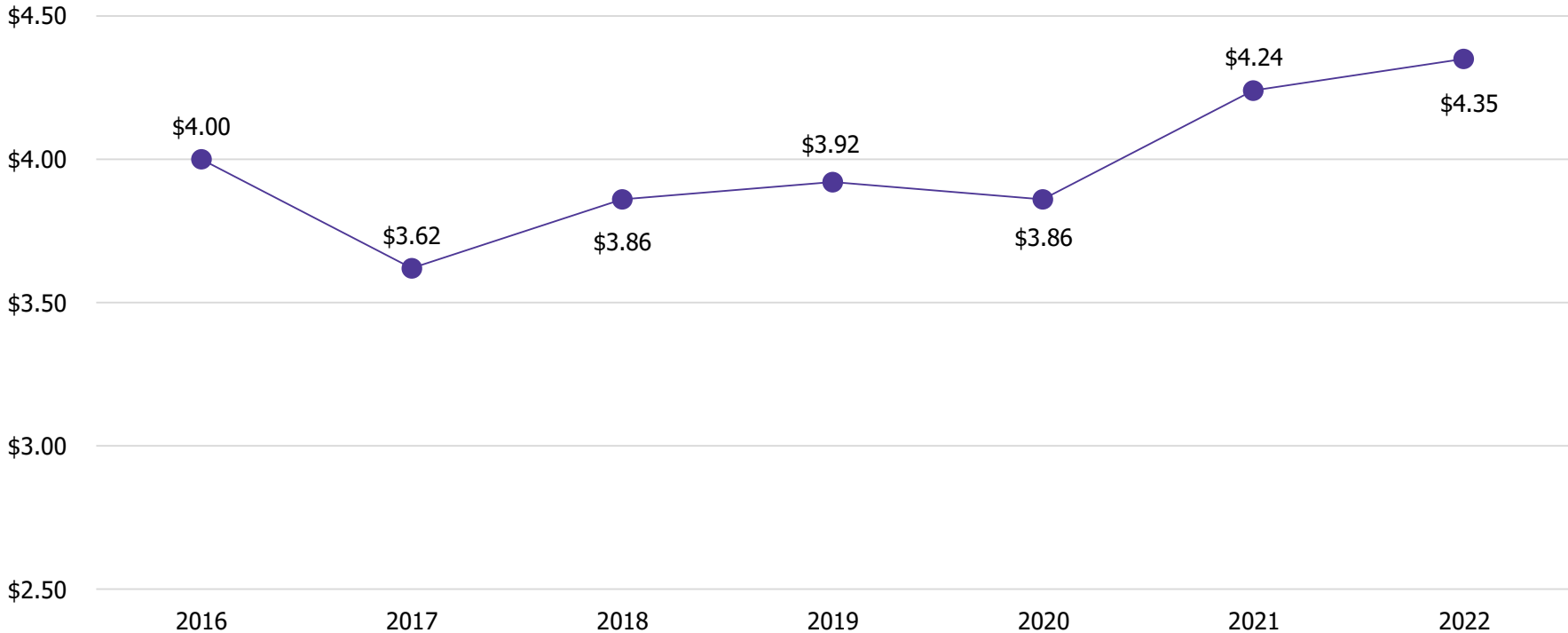
# Human Element

- “The human element continues to drive breaches. This year **82% of breaches involved the human element.**
- “Whether it is the Use of stolen credentials, **Phishing, Misuse, or simply an Error,** people continue to play a very large role in incidents and breaches alike.”

