

Morgan Lewis

**SPOTTING AND MITIGATING ENFORCEMENT
ISSUES CONCERNING CYBERSECURITY-RELATED
CONTROLS AND DISCLOSURES**

September 9, 2020



Presenters



Susan D. Resley



Andrew J. Gray IV


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.

Are You Prepared for Regulatory and Litigation Risks?

1. Hypothetical scenario
2. Key cyber risks
3. Enforcement risks and responding to SEC, DOJ, other Regulators
4. Notification and disclosure obligations
5. Establishment of effective internal controls
6. Insider trading prevention
7. Recommended best practices



Enforcement risks and responding to SEC, DOJ, other Regulators

Morgan Lewis

Enforcement Risks and Considerations

- Federal Law Enforcement (FBI/DOJ)
- Securities and Exchange Commission
- Federal Trade Commission
- Other Federal/State Agencies (HHS, FCC, FINRA, etc.)
- State Attorneys General
- Civil Class Actions

Principal

- **DOJ Cybersecurity Unit
FBI Cyber Action Team**

- Specialized training in 94 US Attorney's Offices/56 FBI field offices
- Criminal investigation/prosecution of hackers

- **SEC Cyber Unit**

- Established Sept. 2017 to "target cyber-related misconduct"
- Civil enforcement of insider trading, market manipulation, public company disclosure and controls, safeguarding financial consumer information



Addressing Notification and Disclosure Obligations

Morgan Lewis

Notification and Disclosure Obligations

If a breach occurs, who should be notified?

- **Law Enforcement?**
 - FBI/Local Authorities (potential criminal activity)
- **Investors?**
 - SEC Filings (disclosure of *material* cybersecurity risks and incidents)
- **Potentially Affected Parties?**
 - Individuals (personal identifying information of consumers, employees)
 - Organizations (e.g., vendors, contractors, financial institutions)
 - Civil Regulators (responsible for oversight of individual notifications)

Notification Considerations: Law Enforcement

- **Criminal Law Enforcement & National Security**
 - FBI Cyber Action Team (56 field offices)
 - Local Police
 - DHS National Cybersecurity and Communications Integration Center
- **Civil Regulators**
 - SEC (e.g., potential insider trading)
 - Federal Trade Commission
 - State AGs and Regulators (varies by state)
 - Industry- and breach-specific (e.g., FDIC, IRS, GSA)

Notification Considerations: Affected Third Parties

- **Federal Law**
 - Federal Trade Commission (regulation of consumer notifications)
 - Other industry-specific regulations (e.g., HHS, FCC)
- **State Law**
 - All 50 states have enacted notification laws
 - Various definitions of (e.g.) “personal information”; what constitutes a breach; timing and content of notice; and exemptions
- **Foreign Law**
 - General Data Protection Regulation (EU)

Disclosure to Investors

Feb. 21, 2018 SEC Staff Interpretive Guidance

- Material risks and incidents must be disclosed
- Timely and complete disclosures
- The obligation to disclose cybersecurity risks and incidents arises from “a number of” requirements under existing reporting rules
- Emphasizes importance of cybersecurity to SEC (but offers limited *new* guidance)
 - SEC has acknowledged: “meaningful disclosure has remained elusive,” “provides only modest changes to the 2011 staff guidance,” and “essentially reiterates years-old staff-level views on this issue”

Disclosure to Investors: Materiality

What is a material event?

- “Tailored” to the company’s “particular cybersecurity risks and incidents”
- The “nature, extent, and potential magnitude” relative to the size of operations
- The “range of harm” that such incidents have caused or could cause
 - Reputation
 - Financial performance
 - Customer and vendor relationships
 - Possibility of litigation or regulatory investigations or actions
- Companies *need not* give a “roadmap” of internal systems to future intruders

Disclosure to Investors: Timing

When should disclosure occur?

- Periodic (Form 10-Q or 10-K) or immediate (Form 8-K) disclosure?
 - Cybersecurity risk versus incident
- Companies “may require time to discern the implications of a cybersecurity incident” before making a disclosure
 - But: an ongoing internal or external investigation cannot “provide a basis for avoiding disclosures of a material cybersecurity incident”
- Duty to Update: after an incident “companies should consider whether they need to revisit or refresh previous disclosure”

Disclosure to Investors: Timing

In the Matter of Altaba Inc., f/d/b/a Yahoo! Inc. (Apr. 2018)

- December 2014: Yahoo! officials allegedly discover theft of “crown jewels” (PII and encrypted passwords for 500+ million user accounts)
- September 2016: Yahoo! discloses breach in connection with potential acquisition by Verizon
- April 2018: Altaba (f/k/a Yahoo!) agrees to \$35M SEC fine for failure to disclose cyberattack to investors (e.g., 10-K and 10-Q risk factors; MD&A re impact on liquidity and net revenues)
 - \$80M settlement of securities class action; \$29M settlement of derivative class action; \$50M settlement* of consumer class action (*rejected by court)

Disclosure to Investors: Timing

SEC EDGAR Cyberintrusion

- 2016: SEC detects EDGAR intrusion
- August 2017: SEC discovers possibility of illicit trading
- September 2017: Public disclosure of breach
- January 2019: Insider trading charges filed

Disclosure to Investors: SEC Guidance

Where should disclosure occur?

