Morgan Lewis

Morgan Lewis Hedge Fund University™

PRIVACY & CYBERSECURITY FOR FUND MANAGERS

January 23, 2019

Ezra Church, Mark Krotoski, Reece Hirsch, Jedd Wider

Agenda

- Cyber Threats Facing Funds
- SEC Guidance and Enforcement
- EU General Data Protection Guidelines
- New York Department of Financial Services (DFS) Cybersecurity Rules
- State Laws
- Key Takeaways

CYBER RISKS FOR HEDGE FUND MANAGERS

Cyber Risks Facing Funds

- Loss of investor information (e.g., names, Social Security and bank account numbers)
- Loss of intellectual property (e.g., proprietary trading algorithms, strategies, source code)
- System disruptions
- Fraudulent trading and transfer activity
- Penalties and fines
- Reputational harm

Fraudulent Trading Activity

- Fraudulent trading activity and electronic funds transfers are also key concerns
  - In a reported attack, hackers broke into a hedge fund system and gained access to execute wire transfers
  - Executed a series of transfers of just under $500K, the firm's "flag" level
  - Able to complete several transfers before the activity was eventually detected
- Firms must secure access to all trading and treasury functions
  - Guarding against potential external and internal fraudulent activity

Protecting Your Fund's Reputation

- The greatest harm that arises from a security breach is often reputational
  - Strong reputations are hard-won and easily lost in the hedge fund world
  - Being a victim of a cyber attack can be extremely damaging to a fund (or any business that maintains personal information)
- Hedge funds are seeing a higher level of focus on cybersecurity in request for proposals (RFPs)
  - Indicates that cybersecurity is an increasingly high priority for high-net-worth and institutional clients
- Unfortunately, no organization can completely immunize itself against sophisticated, targeted cyber attacks
- But you can implement a reasonable cybersecurity compliance program

SEC GUIDANCE AND FOCUS

US Privacy Law – Sector Specific

Money	Health	Kids
• Gramm-Leach-Bliley Act; Regulation S-P • Fair Credit Reporting Act (FCRA) • State Laws	• Health Insurance Portability & Accountability Act (HIPAA)	• Family Educational Rights & Privacy Act (FERPA) • Children's Online Privacy Protection Act (COPPA) • State Laws

- Consumer Marketing! Telephone Consumer Protection Act (TCPA), CAN-SPAM, and Do Not Call regulations

Regulation S-P (2000, amended 2005)

- Privacy Rule: Notice and opt-out requirements for "nonpublic personal information." 17 C.F.R. 248.1 et seq.
- Safeguards Rule: Requires (a) adoption of written policies and procedures for the protection of customer information and records, including administrative, technical, and physical aspects; and (b) protection against anticipated threatrs or hazards to the security or integrity of customer records and information, and against unauthorized access to or use of customer records or information. 17 C.F.R. § 248.30.

SEC Cybersecurity Guidance

- 2014: SEC issues a Risk Alert, signaling its intention to increase oversight of cyber issues
- 2015: SEC publishes high-level cybersecurity guidance
  - Identify who is responsible for cybersecurity (CISO, CIO, or other officer)
- September 2015: Office of Compliance Inspections and Examinations (OCIE), which conducts SEC's National Examination Program, issues an alert announcing that it will be conducting examinations of registered broker-dealers and investment advisers
  - Focus on (1) governance and risk assessment, (2) access rights and controls, (3) data loss prevention, (4) vendor management, (5) training, and (6) incident response

Regulatory Focus

- SEC Cybersecurity Guidance (April 2015)
  - Highlighted that "[c]yber attacks on a wide range of financial services firms highlight the need for firms to review their cybersecurity measures."
  - Recommended that funds and advisers:
    - conduct a periodic risk assessment regarding cybersecurity risk
    - create a strategy designed to prevent, detect, and respond to threats identified through the assessment
    - implement the strategy through written policies and training, including a system for monitoring compliance