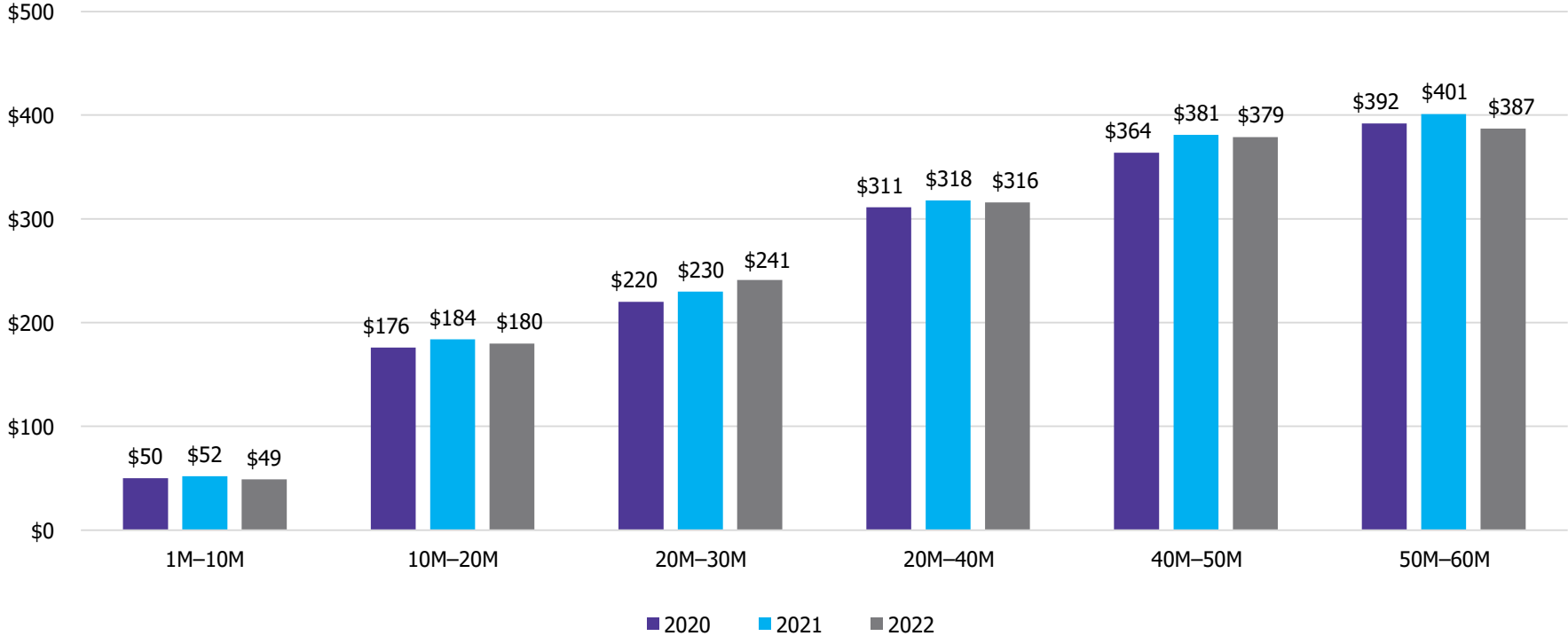


**Figure 9.** The human element in breaches (n=4,110)  
Each glyph represents 25 breaches.

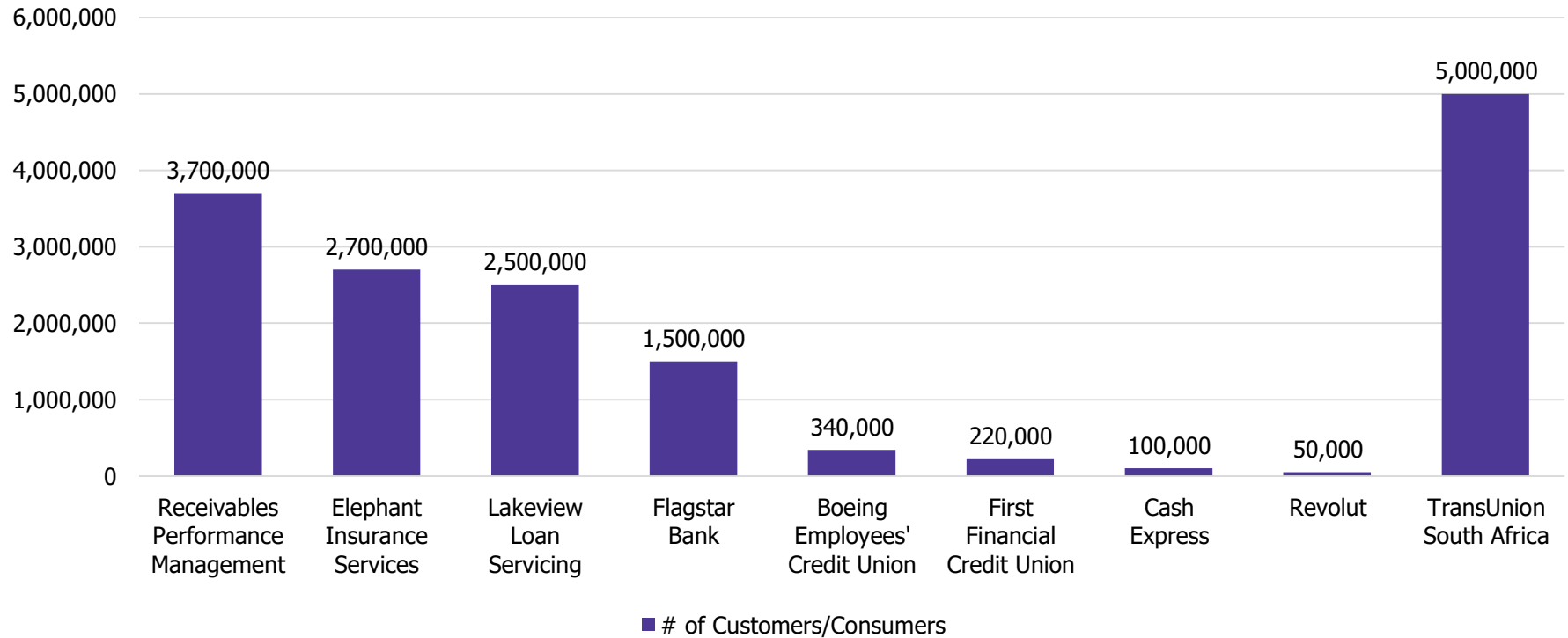
# Average Total Cost of a Data Breach



# Average Cost of a Mega Breach by Number of Records Lost<sup>(1)</sup>



# Largest Financial Data Breaches of 2022



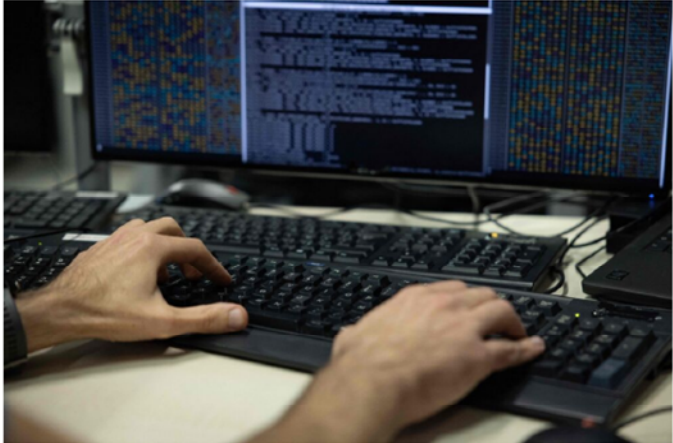
# Targeting Financial Industry

- “[R]ansomware remained the biggest concern. The increase in attacks was likely due to the proliferation of the **ransomware-as-a-service model**, in which hacking groups provide ‘affiliates’ with the malware and services necessary to carry out an attack, in exchange for a share of the criminal proceeds.”

