DORSEY PF 2017 SYMPOSIUM

DORSEY™ always ahead

## Session 7: Cybersecurity Regulation and Best Practices

4:30- 5:30PM

**Moderator:** Nick Akerman, *Partner, Dorsey & Whitney LLP*

**Panelists:**
Janaya Moscony, *President, SEC Compliance Consultants*
Suzan Rose, *Chief Compliance Officer, Marshall Wace North America L.P.*
Edward Stroz, *Co- President, Stroz Friedberg*
Tom Weston, *Partner, Hakluyt*


DORSEY PF 2017 SYMPOSIUM

# Cybersecurity Compliance

# Reactive to Proactive

- State breach notification laws
- Compliance trend
- Seven steps to effective compliance
  1. Develop standards and procedures
  2. Assign a person with overall responsibility
  3. Take care not to assign someone who might pose a risk
  4. Communicate standards and procedures
  5. Regular Audits
  6. Consistently enforce the policies
  7. Mechanism in place to respond to violations

# Cybersecurity Is Not Just IT Security

- **Multi-dimensional Problem**
- **Human Resources**
- **Legal**
- **Risk Management**
- **Compliance**
- **IT Security**
- **Corporate Security**

# Companies can mitigate their “risk” by re-evaluating 8 business areas

- Hiring Practices
- Company Rules
- Appropriate Agreements
- Use of Technology
- Termination Practices
- Protocols for Response
- Company Compliance Program
- Insurance

# Eight Areas of Risk Relating to Cybersecurity

1. Hiring is the time to explain to new employees the rules in place to protect the company's data and to be defensive on competitive data being brought into the workplace
2. Company rules and policies should spell out what employees can and cannot do with the company network and form the foundation of top-to-bottom workforce training
3. Agreements with employees and other third parties are a key component of data protection

# Eight Areas of Risk Relating to Cybersecurity

4. Technology can be employed not only to secure data but to define who is authorized to access what portion of the network and provide admissible evidence of a breach
5. Effective termination procedures are critical to securing data
6. If a breach occurs, it is important to have protocols in place to quickly determine the scope of the breach and the appropriate response
7. Company compliance programs should be amended to include cybersecurity
8. Insurance policies should be reviewed to determine appropriate cyber coverage

PUBLICATIONS

# SEC's Latest Cybersecurity Risk Alert Identifies Elements of Robust Policies and Procedures

August 14, 2017

Nick Akerman, Genna Garver, Kimberly B. Frumkin

On August 7, 2017 the Securities and Exchange Committee ("SEC") Office of Compliance Inspections and Examinations ("OCIE") released yet another cybersecurity Risk Alert entitled, "Observations from Cybersecurity Examinations." In this most recent Risk Alert, OCIE details its findings from its Cybersecurity 2 Initiative, which involved the examination of 75 firms, including broker-dealers, investment advisers, and investment companies between September 2015 and June 2016. Following its 2014 Cybersecurity 1 Initiative, the Cybersecurity 2 Initiative set out to assess industry practices and legal, regulatory and compliance issues associated with cybersecurity preparedness, focusing in greater depth on validation and testing of procedures and controls. As the Risk Alert sets forth a list of elements OCIE considers to be robust policies and procedures, it should be used as a check list for registrants in assessing the adequacy and effectiveness of their cybersecurity compliance program in light of their business risks.

The SEC has made cybersecurity a priority in recent years as more cyber-attacks threaten the industry. In addition to being named as a National Examination Program priority, cybersecurity has been a focus on the SEC's outreach program. The SEC shared the results from its Cybersecurity 1 Initiative in its February 2015 Risk Alert entitled, "Cybersecurity Examination Sweep Summary." In May of this year, OCIE put out a Risk Alert regarding the ransomware called "WannaCry" in which OCIE initially shared its observations from its Cybersecurity 2 Initiative to provide guidance to registrants for strengthening cybersecurity programs and protecting against the ransomware. Beyond its exam program and outreach, the SEC's Enforcement Division has also been focusing on the matter by

bringing cases against investment advisers and broker-dealers for cybersecurity-related violations. On all fronts the SEC is trying to get the message out that cybersecurity is one of the greatest risks facing the financial services industry and registrants must ensure their compliance programs address the risks posed by cyberattacks.

The Cybersecurity 2 Initiative exams focused on the following areas: (1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response. Generally, the staff found the cybersecurity preparedness of the firms they examined had improved since its Cybersecurity 1 Initiative testing in 2013 and 2014. Some of the improvements noted in the Cybersecurity 2 Initiative findings include:

- *Testing and monitoring*:
  - 95% of broker-dealers and 74% of advisers and funds conduct periodic risk assessments of vulnerable systems;
  - Nearly all of the firms had plans in place for addressing incidents;
  - 95% of broker-deals and 43% of advisers and funds conducted penetration tests and vulnerability scans on firm-identified critical systems; and
  - All firms examined had some form of control in place to monitor data loss of personally identifiable information.
- *Policies and Procedures*:
  - Nearly all firms had policies and procedures in place to address cyber-related business continuity planning and Regulation S-P;
  - All of the advisers and funds maintained policies, procedures, and standards related to verifying the authenticity of a customer or shareholder requesting to transfer funds; and
  - Nearly all broker-dealers and most advisers and funds had specific policies addressing Regulation S-ID.

The Risk Alert also discussed some issues noted during the testing, including policies and procedures not reasonably tailored to the firm, firms' actual practices not reflecting their written policies and procedures, and Regulation S-P issues among firms that did not appear to conduct system maintenance. Finally, the Risk Alert provided details of what the SEC considers elements of "robust policies and procedures." These included:

- *Maintenance of an inventory of data, information, and vendors*. Policies and procedures included a complete inventory of data and information, along with classifications of the risks, vulnerabilities, data, business consequences, and information regarding each service provider and vendor, if applicable.
- *Detailed cybersecurity-related instructions*. Examples included:
  - Penetration tests: policies and procedures policies included specific information to review the effectiveness of security solutions.
  - Security monitoring and system auditing: policies and procedures regarding the firm's information security framework included details related to the appropriate testing methodologies.
  - Access rights: requests for access were tracked, and policies and procedures specifically addressed modification of access rights, such as for employee on-boarding, changing positions or responsibilities, or terminating employees.
  - Reporting: policies and procedures specified actions to undertake, including who to contact, if sensitive information was lost, stolen, or unintentionally disclosed/misdirected.
- *Maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities*. Examples included:
  - Vulnerability scans of core IT infrastructure were required to aid in identifying potential weaknesses in a firm's key systems,

with prioritized action items for any concerns identified.