Regulatory Focus

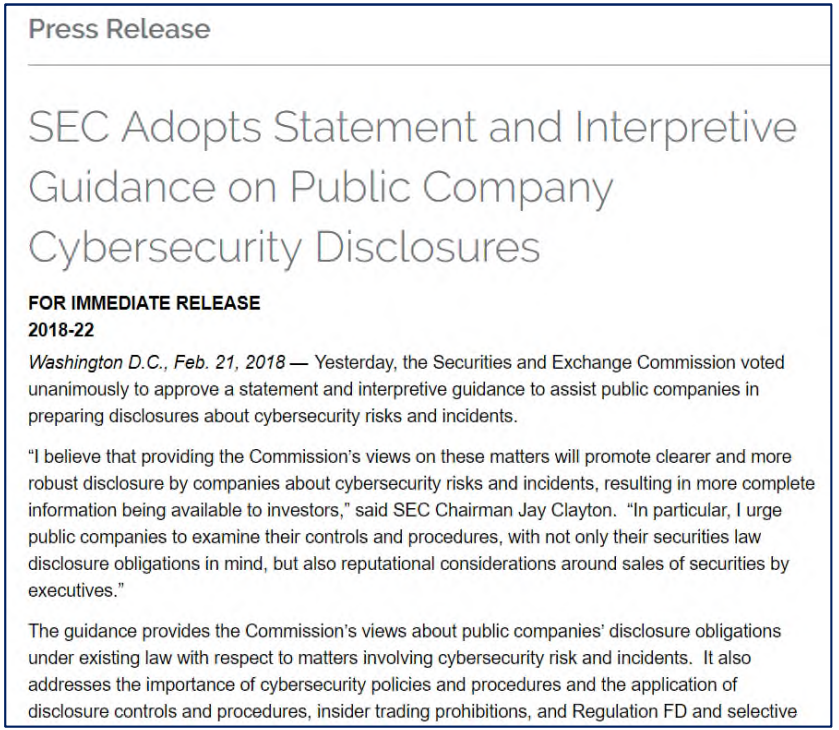
- OCIE Risk Alert, Observations from Cyber Examinations (August 2017)
  - Better preparedness than found in the 2014 exams
  - Less than two-thirds of advisers had breach response and notification plans
  - Written security policies were formulaic and not tailored
  - Spotty adherence to, and enforcement of, policies in place
  - Training required, but little follow-up or confirmation that it occurred
  - Stale security patches
  - Failure to remediate high-risk findings from penetration tests or vulnerability scans
  - Also recommended:
    - maintaining an inventory of data and information, classified by risk
    - enforced controls to access data and systems
    - mandatory employee training
    - engaged senior management

SEC Enforcement

- St. Louis Investment Adviser agrees to settle claims that it failed to adopt proper cybersecurity policies and procedures prior to a breach. SEC Press Release, 2015-202, Sept. 22, 2015.
- Craig Scott Capital and its principals agreed to pay $150,000 to settle charges that they failed to protect confidential customer data. *See* https://www.sec.gov/litigation/admin/2016/34-77595.pdf.
- A major bank agreed to pay $1 million to settle claims that it failed to safeguard customer data. SEC Press Release, 2016-112, June 8, 2016.

SEC Guidance on Cybersecurity Disclosures

- 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

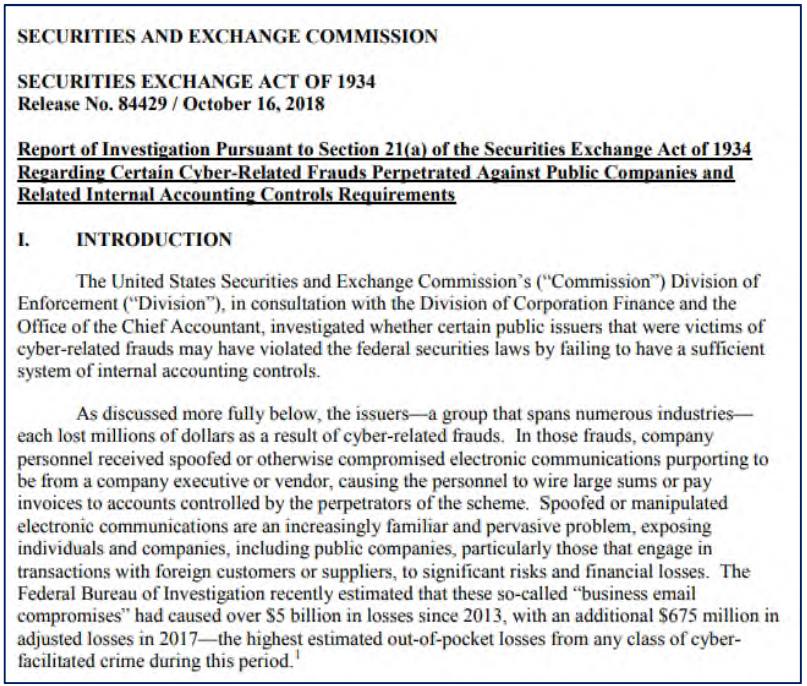
Washington D.C., Feb. 21, 2018 — Yesterday, the Securities and Exchange Commission voted unanimously to approve a statement and interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.