Business  
Cybersecurity

## Banks, Financial Industry Hit by Rising Ransomware Attacks

- More hacks against sector come amid other, more positive signs
- Industry group says AI may lower barriers for cybercriminals



Photographer: Thomas Samsom/AFP/Getty Images

By **Andrew Martin**  
March 21, 2023 at 6:00 AM PDT

# Cyber Threat



[About Us](#)

[Our Offerings](#)

[Events](#)

[Insights](#)

[Knowledge](#)

[Newsroom](#)

[Join Us](#)



## FS-ISAC REPORT FINDS GLOBAL CYBER THREATS ACCELERATE AS CYBER CRIMINALS AND NATION-STATE ACTORS CONVERGE AND COLLABORATE

*Third-party risk, zero-day vulnerability exploits, and ransomware will remain at the forefront of the cyber threats facing financial institutions in 2022*

FS-ISAC expects the **trifecta of third-party risk, the growth in zero-day vulnerabilities as an attack vector, and the ability of ransomware groups to adapt** despite increased scrutiny by law enforcement to complicate an already challenging cyber threat environment.


Looking ahead to 2022, FS-ISAC expects the trifecta of third-party risk, the growth in zero-day vulnerabilities as an attack vector, and the ability of ransomware groups to adapt despite increased scrutiny by law enforcement to complicate an already challenging cyber threat environment.

# Department of Homeland Security Reporting

- 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>



# Conducting A Cyber Investigation



Morgan Lewis



# Legal Issues During Incident Response Phases

Preparation

Cyber Incident Detected

Cyber Investigation, Assessment, Analysis

Law Enforcement Report?

Containment and Eradication

Remediation, Recovery

Determine and Manage Notifications and Other Legal Issues

Public Statements, Business Relations, Address Reputational Issues

Anticipated Civil Litigation Issues

Potential Regulatory Review

# 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).



# Proposed Cybersecurity Incident Reporting for Investment Advisors and Broker-Dealers and Risk Management for Broker Dealers

Morgan Lewis

# Overview of Proposed Cybersecurity Rules

## Applicability

- Registered investment advisers
- Registered investment companies
- Registered broker-dealers

## Background

- Growing number of cybersecurity risks for advisers and funds
- No existing SEC requirement to notify affected individuals in the event of a data breach

## Proposal Elements

- Notify individuals whose sensitive customer information was or is reasonably likely to have been accessed or used without authorization.
- Develop, implement, and maintain written policies and procedures for an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information.

## Comment Period

- The comment period will end on June 5, 2023

# Incident Notification

- Notification is required if “sensitive customer information” was, or is reasonably likely to have been, “accessed or used” without authorization.
  - Sensitive customer information means any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information.
- A customer notice must be clear and conspicuous and provided by a means designed to ensure that each affected individual can reasonably be expected to receive it.
  - The notice should include key information with details about the incident, the breached data, and how affected individuals could respond to the breach to protect themselves.
  - It should also include contact information sufficient to permit an affected individual to contact the covered institution to inquire about the incident, including a telephone number (which should be a toll-free number if available), an email address or equivalent method or means, a postal address, and the name of a specific office to contact for further information and assistance.
- Notice must be provided as soon as practicable but no later than 30 days after becoming aware that the incident occurred or is reasonably likely to have occurred.



# Risk Management Framework for Broker Dealers

Simultaneously, the SEC proposed a new cybersecurity risk management requirement for broker-dealers and “Market Entities” that mirrors the recently proposed risk management requirement for investment advisers and investment companies.

- Cybersecurity policies and procedures would be required to include the following elements:
  - Periodic risk assessments;
  - User security and access;
  - Information protection (including oversight of third parties);
  - Cybersecurity threat and vulnerability management; and
  - Cybersecurity incident detection, response, and recovery.
- At least annually, broker dealers would be required to (1) review the effectiveness of their policies and procedures, and (2) prepare a written report.

# Reporting to the SEC

- Broker Dealers would be required to submit Form SCIR to the SEC promptly, but in no event more than 48 hours, after having a reasonable basis to conclude that a significant cybersecurity incident had occurred or is occurring.
- Trigger: a cybersecurity incident, or a group of related incidents, that significantly disrupts or degrades the broker dealer's ability to maintain critical operations, or leads to the unauthorized access or use of the broker-dealer's information or information systems, where the unauthorized access or use of such information results in (1) substantial harm to the entity, or (2) substantial harm to a customer, counterparty, member, registrant, or user of the entity, or to any other person that interacts with the entity.
- BDs would be required to amend any previously filed Form SCIR, within 48 hours:
  - (1) After information previously reported becomes materially inaccurate;
  - (2) If additional or new material information about a previously reported incident is discovered; or
  - (3) After resolving a previously reported incident or closing an internal investigation relating to a previously reported incident.