- Patch management policies that included, among other things, the beta testing of a patch with a small number of users and servers before deploying it across the firm, an analysis of the problem the patch was designed to fix, the potential risk in applying the patch, and the method to use in applying the patch.

- *Established and enforced controls to access data and systems.* For example, the firms:
  - Implemented detailed “acceptable use” policies that specified employees’ obligations when using the firm’s networks and equipment.
  - Required and enforced restrictions and controls for mobile devices that connected to the firms’ systems, such as passwords and software that encrypted communications.
  - Required third-party vendors to periodically provide logs of their activity on the firms’ networks.
  - Required immediate termination of access for terminated employees and very prompt (typically same day) termination of access for employees that left voluntarily.
- *Mandatory employee training*. Information security training was mandatory for all employees at on-boarding and periodically thereafter, and firms instituted policies and procedures to ensure that employees completed the mandatory training.
- *Engaged senior management*. The policies and procedures were vetted and approved by senior management.

Along with federal regulations that address cybersecurity preparedness, investment advisers and broker-dealers should also watch out for new state cybersecurity regulations aimed at financial institutions. New York was the first state to put out such cybersecurity regulations, which came into force on March 1 of this year. Although investment advisers are not covered entities under the New York law, some may have affiliated outside business activities that are covered by the regulations. Earlier this summer, Colorado adopted a similar set of cybersecurity rules which do cover investment advisers. Those rules became effective July 15, 2017.

In sum, SEC registrants should review OCIE’s suggested "robust policies and procedures" in light of their business and consider whether their current written policies and procedures are adequate and effectively implemented. Registrants should also be prepared to respond to OCIE exam requests regarding these policies and procedures and the registrant’s related testing. Dorsey attorneys are available to assist with any corresponding questions or concerns.

# COMMENTARY: How compliance officers and firms can help limit CCO personal liability

**Feb 22 2017** Janaya Moscony and Steve Troche

Many fear the President Donald Trump's deregulation drive could undo much of the hard work and progress that has been made over the past several years in reforming Wall Street's culture. In particular, Mary Jo White, former Commissioner of the Securities and Exchange Commission (SEC), made significant headway in promoting ethics through her "broken-window" approach to enforcing SEC rules.

Before 2008, we witnessed an industry that dismissed compliance much more readily than today. The recent critical eye on compliance has resulted in tightened controls and operations at firms which in turn has resulted in additional protections for investors.

The discussion regarding the affects the new administration will have on the compliance and the industry reverberates throughout the financial services industry. It appears the SEC does not plan on reversing course anytime soon despite assumptions being made about Trump's administration.

In fact, the SEC's more recent trend toward holding individuals personally liable for their conduct will continue to hold steady as well.

Speaking last November at ACI's 33rd International Conference on the Foreign Corrupt Practices Act (FCPA), the SEC's then-Enforcement Director, Andrew Ceresney, described how the SEC has prioritized FCPA enforcement with a focus on individual liability. Ceresney explained that "pursuing individual accountability is a critical part of deterrence" and holding officers accountable for negligence.

Ceresney's statements are the kind that keep financial professionals wondering when the other shoe will drop. This guidance – and the varying fact patterns inherent in the cases involving recent instances of CCOs being held personally liable – reinforce the necessity that companies and officers (like CCOs) evaluate what they can do to shield themselves from professional and personal liability.

**Indemnities – the first line of defense**

Directors and officers are generally provided with indemnification with respect to the entity that they serve. Subject to limitations, indemnification generally allows for directors and officers to be financially covered by the firm for legal expenses and other liabilities incurred by them as defendants or witnesses in related actions.

Indemnification protections are generally delineated in contracts, but can occasionally be found in an insured entity's organizational documents. They typically provide directors and officers with the maximum indemnification permitted under state and federal law.

Whether a CCO is required to be indemnified by a company depends on the state of incorporation, so it is important to make sure that the CCO is properly recognized as a corporate officer of the insured entity. Some states require that the CCOs are need only be appointed in the bylaws of the insured entity as a corporate officer, while other states might additionally require that the CCO also be appointed as a corporate officer in state filings.

Some circumstances could cause the entity providing the indemnity to withhold it. The entity may not have the funds or it may just choose to withhold it because of a conflict with the director or officer. This is why the indemnity is only the first line of defense.

**Insurance – Do not cut corners**

When considering insurance, CCOs initially must understand exactly what risks can be transferred or mitigated.

Careful attention must be given to matching the exact insurance products and riders to the risk sought to be transferred, and knowing where the pitfalls exist which could result in a claim being denied. Both errors-and-omissions and directors and officer liability coverage have been in the marketplace for decades, and as such, have well-established standards and terms.

Other types of coverage, such as cyber security insurance, which are infants in the marketplace, do not have the same conventions as other policies.

**Errors & omissions (E&O) policies** are widely used throughout the industry to help protect against claims by clients arising out of professional services provided by the insured.

**Directors & Officer Liability (D&O)** coverage can be added to an E&O policy or purchased separately, to protect the firm as well as the directors, officers, partners and employees of the insured entity for claims arising out of business decisions, not investment decisions.

D&O is where one would find coverage for "claims" (including formal regulatory investigations costs) by non-clients such as the SEC and U.S. Department of Labor that are not triggered by a client complaint.

**Side A, Independent Directors Liability (IDL) Insurance** typically serves as a supplemental policy to D&O coverage, and would come into play in circumstances where indemnification is not available or is refused. Side A IDL insurance helps fund independent directors mitigate liability and exposure to various risks associated with indemnification (when a fund is legally prohibited from paying for a director/officer's defense); erosion risk (when a D&O policy has exhausted its limits of liability); and coverage risk (when a D&O policy does not provide coverage for the situation).