"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 Report on Cyber-Related Frauds

- Cyber Frauds
  - Business Email Compromise
- Nine companies lost at least $1 million
  - Two lost more than $30 million
  - In total, nearly $100 million was lost
- Internal accounting controls [Section 13(b)(2)(B)]
  - Need to "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."
- SEC
  - "[I]nternal accounting controls may need to be reassessed in light of emerging risks [. . .] Public issuers subject to the requirements of Section 13(b)(2)(B) must **calibrate their internal account controls to the current risk environment and assess and adjust policies and procedures accordingly**."



SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 84429 / October 16, 2018

Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements

I. INTRODUCTION

The United States Securities and Exchange Commission's ("Commission") Division of Enforcement ("Division"), in consultation with the Division of Corporation Finance and the Office of the Chief Accountant, investigated whether certain public issuers that were victims of cyber-related frauds may have violated the federal securities laws by failing to have a sufficient system of internal accounting controls.

As discussed more fully below, the issuers—a group that spans numerous industries—each lost millions of dollars as a result of cyber-related frauds. In those frauds, company personnel received spoofed or otherwise compromised electronic communications purporting to be from a company executive or vendor, causing the personnel to wire large sums or pay invoices to accounts controlled by the perpetrators of the scheme. Spoofed or manipulated electronic communications are an increasingly familiar and pervasive problem, exposing individuals and companies, including public companies, particularly those that engage in transactions with foreign customers or suppliers, to significant risks and financial losses. The Federal Bureau of Investigation recently estimated that these so-called "business email compromises" had caused over $5 billion in losses since 2013, with an additional $675 million in adjusted losses in 2017—the highest estimated out-of-pocket losses from any class of cyber-facilitated crime during this period.[1]

EU GENERAL DATA PROTECTION REGULATION

The New EU General Data Protection Regulation

- **New GDPR**
  - EU Parliament approved: April 14, 2016
  - Enforcement date: May 25, 2018
  - Replaces the Data Protection Directive 95/46/EC
  - Objective "to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy"
- **"Personal Data"**
  - Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person
- **Rights**
  - Data Access, To Be Forgotten, Data Portability
- **Consent**
  - Explicit, freely given, fully informed

The New EU General Data Protection Regulation

- **Data Breach Notification**
  - To Data Protection Authority (DPA), without undue delay/within **72 hours**
  - To individuals, without undue delay, if there is likely to be high risk to individuals

- **Data Protection Impact Assessment**
  - Prior to processing if high risk for individuals

- **GDPR Penalties**
  - Up to the higher of 4% global turnover or €20,000,000
    - Most EU countries currently limit data protection breaches to around £500,000 per breach (an average is £100,000)
  - Controllers and processors will be directly liable under GDPR

The New EU General Data Protection Regulation: Extraterritorial Scope

- The GDPR will apply to "all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location."