# Related Regulatory Actions

- The SEC is also proposing to broaden and align the scope of the Safeguards Rule and Disposal Rule (related to disposal of collected information) to cover “customer information,” a new defined term. This change would expand those rules to both nonpublic personal information that a Covered Entity collects about its own customers and to nonpublic personal information that a Covered Entity receives about customers of other financial institutions. The new notification requirement only relates to the first subset of information.
- In March 2022, the SEC proposed new rules and amendments to mandate disclosure regarding cybersecurity risk management, strategy, governance, and incident reporting, including amendments to Form 8-K, Form 10-Q and Form 10-K.



# SEC Focus on Cybersecurity

- SEC Division of Examination 2023 Priorities
- SEC Risk Alerts
- Enforcement Actions



[This photo](#) by Unknown Author is licensed under [CC BY-NC](#)

# Three Recent Actions Charging Deficient Cybersecurity Procedures (August 2021)

- Eight firms were charged in three actions for failures in their cybersecurity policies and procedures that resulted in email account takeovers exposing the personal information of thousands of customers and clients at each firm.
- Two of the firms also sent breach notifications to clients that included misleading language suggesting that the notifications had been issued much sooner after discovery of the incidents than they actually were.
- The firms settled with the SEC for fines ranging from \$200,000 to \$300,000.

# Previous Significant Enforcement Actions

## **Investment Adviser (Sept. 2015)**

- First SEC cybersecurity enforcement case.
- The SEC found that investment adviser R.T. Jones failed to establish required cyber policies and procedures under Regulation S-P in advance of a breach that exposed PII of approximately 100,000 individuals.
- \$75,000 penalty.

## **Global Financial Institution (June 2016)**

- The SEC concluded that a global financial institutional had failed to adopt written policies and procedures reasonably designed to protect customer data and the company paid a \$1 million penalty.
- A former employee improperly accessed and transferred data from more than 700,000 accounts to his personal server, which was then hacked by a third party, conduct for which he was criminally convicted.

## **Financial, Retirement, Investment and Insurance Company (Sept. 2018)**

- The SEC charged this broker-dealer and investment adviser, with violation of the Safeguards Rule in connection with a massive data breach in 2016.
- The company was fined \$1 million.

# Enforcement Actions Against Public Companies for Disclosure Violations

## Title Insurance Company

- 2021
- The company failed to maintain disclosure procedures designed to ensure that the company's senior management received relevant information about the identified vulnerability or lack of remediation.
- The company agreed to a cease-and-desist order and a \$487,616 civil monetary penalty.

## Media Company

- 2021
- In a media statement, the company referred to the breach as hypothetical when the breach had in fact occurred and claimed that it had “strict protections” in place to prevent such a breach when it had known for six months about the vulnerability that led to the breach.
- The company agreed to cease and desist from committing violations of these provisions and was asked to pay a \$1 million civil penalty.

# 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



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 § 200-7(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 >

# 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

# 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.

# DOL Guidance

Morgan Lewis

# ERISA 101

- ERISA regulates private employee benefit plans and assets.
- ERISA imposes fiduciary duties of loyalty and prudence.
- Fiduciary duties apply to:
  - “Plan sponsor” fiduciaries
  - Asset managers and administrative service providers that accept ERISA fiduciary status by contract or in their actions
- However, ERISA’s standards can impact asset managers and administrative service providers that are not ERISA fiduciaries



# ERISA and Cybersecurity

## Cybersecurity Incidents Involving ERISA Plan Assets Are Happening

Public report of plan participants' accounts being accessed and unauthorized distributions being made (e.g., \$245K, \$400K, \$99K).