**Cyber Insurance** is designed to cover consumers of technology services or products. More specifically, the policies are intended to cover a variety of both liability and property losses that may result when a business engages in various electronic

activities.

Most notably, but not exclusively, cyber policies cover liability for a data breach in which client information is exposed or stolen by an individual who has gained access to the firm's electronic network.

**Additional riders**

Many insurance riders can accompany the policies outlined above. An insurance rider is an available enhancement option that a broker can negotiate to be included in a policy.

Riders can help supplement your existing coverage and provide additional benefits usually at little additional cost. Financial professionals need to understand policy definitions and exclusions, and discuss the various options available with their broker.

When reviewing these policies, directors and CCOs should gauge their total risk profile (including total amount of assets) and review against existing protections, such as indemnification. Then, while consulting with an insurance professional, you should work towards understanding what risks are covered, and which risks are not.

Chief Compliance Officers must ensure they are diligent when reviewing or purchasing insurance products. Quite often, when it is time to file a claim the fine print is what matters.

**What to look for in a CCO**

Given the SEC's recent cases and speeches, advisers should ensure that the CCO has the right experience and background – specifically a background that shows he or she understands all relevant SEC regulations. Advisers should also ask questions and understand the niche experience that is needed to be an effective CCO.

Several factors distinguish a well-suited CCO from an inexperienced, lower-cost alternative. Such examples include:

- extensive experience;
- the ability to customize a compliance program to the fund's business, interact with service providers and test the compliance program to appropriately identify potential failures;
- accountability and time-management skills; and
- dependability and reliability.

These skills are not exclusive to CCOs however, as fund directors must possess many of the aforementioned skills in order to perform their oversight tasks in an ever-evolving regulatory environment.

Additionally, while fund directors do not need to customize and test a compliance program, they must have a certain level of familiarity in order to properly identify potential failures.

These traits and issues for both board members and officers are long standing and well-established in the industry, and will remain paramount for the foreseeable future. Whether under one administration or the next, certain issues remain enduring.

**New regime**

Even if SEC enforcement under Trump's nominee for SEC chair, Jay Clayton, proves to be less prone to bringing cases than White, there are more reasons to take compliance seriously than just to avoid SEC enforcement.

Even under the new regime, insurance claims are expected to continue to rise.

In ICI Mutual's 2015 Annual Claims Trends, the company noted that 2015 saw an increase in the overall number of claims submitted to them by fund groups under their D&O/E&O policies. Further, ICI Mutual stated that nearly 25 percent of their insured fund groups submitted at least one claim notice during 2015.

Over the five-year period from 2011 to 2015, approximately 50 percent of their insured fund group submitted at least one claim notice. The continuing trend of claims increasing year over year will remain largely unaffected by a new administration, and any possible effect down the road would likely be marginal at best.

Another trend that unlikely to lose steam is increasing institutional investor demand for compliance. Institutional investors are not unlikely to turn back the clock with their due diligence procedures nor are they likely to reduce demands.

Heightened demand for due diligence on cyber security is rampant throughout the industry.

Also, even if the new administration shows a lighter touch on enforcement, deficiency letters are likely to remain unchanged. Institutional investors and boards will still need to know about compliance issues and they will still present liability concerns and hence, require mitigation.

Some expect the Trump administration to promote a deregulatory regime similar to the Reagan Administration, which would reduce SEC oversight, and subsequently, reduce oversight by financial industry participants.

Even if some areas of financial and securities regulations are rolled back, the SEC will likely continue to name individuals in future enforcement cases. Recent history has shown that CCOs and boards of directors need to know more than compliance.They need to understand how to protect their reputation and livelihood. Even under a deregulatory administration this will be critical.

SEC3 COMPLIANCE CONSULTANTS
BRIDGING THE GAP

***Janaya Moscony**, is founder and President of SEC Compliance Consultants, Inc. **Steve Troche** is an Associate Consultant with SEC Compliance Consultants, Inc. Both can be reached at info@seccc.com.*

THE NATIONAL LAW JOURNAL
JULY 2017
An ALM Publication
THE PRACTICE | Commentary and advice on developments in the law

# China's New Cybersecurity Law Is a Start

BY NICK AKERMAN AND DAN GOLDBERGER

ON JUNE 1, CHINA'S NEW CYBERsecurity law took effect. The new law applies not only to domestic Chinese companies but has wide-ranging implications for U.S. and other foreign companies doing business in China.

Since its passage last November, the cybersecurity law has faced heavy criticism from the international business community, primarily due to the burdens it places on multinational companies operating in China that use, store and move data in and out of China. The law has also faced criticism over its ambiguous language. Even the most seasoned China watchers cannot say with any certainty how the Chinese government will enforce it.

The cybersecurity law applies to businesses in all sectors of the Chinese economy and creates a national approach to protecting data. It regulates the data that companies may store, and where and how they store it. It also heavily restricts what a company may do with personal data collected and stored in China.

However, the law is ambiguous in many respects, which has created significant uncertainty for businesses operating in China. For example, operators of "Critical Information Infrastructure," an undefined term in the law, are subjected to heightened security obligations. Because the term is not defined, we cannot be sure which companies qualify as these operators.

Despite the unease and uncertainty over the new law, there are positives, as well. The law adopts data regulatory standards from the European Union and the U.S. Thus, at least with respect to data security compliance, multinational companies operating in China will not need to develop a new framework from the ground up. Instead, they likely have the building blocks in place with their current data compliance programs operative in the U.S. and EU.

In the U.S., the trend has moved away from a reactive approach of dealing with data breaches after they occur to a more proactive approach of preventing data breaches through a seven-step data security compliance program.

In drafting its new cybersecurity law, China has adopted the criteria of what has become the gold standard in the U.S. for an effective data security compliance program.