  - **EU-Based Establishment**:
    - Processors and controllers where personal data are processed in the context of the activities of the establishment

  - **Establishment Based Outside EU**:
    - Controllers and processors where the processing of personal data regarding EU data subjects relates to:

      - the offering of goods or services (regardless of payment)

      - the monitoring of data subjects' behavior within the EU

NY DFS CYBERSECURITY RULE

Final Cybersecurity Regulation

Press Release

February 16, 2017

Contact: Richard Loconte, 212-709-1691

GOVERNOR CUOMO ANNOUNCES FIRST-IN-THE-NATION CYBERSECURITY REGULATION PROTECTING CONSUMERS AND FINANCIAL INSTITUTIONS FROM CYBER-ATTACKS TO TAKE EFFECT MARCH 1

Regulation Protects Consumer Data and Financial Systems from Terrorist Organizations and Other Cyber Criminals

Regulated Financial Institutions Must Establish and Maintain a Cybersecurity Program to Protect Consumers and the Industry

Regulation Emphasizes Compliance Culture at Top Levels of the Institution

Governor Andrew M. Cuomo today announced the first-in-the-nation cybersecurity regulation to protect New York's financial services industry and consumers from the ever-growing threat of cyber-attacks will take effect on March 1, 2017. The final **regulation** requires banks, insurance companies, and other financial services institutions regulated by the Department of Financial Services to establish and maintain a cybersecurity program designed to protect consumers' private data and ensure the safety and soundness of New York's financial services industry.

"New York is the financial capital of the world, and it is critical that we do everything in our power to protect consumers and our financial system from the ever increasing threat of cyber-attacks," **Governor Cuomo said.** "These strong, first-in-the-nation protections will help ensure this industry has the necessary safeguards in place in order to protect themselves and the New Yorkers they serve from the serious economic harm caused by these devastating cyber-crimes."

New York State Department of Financial Services Superintendent Maria T. Vullo said, "With this landmark regulation, DFS is ensuring that New York consumers can trust that their financial institutions have protocols in place to protect the security and privacy of their sensitive personal information. As our global financial network becomes even more interconnected and entities around the world increasingly suffer information breaches, New York is leading the charge to combat the ever-increasing risk of cyber-attacks."

http://www.dfs.ny.gov/about/press/pr1702161.htm

NY DFS Regulation Requirements

Effective: March 1, 2017

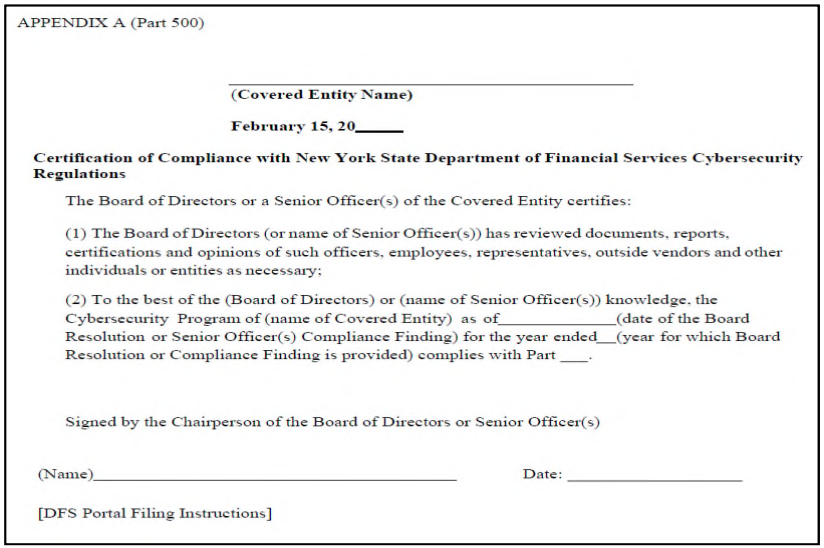
First certification: Feb. 15, 2018

6 MONTHS	1 YEAR	18 MONTHS	2 YEARS
• Cybersecurity Program • Cybersecurity Policy • Appoint CISO • Access Privileges • Perform Risk Assessment • Train Cybersecurity Personnel • Prepare/Update Incident Response Plan • Notify Superintendent of Breach	• CISO reports to Board of Directors • Penetration Testing and Vulnerability Assessments • Risk Assessments • Multi-Factor Authentication • Cybersecurity Awareness Training	• Audit Trails • Application Security • Data Retention • Policies and Procedures to Monitor the Activity of Authorized Users • Encryption	• Third-Party Service Provider Security Policy

Annual Compliance Certification

- Annual Certification Requirement
  - **February 15, 2018**

- "[C]ertifying that the Covered Entity is in compliance with the requirements set forth in this Part."