In some cases, this has resulted in litigation

## Possible Fiduciary Duty

ERISA's prudence standard may require fiduciaries to be proactive and reactive to ever-changing data security threats (mostly by monitoring service providers)

## DOL Guidance Issued in 2021

1) Tips for Hiring a Service Provider with Strong Cybersecurity Practices  
DOL view of "best practices" for plan fiduciaries when hiring a service provider

2) Cybersecurity Program Best Practices  
DOL view of 12 "best practices" for recordkeepers and other service providers  
Often aligns with industry standards

3) Online Security Tips  
Tips for participants

## DOL Conducting Investigations

At the same, the DOL has been conducting civil investigations related to cybersecurity practices

# DOL Guidance: Tips for Hiring a Service Provider

**Guidance to Plan Sponsors:** Tips for plan fiduciaries when hiring a service provider; largely focused on hiring **recordkeepers** and **custodians/trustees**, (but question about application to other service providers, like asset managers).

## Tips 1–3

1. Ask about the service provider's data security standards, practices, policies, and audit results and benchmark those against industry standards.
2. Analyze the service provider's security standards and security validation practices.
3. Evaluate the service provider's track record in the industry.

## Tips 4–6

4. Ask about past security events and responses.
5. Confirm that the service provider has adequate insurance coverage for losses relating to cybersecurity and identity theft events.
6. Ensure that the services agreement between the plan fiduciary and the service provider includes provisions requiring ongoing compliance with cybersecurity standards.

# DOL Guidance: Service Provider Best Practices

**Guidance to Service Providers:** Practices that plan service providers “should” implement to mitigate risks. Largely directed to **recordkeepers** and **custodians/trustees**, (but question about application to other service providers, like asset managers).

## Practices 1–6

1. Have a formal well-documented cybersecurity program
2. Conduct prudent annual risk assessments
3. Have a reliable annual third-party audit of security controls
4. Clearly define and assign information security roles and responsibilities
5. Have strong access-control procedures
6. Ensure that any assets or data stored in a cloud or managed by a third party are subject to appropriate safeguards

## Practices 7–12

7. Conduct periodic cybersecurity training
8. Implement and manage an SDLC program
9. Have an effective business resiliency program addressing BCDR and incident response
10. Encrypt sensitive data, stored and in transit
11. Implement strong technical controls in accordance with best practices
12. Appropriately respond to any past cybersecurity incidents

# What Might this Mean for Vendors to ERISA Plans

- **What might this mean for vendors to ERISA plans**
  - Vendors that are ERISA fiduciaries might be subject to DOL guidance and/or face litigation and investigation risks.
  - But even if NOT an ERISA fiduciary, may still be subject to litigation or investigator risks.

# A Recent Cautionary Tale Involving a Non-Fiduciary Vendor

In February 2021, the DOL filed subpoena enforcement in Illinois by recordkeeper.

- A national recordkeeper contested the DOL's investigatory authority because, among other reasons, the service provider was not a fiduciary, the DOL has not articulated any conduct constituting a violation of ERISA, and the subpoena was too broad.
- The DOL objected and filed subpoena enforcement, arguing that it "may seek information that 'might assist in determining whether any person is violating or has violated any provision of Title I of ERISA.'"
- The DOL litigated the case up to the Court of Appeals for the 7<sup>th</sup> Circuit and won. The court found:
  - DOL's enforcement and subpoena power extends to **non-fiduciaries** and is not simply limited to named or implied fiduciaries of a plan.
  - DOL has the authority to **investigate cybersecurity practices**.

# What Might this Mean for Vendors to ERISA Plans (con't)

- **How can we help?**

- Help with navigating the DOL guidance and enforcement and litigation risks.
- Help in the event of a breach or incident involving ERISA assets or data.
- Help with contract/side letter negotiations.

# Practical Steps to Respond to This Guidance

**Review the guidance** and consider direct changes or working with service providers to ensure that existing data security protocols reflect the best practices set forth by the DOL.