OSTILL/SHUTTERSTOCK.COM

U.S. compliance, based on the seven steps in the Federal Sentencing Guidelines, requires companies to promulgate data security policies and procedures that are consistently enforced through high-level oversight, periodic audits to ensure the compliance plan's effectiveness and mechanisms for reporting and responding to violations. However, the "national standards" referenced in the China law have not yet been promulgated, and until they are, compliance with these articles remains aspirational.

Under the law, companies must identify the relevant persons responsible for corporate data security oversight and ensure that those individuals do not pose a risk for unethical behavior. Without adequately trained compliance personnel, the policies and procedures obviously cannot be effectively enforced.

Importantly, periodic audits are also mandated by the law to ensure enforcement of policies. Testing the efficacy of its data compliance program enables a company to assess its effectiveness before a data breach has occurred.

The new law also requires companies to establish mechanisms for reporting data security violations and relies on company employees to do so.

Though China now has the building blocks in place for data security compliance, the government hasn't been clear enough about its new cybersecurity law and how it will interpret it. This creates uncertainties and unknown risks for companies doing business in China.

For now, China has created an effective framework for data security compliance. The devil will be in the details.

**NICK AKERMAN** *and* **DAN GOLDBERGER** *are partners at Dorsey & Whitney. Akerman's practice focuses on civil and criminal trials and data protection. Goldberger's practice focuses on complex commercial litigation, intellectual property litigation and data protection.*

THE NATIONAL LAW JOURNAL
JUNE 27, 2016
An ALM Publication
THE PRACTICE | Commentary and advice on developments in the law

# How to Prepare for Theft of Company Information

Companies should take three steps now to ensure use of the Defend Trade Secrets Act.

BY NICK AKERMAN AND J JACKSON

AUDE GUERRUCCI

Done: President Obama signs the Defend Trade Secrets Act May 11.

In May, President Barack Obama signed into law the Defend Trade Secrets Act that creates a federal civil cause of action for the misappropriation of trade secrets. This new law amends the Economic Espionage Act, which makes it a federal crime to steal and use trade secrets. Title 18 U.S.C. 1831, et. seq. For companies that depend on confidential information to provide them a competitive edge, there are several proactive steps they should take to ensure their use and the full benefits of this statute if their trade secrets are stolen.

Most significantly, the Defend Trade Secrets Act, unlike the state trade secrets laws, provides for an ex parte "order for the seizure of property necessary to prevent the propagation or dissemination of the trade secret," upon a showing of "exceptional circumstance." Traditional state court equitable remedies are limited to a temporary restraining order and a preliminary injunction.

The law also makes the theft, possession and use of trade secrets a predicate act for the Racketeer Influenced and Corrupt Organizations Statue, which can form the basis of a civil RICO action for treble damages and attorney fees. (In the past, federal courts have been reluctant under most circumstances to find a RICO "pattern" for trade secrets theft as part of a scheme to defraud based on the mail and wire fraud statutes. See, e.g., *Bro-Tech Corp. v. Thermax* (E.D. Pa. 2009).

## DEFINE TRADE SECRETS

An obvious first step for any company thinking it might use the Defend Trade Secrets Act is to inventory and define its trade secrets and specify them in company policies and employee and third-party confidentiality agreements.

The act follows the classic definition of a trade secret, as defined by state law, to mean "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes." It makes no difference whether this information is stored on paper, electronically on a computer or is intangible information committed to memory. Section 1839 (3). The "information" must

"derive economic value, actual or potential, from not being generally known to, and being readily ascertainable through proper means by, the public." Id. at 3(B).

## REASONABLE MEASURES

Identifying the company's trade secrets is critical to meeting the next requirement of the statute—"the owner has taken reasonable measures to keep such information secret." Id. At 3(A).

The U.S. Court of Appeals for the Seventh Circuit in *United States v. Lange*, which upheld a criminal conviction under the Economic Espionage Act of a disgruntled former employee who attempted to sell his company's secret manufacturing processes to third parties, is instructive on what constitutes reasonable measures: 1) the processes were physically secured in a designated room "protected by a special lock, an alarm system, and a motion detector"; 2) the documentation describing the process was limited with "surplus copies … shredded"; 3) certain information "in the plan" was "coded" with "few people" knowing the codes; 4) the documentation contained warnings of the company's "intellectual-property rights"; 5) "every employee received a notice that the information with which he works is confidential"; and 6) the company divided work among vendors to ensure "that none can replicate the product."

## ADDITIONAL ACTIONS

The *Lange* listing is not exhaustive. Other measures such as confidentiality agreements, employee training programs, password-protected access and access to the confidential information on a "need to know" basis are traditionally relied upon by state courts in finding reasonable measures to protect the information, which measures apply equally to the Economic Espionage Act.

In addition, because most confidential information is maintained in computers or electronic databases, there needs to be an emphasis on policies, procedures and technology to protect such data.

The Defend Trade Secrets Act also provides for "reasonable attorney's fees" and "exemplary damages in an amount not more than 2 times the amount of" the compensatory damages if the theft is willful and malicious.

To be entitled to exemplary damages and attorney fees under the new law, employers must amend their employee agreements and/or policies.

Under the act, an employee "who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding if the individual—(A) files any document containing the trade secret under seal; and (B) does not disclose the trade secret, except pursuant to court order."

For an employer to receive exemplary damages or attorney fees under this statute, it must amend its employee agreements to provide "notice" of this "immunity" "in any contract or agreement with an employee that governs the use of a trade secret or other confidential information." An employer is "considered to be in compliance with the notice requirement," if it provides to its employees "a cross-reference to a policy document" setting "forth the employer's reporting policy for a suspected violation of law."

Taking inventory of trade secrets, reviewing and establishing reasonable measures to protect them, and amending confidentiality agreements will position companies to best utilize the new trade secrets law. The time to start thinking about using this new civil remedy is now, not in the future, when you learn someone has stolen your company's trade secrets.