APPENDIX A (Part 500)

_____

(Covered Entity Name)

February 15, 20____

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

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

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

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

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

(Name)_____ Date: _____

[DFS Portal Filing Instructions]

[Section 500.17(b)]

Compare Notification Standards

California	Texas
• "The disclosure shall be made in the most expedient time possible and **without unreasonable delay**, consistent with the legitimate needs of law enforcement . . . or any measures necessary to **determine the scope of the breach** and restore the reasonable integrity of the data system." Cal. Civ. Code § 1798.82(a).	• "The disclosure shall be made **as quickly as possible**, except as provided by Subsection (d) [for law enforcement] or as necessary to **determine the scope of the breach** and restore the reasonable integrity of the data system." Tex. Bus. & Com. Code Ann. § 521.053(b).

New Notification Requirement

(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that 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.

New Notification Requirement

(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than **72 hours** from a determination that 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.

STATE LAWS

State Laws on Privacy & Cybersecurity

- Data breach notification laws (50 states and DC)
- State laws on financial privacy and biometrics broader than federal requirements (e.g., CA, IL, TX)
- State laws on security of personal information, but stricter federal requirements (e.g., CA, MA, CO)

KEY TAKEAWAYS

Develop a Formal Program

- Implement and enforce written cybersecurity procedures
- Designate someone responsible for cybersecurity
- Provide mandatory training for all personnel
- Ensure that wireless internet service provides (WISPs) are tailored to the firm
- Encrypt nonpublic personal information
- Fix inadequate antivirus software/firewalls; update security patches
- Don’t forget about the little things
- Ensure program demonstrates that firm acted reasonably, not negligently

Incident Response

- An effective incident response plan should
  - Establish an incident response team with representatives from key areas of the organization (compliance, legal, IT, HR, etc.)
  - Identify necessary resources in advance (forensic IT consultant, mailing vendor, call center operator, credit-monitoring service)
  - Provide for training of personnel to recognize and report security breaches
  - Outline media relations strategy and point person
- Meet during peacetime
  - Team members should not have to learn their roles during a crisis

Vendor Management

- Hedge funds often outsource key business functions to third-party vendors
  - If vendors are being entrusted with sensitive personal information or IP, they should be required to commit to robust privacy and security provisions
  - Security certification or third-party assessments (such as a SOC 2 report)
  - Prompt reporting of breaches to the fund
  - Indemnification for costs associated with a security breach
  - Clear instructions regarding permitted uses of data
  - Require/obtain cybersecurity insurance

ATTORNEY BIOGRAPHIES

Ezra D. Church

Philadelphia
T +1.215.963.5710
F +1.215.963.5001
ezra.church@morganlewis.com

Ezra D. Church focuses his practice on class action lawsuits and complex commercial and product-related litigation, with particular emphasis on the unique issues facing retail, ecommerce, and other consumer-facing companies. Ezra also focuses on privacy and data security matters, and regularly advises and represents clients in connection with these issues. He is co-chair of Morgan Lewis's Class Action Working Group.

Ezra has extensive experience handling complex and unusual class action litigation, and has handled all aspects of such cases from inception through trial and appeal. His work in this area includes defeat of class certification in a rare copyright class action against one of the world's leading publishers, successful opposition of class certification in an unusual *defendant* class action against many large financial institutions, and a successful defense verdict in a consumer class action trial against an international retailer, including affirmance on appeal. He is an active member of the Firm's Class Action Working Group and regularly writes and speaks on class action issues. He is a contributor to the Firm's chapter on class action litigation in the leading treatise *Business and Commercial Litigation in Federal Courts* and co-author of a chapter in *A Practitioner's Guide to Class Actions*, among others.

Mark L. Krotoski

Silicon Valley
T +1.650.843.7212
F +1.650.843.4001
mark.krotoski@morganlewis.com

- 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 a variety of complex and novel cyber investigations
  - 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, in addition to other DOJ leadership positions, and as a cybercrime prosecutor in Silicon Valley.