**Consider fiduciary training** on how best to address fiduciary exposure to cybersecurity events.

**Consider reviewing plan documents**, including SPDs and participant communications.

**Consider contract terms**, especially older contracts.

**Consider questionnaires for vendors (and vendors, proactive communications to plans)**

**Consider establishing formal procedures** designed to ensure that cybersecurity issues are regularly considered and properly addressed.

**Consider educating participants** as to their obligations with respect to cybersecurity and advising them of the DOL's *Online Security Tips*.

**Consider engaging counsel and third-party vendors** to conduct a benefit plan cybersecurity audit to analyze potential weaknesses in cybersecurity practices and the best way to resolve such weaknesses.

- There may be value to engaging third-party vendors through counsel in order to maintain privilege.

# ERISA and Data

- **A New Area of Risk: ERISA and Data Usage**

- Plaintiffs have filed cases alleging that plan fiduciaries breached their ERISA fiduciary duties by allowing recordkeepers/administrators to use plan data for cross-selling.
- Plaintiffs allege that data used for cross-selling is a plan asset and therefore the data must be used in the best interest of participants.
- Cases include:
  - *Harmon v. Shell Oil Co.* No. 3:20-cv-00021 (S.D. Tex. Mar. 30, 2021)
  - *Divane v. Northwestern University*, 2018 US Dist. LEXIS 87645 (N.D. Ill. May 25, 2018), *aff'd*, 953 F.3d 980 (7th Cir. 2020), *rev'd on other grounds*, *Hughes v. Northwestern University*, No. 19-1401 (Jan. 24, 2022)
- A number of settlements have been conditioned on limiting vendor use of data.



# ERISA and Data

- Regulatory Risks: DOL
  - The DOL's long-held position is that plan assets are determined based on an ordinary notion of property rights.
    - If data is property of a participant (or plan), one would expect the DOL to view it as a plan asset.
  - The DOL is currently prioritizing cybersecurity in investigations and has asked about the use of plan data by the plan vendor.
- To our knowledge, no court has found plan data to be a plan asset.
- This means that currently there is no judicial decision holding that the challenged practices breach ERISA.
- But risks remain...

# 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

**Morgan Lewis**



# 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!



# ELIZABETH S. GOLDBERG



Pittsburgh

+1.415.560.7428

[elizabeth.goldberg@morganlewis.com](mailto:elizabeth.goldberg@morganlewis.com)

Elizabeth (Liz) Goldberg advises employee benefit plan sponsors and service providers to those plans (including financial service firms) on ERISA US Department of Labor (DOL) enforcement investigations, DOL ERISA regulatory matters, and ERISA fiduciary counseling and compliance.

Liz has broad experience representing both plan and service provider clients in DOL ERISA investigations. Liz has worked on more than 30 such DOL investigations including matters that have involved significant monetary disputes or enterprise risk. In assisting in such matters, Liz draws on her prior work experience that includes six years at the DOL's Office of the Solicitor, primarily as an ERISA litigator. Liz also works with clients to perform internal audits to minimize any potential liability related to DOL investigations or ERISA litigation.

Liz's experience also includes other matters before the DOL, including prohibited transaction exemption applications and representing clients in other DOL regulatory processes (such as ERISA rulemaking).

Liz advises fiduciaries and related parties and service providers on ERISA fiduciary compliance including on ERISA's fiduciary rules, governance issues, and prohibited transaction exemptions. This includes her work with fiduciaries on governance issues, such as setting up fiduciary committees and drafting investment policies. She also provides related counseling on general employee benefit plan issues, such as tax qualification rules.

# MARK L. KROTOSKI



Silicon Valley

Washington DC

+1.650.843.7212

+1.202.739.5024

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

# MARTIN HIRSCHPRUNG



New York

+1.212.309.6837

[martin.hirschprung@morganlewis.com](mailto:martin.hirschprung@morganlewis.com)

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).