**NICK AKERMAN** *and* **J JACKSON** *are partners in the international law firm Dorsey & Whitney. Both are members of the trial group and include among their specialties the protection of competitively sensitive information and trade secrets litigation. Akerman and Jackson can be contacted, respectively, at akerman.nick@dorsey.com and at jackson.j@dorsey.com.*

FEBRUARY 2016 SPECIAL REPRINT
NSCP CURRENTS

# Liability and Outsourcing – Identifying and Controlling the Real Risks

## Part 2 of 2: Choosing a CCO

Courtesy of SEC Compliance Consultants, Inc.

**Introduction**

This is the second of two articles discussing risk identification and control. Part 1, published in December 2015 explored CCO liability and what to keep in mind when outsourcing the CCO function. This article reviews the key discussion points of Part 1 and examines what to look for in choosing a CCO, and reviews the concepts of supervision versus oversight and CCO responsibilities.

Individual liability is quickly rising to the forefront of the radar of the Securities and Exchange Commission. In fact, over the last five years, 80% of SEC enforcement cases have involved charges being brought against individuals. In a recent speech, Andrew Ceresney explained this increased focus stating "Holding individuals accountable for their wrongdoing is critical to effective deterrence and, therefore, the Division considers individual liability in every case". [1]

In a separate speech also highlighting individual liability, Mr. Ceresney noted that many of the recent enforcement cases brought against individuals make it clear that the SEC will "aggressively pursue business line personnel and firms who mislead or deceive".[2] Recent SEC enforcement cases have shown that the SEC is willing to bring cases for compliance oversights even when there is no harm to clients. We bring this to the attention of investment advisers, fund boards and CCO's so that they stay alert and informed. A vast majority of such enforcement actions can easily be avoided with proper oversight.

**Improving your Compliance Program**

**The Importance of A Proper Risk Assessment**

In order for any compliance program to adequately insulate advisers, fund boards and CCOs, it must begin with a detailed risk assessment and gap analysis. This will lead to the creation of a compliance program that encompasses all risks.

Any discussion on CCO liability must begin with the foundation of building one's compliance program, the adoption of firm policies and procedures. In order to create comprehensive policies and procedures, a CCO must take into account the specific investment adviser, broker dealer or investment company business model, and tailor a program to deal with the risks inherent to the particular model.

As noted in the SFX case[3], if the CCO conducted a risk assessment and prioritized his time to address the highest areas of risk, he likely could have avoided enforcement action even in light of fraudulent activity personnel.

The real cause of failure to supervise actions is often insidious where the impetus is a poor process to identify risk.

Section 203(e)-6 of the Advisers Act, in part, reads:

"…no person shall be deemed to have failed reasonably to supervise any person, if--

A. there have been established procedures, and a system for applying such procedures, which would reasonably be expected to prevent and detect, insofar as practicable, any such violation by such other person, and

B. such person has reasonably discharged the duties and obligations incumbent upon him by reason of such procedures and system without reasonable cause to believe that such procedures and system were not being complied with."

To avail yourself of the safe harbor, subparagraph A requires that the adviser has adequate policies and procedures, and subparagraph B requires that you be able to adequately demonstrate that you "reasonably discharged" your duty to supervise. Too many CCO's focus on subparagraph B and ensure timely compliance work and documentation. However, while the existing compliance procedures may be working well, if certain key risks have not been addressed, the CCO can unknowingly bear significant risk. CCO's who wish to quantify and manage their liability need to focus on ensuring they have the policies and procedures to address the business's risk.

A best practice is to develop a scheduled process that involves the CCO and executive management team working together to conduct a review of the business from top to bottom. The process should be thorough and involve a broad range of questions. Each risk should be identified and rated, and based on ratings, adequate policies and procedures drafted.

1. https://www.sec.gov/news/speech/ceresney-fcpa-keynote-11-17-15.html
2. https://www.sec.gov/news/speech/keynote-address-2015-national-society-compliance-prof-cereseney.html
3. http://www.sec.gov/news/pressrelease/2015-120.html

**ABOUT THE AUTHORS**

The co-authors are all located at SEC Compliance Consultants, Inc., www.seccc.com. **Janaya Moscony**, is President and can be reached at Janaya@seccc.com; **John Lukan** and **Joseph Guarino** are Managing Directors, and can be reached at Jlukan@seccc.com and jguarino@seccc.com respectively. **Steve Troche** is an Associate Consultant and can be reached at stroche@seccc.com.

In the SEC's Risk Alert on Outsourcing[4], the SEC found some concerns with outsourced CCO's ability to communicate firm risk. However, such a concern is not limited to outsourced CCO's – all CCO's should be communicating frequently with fund boards and senior management. Assessing firm risk and conflicts of interest should always involve a team approach with open communication.

**Fund Board and Management Takeaways**

*Tone at the Top Really Does Matter*

In Malcolm Gladwell's, 2006 New York Times bestseller, *Blink*, he discusses the work conducted by researcher John Gottman who can predict with 95% accuracy, after watching a husband and wife talking for one hour, whether the couple will still be married 15 years later. The premise of *Blink* is that certain quick decisions often prove accurate. During Mr. Ceresney's speech[5], he stated that "the state of a firm's compliance function says a lot about the firm's likelihood of engaging in misconduct and facing sanctions." Mr. Ceresney also specifically noted that you can "predict a lot about the likelihood of an enforcement action by asking a few simple questions about the role of the company's compliance department in the firm." Such questions included:

- Are compliance personnel included in critical meetings?
- Are their views typically sought and followed?
- Do compliance officers report to the CEO and have significant visibility with the board?
- Is the compliance department viewed as an important partner in the business and not simply as a support function or a cost center?
- Is compliance given the personnel and resources necessary to fully cover the entity's needs?

Mr. Ceresney observed that "far too often, the answer to these questions is no, and the absence of real compliance involvement in company deliberations can lead to compliance lapses, which, in turn, result in enforcement issues". Mr. Ceresney reassured the audience of CCOs noting that, "the Commission is in your corner when your work is hindered by uncooperative or obstructionist business personnel, and that a number of our actions have sent the clear message that you must be provided with the resources and support necessary to succeed".