W. Reece Hirsch

San Francisco
T +1.415.442.1422
F +1.415.442.1001
reece.hirsch@morganlewis.com

W. Reece Hirsch counsels clients on healthcare regulatory and transactional matters and co-heads the firm's privacy and cybersecurity practice. Representing healthcare organizations such as hospitals, health plans, insurers, physician organizations, healthcare information technology companies, and pharmaceutical and biotech companies, Reece advises clients on issues such as privacy, fraud and abuse, and self-referral issues. This includes healthcare-specific data privacy and security matters, such as compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act.

Reece represents clients in almost all sectors of the healthcare industry on privacy and security compliance matters. He helps them develop policies and procedures, structures healthcare information technology ventures, addresses Big Data issues, and responds to security breaches. Reece also works with clients to develop and implement corporate compliance programs. Healthcare companies turn to Reece for guidance on conforming their operations—including recruitment, marketing, and data transmissions—to US federal and state healthcare regulatory requirements.

Jedd H. Wider

New York

T +1.212.309.6605

F +1.212.309.6001

jedd.wider@morganlewis.com

Jedd H. Wider focuses on global private investment funds and managed accounts, particularly global hedge, private equity, secondary, and venture capital funds. As co-leader of the global hedge funds practice, he represents leading financial institutions, fund managers, and institutional investors in their roles as fund sponsors, placement agents, and investment entities. He assists clients through all stages of product development and capital raising as well as customized arrangements, seed and lead investor arrangements, and joint ventures. He specializes in all aspects of secondary transactions, and complex financial structurings.

Jedd concentrates on all aspects of bespoke fund products and arrangements including funds of one and managed accounts and regularly advises clients on all aspects of regulatory compliance.

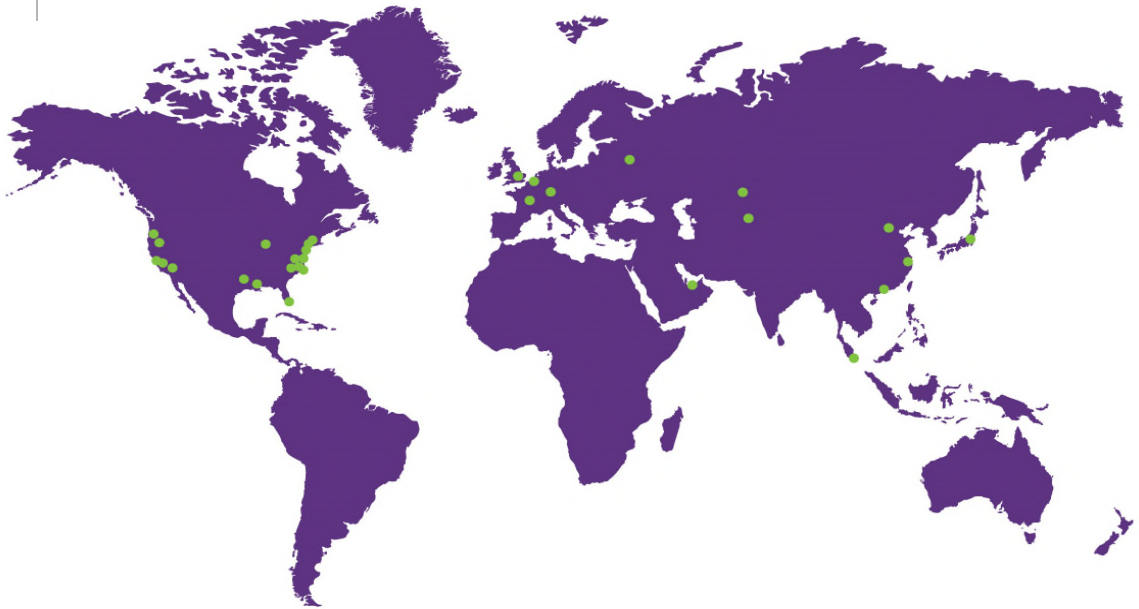
Members of the international media often seek out Jedd for his views on the hedge fund and private equity fund industries and capital markets. His analysis can be found in US and international publications, including *The Wall Street Journal, The Economist*, and *Financial Times,* as well as on television networks such as Bloomberg and CNN.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

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