- The description of general risk factors to investors;
- Management's discussion and analysis (MD&A) of potential financial or operational trends;
- The description of the registrant's business and market conditions;
- Potential legal proceedings;
- Financial statement disclosures before, during, and after a cyber incident; and
- Disclosure of controls and procedures jeopardized or impaired by cyber incidents.



Establishment of Effective Internal Controls

Morgan Lewis

Establishment of Effective Internal Controls

Per the 2018 Guidance, SEC expects companies to:

- “maintain comprehensive policies and procedures related to cybersecurity risks and incidents” that include:
- “appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity.”

Effective controls must ensure that incidents and risks are:

- timely “recorded, processed, summarized, and reported,” and
- “accumulated and communicated to the company’s management . . . as appropriate to allow timely decisions regarding required disclosures.”

Establishment of Effective Internal Controls

In the Matter of Voya Financial Advisors, Inc. (Sept. 2018)

- First SEC enforcement action under SEC's Safeguards Rule and Identify Theft Red Flags Rule (Fair Credit Reporting Act regulations)
- Cyber thieves allegedly impersonated Voya contractors to obtain password resets via Voya support line and stole personal information of 5,600 customers
- Voya allegedly did not update its Identify Theft Prevention Program after 2009
 - Voya did undertake prompt remedial acts, including (a) blocking the malicious IP addresses; (b) prohibiting provision of a temporary password by phone; and (c) issuing breach notices to the affected customers
- Voya nonetheless agreed to pay \$1M and retain independent consultant for evaluation of cybersecurity policies and procedures

Establishment of Effective Internal Controls

SEC Declination: Nine Public Companies (Oct. 2018)

- SEC found that nine publicly listed companies (not identified) were defrauded of nearly \$100M combined via spoofing/phishing email attacks
 - Hackers “spoofed” email accounts of executives and tricked finance personnel into transferring money to foreign bank accounts
 - Hackers broke into email accounts of actual vendors to demand payment for invoices
- SEC stressed that federal securities laws require companies to have procedures designed to prevent employees from making unauthorized transactions
- The victimized industries included technology, machinery, real estate, energy, financial and consumer goods; two companies lost more than \$30 million each

Disclosures to Investors: Cybersecurity risk factors

With regard to forward-looking risks, factors include:

- the occurrence of prior cybersecurity incidents;
- the probability and potential magnitude of cybersecurity incidents;
- the adequacy of preventative actions;
- the aspects of the company's business and operations that give rise to material risks;
- the costs associated with maintaining cybersecurity protections;
- the potential for reputational harm;
- existing or pending laws and regulations; and
- litigation, regulatory investigation, and remediation costs.

Disclosures to Investors: Management Discussion & Analysis

Cybersecurity disclosures may be required in MD&A discussion of financial condition and results of operations, specifically including:

- “the cost of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents, among other matters.”

Other relevant costs might include:

- “loss of intellectual property,
- the immediate costs of the incident, as well as the costs associated with implementing preventative measures,
- maintaining insurance, responding to litigation and regulatory investigations, preparing for and complying with proposed or current legislation, engaging in remediation efforts, addressing harm to reputation, and the loss of competitive advantage that may result.”

Disclosures to Investors: The Board of Directors

The 2018 SEC Guidance specifically notes that disclosure about how the board of directors oversees management's actions relating to cybersecurity risks is important to investors' assessment of risk oversight.

The SEC recommends that this discussion include:

- the nature of the board's role,
- how the board engages with management on cybersecurity issues, and
- as much transparency as practicable into the board's oversight of corporate cybersecurity assessments, policies, and procedures.



Insider Trading Prevention

Morgan Lewis

Trading

Elaborate International Hacking and Trading Scheme

- 2015: SEC charged 32 defendants in an international scheme to steal and trade on news wire information relating to corporate earnings releases.
- Hackers infiltrated news wire services to obtain corporate announcement information in advance of release
- Hacking ring provided information to traders who reaped over \$100 million over a **five-year period**
- Several traders and hackers were charged criminally

Insider Trading After Learning of Hack

Equifax Inc. Insider Trading Cases (March 2018)

- August 2017: Equifax detects data breach; former CIO exercises stock options
- September 2017: Equifax publicly discloses data breach
- March 2018: Criminal (DOJ) indictment and Civil (SEC) complaint charging former CIO with insider trading violations
- June 2018: SEC charges second Equifax employee for insider trading



Recommended Best Practices

Morgan Lewis

Best Practices

- **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, Bespond 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