Mr. Ceresney also highlighted a few important points that investment advisers should be sure to remember. Mr. Ceresney noted that compliance officers have the full support of the Commission and that the SEC relies on them "as essential partners in ensuring compliance with the federal securities laws", and "will do all we can to help you perform your work". Mr. Ceresney made clear that the SEC will not hesitate to bring enforcement actions against personnel in circumstances where they have deceived or misled compliance personnel, or where their failure to provide compliance professionals with adequate resources and information causes compliance rule violations.

The point he was driving home is that management must support the CCO and provide proper resources.

Last summer, the SEC settled a proceeding brought against Pekin Singer Strauss Asset Management Inc., Ronald L. Strauss, William A. Pekin, Joshua D. Strauss[6], its former President, as well as other principals at the firm. The proceedings were initiated when it was determined the compliance function within the firm was not adequately staffed and not adequately resourced. An independent compliance consultant along with SEC staff subsequently identified a number of compliance violations during an examination of the firm that had not been previously detected by the firm or its Chief Compliance Officer.

**Many of the SEC's findings are worth highlighting:**

- The SEC found that the President had promoted the CCO to that role, knowing that he had limited prior experience and training in compliance; that the new CCO still retained his previous functions, including backup trader, backup trade reconciliation, research analyst, and portfolio manager; and that he failed to provide the CCO with sufficient guidance regarding his duties and responsibilities in his new role.
- The SEC found that the CCO lacked the experience, resources and knowledge as to how to adopt and implement an effective compliance program or how to conduct a comprehensive and effective annual compliance program review. Additionally, the firm failed to conduct the required annual compliance reviews several times, and there was a three-year gap between annual reviews.
- In spite of the circumstances, the CCO was able to learn certain aspects of the CCO role from the former CCO and from attending a compliance conference. He was thus able to identify certain weaknesses in the firm's compliance program and began to implement new compliance policies and testing procedures.
- The SEC found the President did not make the compliance program a priority for the firm. He directed the CCO to prioritize his investment research responsibilities over compliance, and also gave him other responsibilities including naming him CFO.
- Between his research and other responsibilities, the SEC found that the CCO was only able to devote between 10% and 20% of his time on compliance matters.
- The CCO told the President on multiple occasions that he needed help fulfilling his compliance responsibilities, including the annual compliance program review. However, the President told the CCO that the firm's primary responsibility was serving clients, and that they could address any problems that came up in an SEC examination at that time.
- The firm eventually engaged a compliance consultant to assist the CCO, primarily because the firm needed to conduct an annual review for the board of a mutual fund that the firm advised, and they needed the compliance consultant to handle the annual review.
- The President narrowed the scope of the compliance consultant's engagement from a more comprehensive compliance review, in part to reduce the cost of the engagement.
- The compliance consultant issued a report that enumerated several compliance deficiencies at the firm. Shortly thereafter, the SEC exam staff conducted an examination and cited the firm for several compliance deficiencies, most notably the failure to conduct annual compliance program reviews and code of ethics violations surrounding personal trading accounts.

4. https://www.sec.gov/ocie/announcement/ocie-2015-risk-alert-cco-outsourcing.pdf
5. http://www.sec.gov/news/speech/keynote-address-2015-national-society-compliance-prof-cereseney.html
6. http://www.sec.gov/litigation/admin/2015/ia-4126.pdf

- Subsequently, the CCO stepped down as CCO and remained as CFO. The firm hired a new CCO with compliance and operations experience.

Based on these and other findings, the SEC found the firm willfully violated the Advisers Act, and the firm eventually settled with cease-and-desist orders and payment of monetary damages.

The SEC, in agreeing to accept the settlement offer, noted the firm's remedial efforts, which included:

- The firm expanded its relationship with its outside compliance consultant and hired an additional full-time Compliance Director to support the firm's CCO.
- The firm has continued to retain a compliance consultant as an additional compliance resource and to ensure that the consultant will monitor and advise on the firm's annual compliance program reviews.
- The firm hired a new CCO.

While many of the specific factual findings may strike some readers as being egregious, many firms do struggle in trying to find the right level of experience, resources and independence for their CCOs and compliance obligations.

It is also common, particularly with smaller advisers, that many CCOs have other non-compliance roles with substantial duties.

Many of these "dual hatted" CCOs also have specific expertise in those other non-compliance areas, and may feel challenged to find the time or acquire the expertise to discharge their compliance duties in the way the SEC and investors would expect.

A notable factor in this case is the lack of a "compliance culture," or "tone from the top," which can manifest in a variety of ways, such as failing to appreciate the importance of the compliance function, prioritizing non-compliance functions over compliance functions or not allocating appropriate resources to compliance functions.

Another frequent compliance violation is the failure to conduct the required annual compliance review. Whether it is due to time constraints, resource constraints or having other priorities, it is important for registered investment advisers to remember that the annual compliance review is a legal requirement and there are potentially significant consequences for overlooking this obligation.

Finally, it is noteworthy that the facts in this case date back a few years. The current regulatory regime emphasizes "broken windows," enforcement actions, record penalties, and "message cases." There is also enhanced focus on CCOs as "gatekeepers," in addition to CCO liability. All this to say that we all can expect the SEC to continue to focus on firms' CCOs and their compliance efforts and resources.

*Stay Diligent and Informed*

Executives and fund boards should keep abreast of current enforcement actions taken by the Commission, especially relating to CCO and executive liability. Such cases include the Ted Urban case which can provide insight on how advisers can avoid coming under fire from the SEC. This seminal case provides that, in addition to executives and directors, CCOs can be held liable for failure to supervise if they are deemed a "supervisor" by a totality-of-the-circumstances review. Knowing what steps the regulators are taking, who they are going after, and for what specifically, will help firms steer clear of enforcement action.

*What to look for when choosing a CCO*

Given the SEC's recent cases and speeches, advisers should ensure that the CCO has the right **experience and background** — specifically a background that shows he or she understands all relevant SEC regulations. Advisers should also ask questions and understand the niche experience that is needed to be an effective CCO. Several factors distinguish a well-suited CCO from an inexperienced, lower-cost alternative. For example, a suitable CCO will customize a compliance program to the fund's business, interact with service providers and test the compliance program to appropriately identify potential failures.