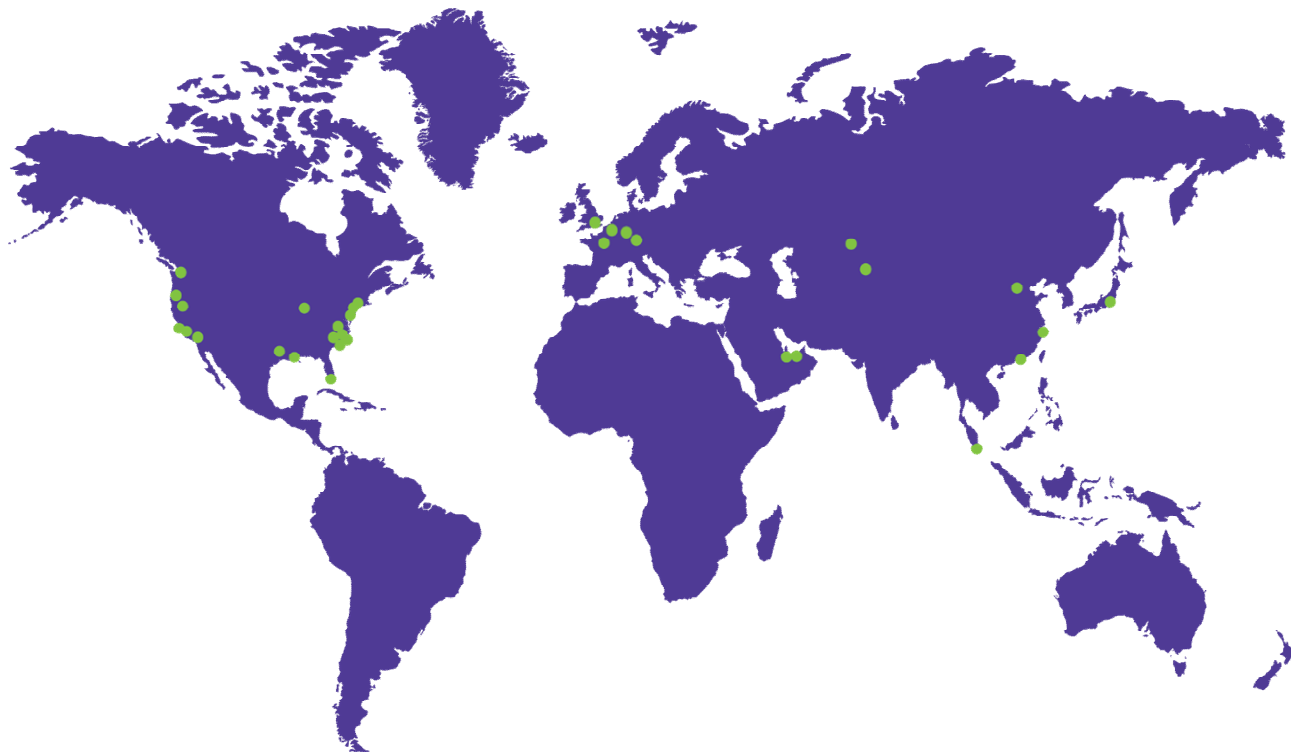
He works with companies on designing and building aspects of their privacy programs, including internal policies, procedures, and guidelines that incorporate best practices and legal requirements. Martin also represents mutual fund complexes, their independent trustees and investment advisers in a number 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  
Astana  
Beijing  
Boston  
Brussels  
Century City  
Chicago  
Dallas  
Dubai  
Frankfurt  
Hartford  
Hong Kong  
Houston  
London  
Los Angeles  
Miami  
Munich  
New York  
Orange County  
Paris  
Philadelphia  
Pittsburgh  
Princeton  
San Francisco  
Seattle  
Shanghai  
Silicon Valley  
Singapore  
Tokyo  
Washington, DC  
Wilmington



**Morgan Lewis**

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



# THANK YOU

© 2023 Morgan Lewis

Morgan, Lewis & Bockius LLP, a Pennsylvania limited liability partnership

Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

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

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP.

In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong.

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.