Best Practices

- **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

Morgan Lewis

Biography



Andrew J. Gray IV

Silicon Valley

+1.650.843.7575

andrew.gray@morganlewis.com

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

Morgan Lewis

Biography



Susan D. Resley

San Francisco

+1.415.422.1351

susan.resley@morganlewis.com

Susan D. Resley serves as deputy practice leader of the firm's securities enforcement and litigation practice. Clients rely on Susan's guidance to counsel and defend them in regulatory matters concerning accounting and disclosure issues, insider trading, Foreign Corrupt Practices Act (FCPA) (including due diligence and compliance), internal controls, cybersecurity concerns, whistleblower-related issues, and Securities and Exchange Commission (SEC) or Financial Industry Regulatory Authority (FINRA) rules related to broker-dealers and investment advisors. She has represented clients in international investigations, including in the United Kingdom, France, China, Japan, Korea, and India.

Our Global Reach

Africa

Asia Pacific

Europe

Latin America

Middle East

North America

Our Locations

Abu Dhabi

Almaty

Beijing*

Boston

Brussels

Century City

Chicago

Dallas

Dubai

Frankfurt

Hartford

Hong Kong*

Houston

London

Los Angeles

Miami

Moscow

New York

Nur-Sultan

Orange County

Paris

Philadelphia

Pittsburgh

Princeton

San Francisco

Shanghai*

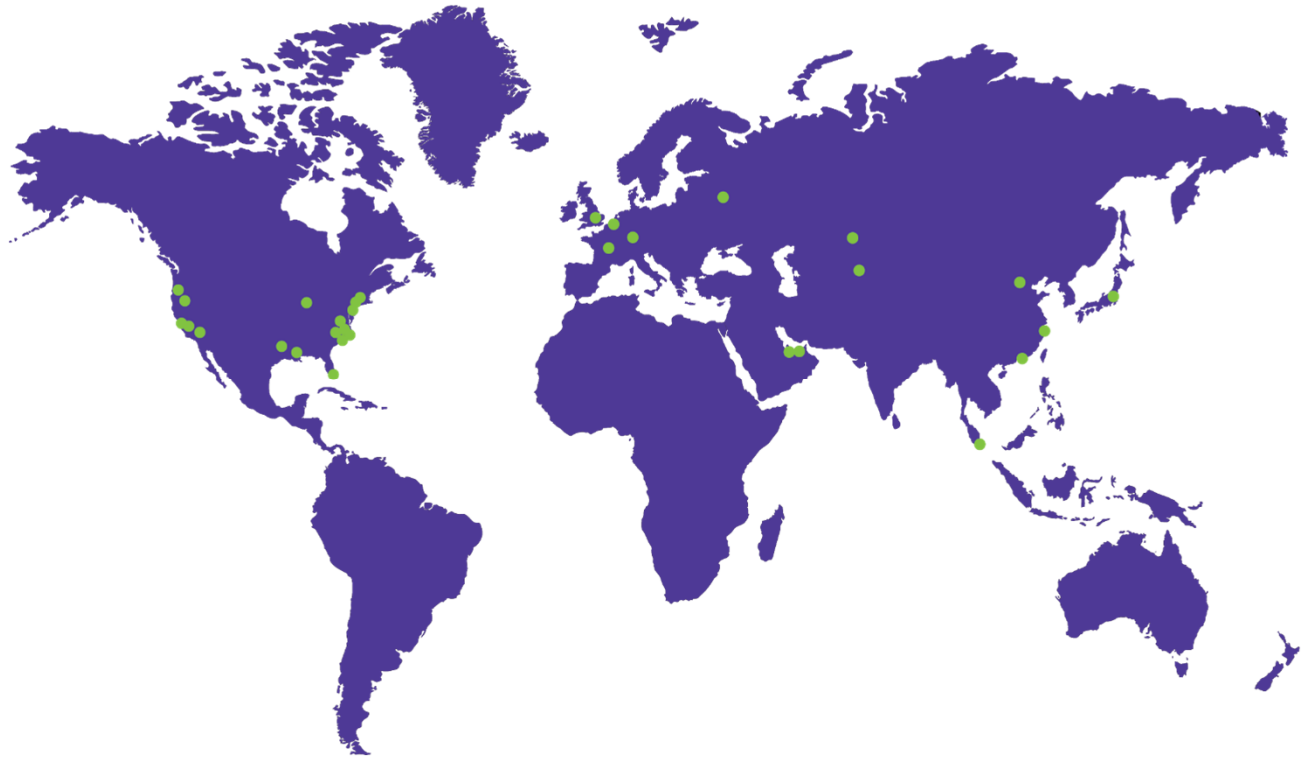
Silicon Valley

Singapore*

Tokyo

Washington, DC

Wilmington



Morgan Lewis

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

THANK YOU

© 2020 Morgan, Lewis & Bockius LLP
© 2020 Morgan Lewis Stamford LLC
© 2020 Morgan, Lewis & Bockius UK LLP

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

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

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