Another important aspect for advisers to consider when determining whether it is beneficial to hire an outsourced CCO is **accountability and time-management skills**. This is critical for a CCO because if he or she fails to either cover the ground required, or follow through on designated responsibilities, the adviser could be subject to enforcement action. Mr. Ceresney spoke about how the SEC will charge CCOs in cases where they have failed to carry out their responsibilities. Certain individuals might have exceptional experience and backgrounds and yet lack this basic skill of accountability. Advisers must be diligent to ensure hired CCOs are dependable and reliable.

CCOs must not only ensure that they create the necessary policies and procedures to effectively prevent violations of federal securities laws, they must also take steps to ensure such policies and procedures are properly implemented and tested. The failure to do so allows for impropriety to occur, and harms the shareholders and industry at-large. Ask potential CCO candidates how they will create or manage your policies and procedures. Asking detailed questions will help you identify the best fit candidate.

It is important to note that CCOs should make it a priority to keep up to date on new and changing securities regulations. In doing so, they will recognize what rules they are being required to comply with and can subsequently impart that knowledge to the adviser, providing assurance that they are capable of fulfilling the responsibilities delegated to them. Be sure you communicate with your CCO, and understand his or her continuing education efforts and diligence.

*The CCO Needs Oversight Too*

Failing to monitor the CCO's activities is more common than you'd think. Advisers should monitor outsourced CCOs the same way they would a full-time CCO. When choosing to outsource compliance duties, executives and directors should make a concerted effort to ensure that they are comfortable with the individual, as well as his/her ability and self-discipline. The adviser can't simply delegate these important responsibilities and walk away. They must remain diligent in their oversight, and stay current with the ever-evolving regulatory environment. The inherent risks and pitfalls that the regulators associate with outsourcing the role of CCO should be considered by all advisers, even ones that do not outsource the position. This is because the weaknesses found are not necessarily correlated with the decision to outsource or not, but are often related to the specific skills and drive of the individual CCO.

Not only should senior management oversee CCOs to be sure they are actively doing their job, but also to prevent fraud in the extreme cases. There have been several cases where compliance personnel are the perpetrators. For example, the SEC is currently taking action against a compliance associate alleged to have traded on material nonpublic information obtained from his investment bank employer Goldman Sachs. The SEC asserts that Yue Han misappropriated nonpublic information about impending mergers, and traded on this information through undisclosed brokerage accounts in violation of the firm's policies[7].

7. http://www.sec.gov/litigation/complaints/2015/comp-pr2015-267.pdf

***Compliance Personnel Takeaways***

*Go Desktop?*

Recent SEC deficiency letters emphasize that the policies and procedures need to be detailed and explain your overall operations. This can present a conundrum where you might be increasing your liability exposure with such over-disclosure. Compliance needs

to weigh the many reasons to *not* include every minute risk and corresponding control in a manual.

For example, former Commissioner Gallagher opined that Rule 206(4)-7 is at the center of the Commission's concerns.[8] The rule is "not a model of clarity". It provides, in part, that the adviser is required to adopt "and implement written policies and procedures reasonably designed . . ." to prevent violations of the Act. On its face, the rule addresses the adviser in that it requires *the firm* to designate a CCO. However, while the adviser is responsible for implementation, the SEC has shown an interpretation of Rule 206(4)-7 as if it is directed to CCOs.

Yet neither the Rule itself, nor the SEC offer guidance on compliance. According to Gallagher, this sends a troubling message, "…that CCOs should not take ownership of their firm's compliance policies and procedures, lest they be held accountable for conduct that, under Rule 206(4)-7, is the responsibility of the adviser itself. Or worse, that CCOs should opt for less comprehensive policies and procedures with fewer specified compliance duties and responsibilities to avoid liability when the government plays Monday morning quarterback." Gallagher stated he is "…very concerned that continuing uncertainty as to the contours of liability under Rule 206(4)-7 will disincentivize a vigorous compliance function at investment advisers." He recommended that the Commission take a hard look at Rule 206(4)-7 and consider whether amendments, or at a minimum staff or Commission-level guidance, are needed to clarify the roles and responsibilities of compliance personnel.

As a result of this uncertainty, many argue for shorter, pointed compliance manuals separate from desktop procedures, or even suggest avoiding desktop policies altogether. However, given recent cases and deficiency letters, it is possible that a CCO who does not consider every material detail to include in their policy and procedure manual may be exposing their firm to liability.

According to Mr. Ceresney[9], "When we have charged a CCO with causing violations of rule 206(4)-7, we have not second guessed their professional judgment, critiquing the choices they made in the creation of policies; rather, we have brought actions where there was a wholesale failure to develop such policies or to implement them, and where the CCO was properly held responsible for that failure."

The root of the issue is that you need a risk assessment that flows into the policies and procedures and certain policies and procedures should therefore be desktop. This should be considered one of the higher risk areas in your compliance program.

Rules 206(4)-7 and 38a-(1) suggests areas where advisers and funds, respectively, should consider adopting policies and procedures. They do not provide specific instruction on how policies and procedures should address: 1) how to monitor and assess employees for conflicts of interest; 2) how to monitor employees who participate in firm-approved outside business activity ("OBA"); or 3) how to determine when an employee's OBA should be disclosed to the board or clients.

It is this type of detail regarding policies and procedures that causes grave concern for CCOs.

*Continue to try to avoid being deemed a supervisor - lessons learned from Ted Urban*

Even though Chief Compliance Officer Ted Urban was exonerated from liability, a curious dicta emerged from SEC enforcement action against him. The dicta provided that Urban was deemed a "supervisor" over an employee, a classification which led to additional liability placed over him. Under a totality-of-the-circumstances review, the administrative judge had to determine whether Urban met the classification of "supervisor." The court reviewed whether Urban had the "requisite degree of responsibility, ability or authority to affect" one's conduct, despite not being a supervisor in the classical sense.

Despite Urban not having any of the traditional powers associated with a person supervising a firm's employees, the case law found Urban to be classified as the employee's supervisor. Once deemed a "supervisor", one is subject to maintaining "reasonable supervision," which extends above and beyond the usual and customary duties of a CCO. Reasonable supervision is determined by whether there is negligence under the reasonably prudent person test. This is an unnecessary hurdle for a CCO when so much liability is inherently built into Rule 206 (4)-7, Rule 38a-1 and the corresponding securities laws. The Ted Urban case also emphasizes the need to review your insurance coverage and make sure CCOs are well covered and protected shielded from liability.

*Know Your Responsibilities and Be Diligent*

The SEC noted in the Risk Alert following the Outsourced CCO Initiative that in many instances, the outsourced CCOs were designated as the individuals responsible for conducting reviews to ensure compliance met the requirements of Rule 206(4)-7.[10] This included testing of the existing policies and procedures. However, the staff observed throughout these examinations a "general lack of documentation evidencing the testing" recorded by the firms. All CCOs should take note of this observation, as it is not limited solely to outsourced CCOs.

CCOs must remain proactive when updating the compliance program, and ensure that they stay current with guidance provided by the SEC through recent cases, speeches and risk alerts.

Understand that your duties as CCO are to develop and implement the compliance program, but also understand that you alone are not solely responsible for the implementation and development of a "*culture*" of compliance. It is imperative that executive management and fund boards work cooperatively with CCOs to efficiently mitigate risks and liabilities particular to their business model. This is essential to proper risk assessment, and the creation, implementation and testing of a successful compliance program.

Fund boards, adviser personnel and compliance professionals should be sure to keep up with current regulatory guidance and enforcement cases. This is not just best practice; this should be the only practice for any staff tasked with compliance oversight. CCOs now find themselves more and more often coming under the SEC's crosshairs for issues related to the compliance programs they oversee. This presents additional risks that are largely unnecessary but based on recent history, it stands to reason that the SEC will continue naming CCOs for compliance oversights. ✦

8. Statement on Recent SEC Settlements Charging Chief Compliance Officers With Violations of Investment Advisers Act Rule 206(4)-7 Commissioner Daniel M. Gallagher, June 18, 2015

9. http://www.sec.gov/news/speech/keynote-address-2015-national-society-compliance-prof-cereseney.html

10. https://www.sec.gov/rules/finasl/ia-2204.htm#P170_59174

THE NATIONAL LAW JOURNAL
APRIL 18, 2016
An ALM Publication
THE PRACTICE | Commentary and advice on developments in the law

# Cybersecurity Compliance Just Got Tougher

Companies need specific, well-executed plans to meet growing demands of federal and state agencies.

BY NICK AKERMAN AND DAN GOLDBERGER

KIRILL_SAVENKO/ISTOCKPHOTO.COM

While cybersecurity risks have increased, government regulation has traditionally lagged behind. Recently, some government entities have tried to catch up by mandating that companies take a proactive approach toward protecting personal and competitively sensitive data. The move is a departure from the traditional reactive response of simply notifying consumers after their personal data is breached.

With this shift in emphasis, companies are asking the obvious questions: "What are we expected to do and what is a proactive cybersecurity compliance program?"

Both on the state level and through federal regulatory agencies, the government is beginning to dictate a comprehensive compliance approach to data protection. Late last year, the U.S. Securities and Exchange Commission's Cybersecurity Examination Initiative directed broker-dealers to "further assess cybersecurity preparedness in the securities industry." Thus, the SEC announced that it "will focus on key topics including governance and risk assessment, access rights and controls, data loss prevention, vendor management, training and incident response."

In January, the Financial Industry Regulator Authority announced that in reviewing a securities firm's approaches to cybersecurity risk management its examinations may include "governance, risk assessment, technical controls, incident response, vendor management, data loss prevention and staff training." On the state level, Massachusetts is the only state thus far to require all businesses that store personal data of its residents to secure that data through a compliance program modeled after the federal sentencing guidelines.

The framework under the federal sentencing guidelines is the gold standard for an effective compliance program. Having expanded well beyond its original goal of detecting and preventing criminal activities, it is fast becoming the corporate framework to protect data. These guidelines establish seven steps for companies to follow: first, promulgate standards and procedures; second, establish high-level corporate oversight including the board of directors that

must provide adequate funding of the program in proportion to the size of the company and the risk; third, place responsibility with individuals who do not pose a risk for unethical behavior; fourth, communicate the program to the entire workforce; fifth, conduct periodic audits of the effectiveness of the program; sixth consistently enforce the polices; seventh establish mechanisms for reporting violations.

## COLLABORATION IS CRITICAL

Because a compliance program must be tailored to an organization's culture, it is critical to its success that all data-protection stakeholders collaborate in its creation and daily operation. This means that data compliance is not just an issue for information-technology security. Other stakeholders include human resources and legal, which are responsible for company rules, employee agreements and training, and may assist in responding to company data breaches; risk management, which may determine, along with legal, the adequacy of the company's cyber insurance; and compliance, which is often the logical focus of the company's data protection efforts.

Stakeholders in turn should focus on six areas of risk when developing a company-specific compliance program to minimize the risks posed by each area.

First, hiring is the time to explain to new employees the rules in place to protect the company's data. Additionally, companies must approach hiring defensively, ensuring new employees do not bring into the workplace data that belongs to a competitor that can result in civil or criminal liability.

Second, company rules and policies should spell out what employees can and cannot do with the company network and form the foundation of top-to-bottom workforce training. At least one court has recognized that such "explicit policies are nothing but security measures employers may implement to prevent individuals from doing things in an improper manner on the employer's computer systems." (*American Furukawa v. Hossain*).

Third, agreements with employees and other third parties are a key component of data protection. Employee agreements are an opportunity to reinforce the lack of an expectation of privacy in using company computers and define the scope of authorized access. When company data is outsourced to a cloud provider, agreements formalize the responsibilities of that third party to protect the company's data.

Fourth, technology can be employed not only to secure data but to define who is authorized to access what portion of the network and provide admissible evidence of a breach. Information-technology security, working with legal, can prepare mechanisms to capture audit trails in the network that can be used to identify the source and scope of a breach.

Fifth, effective termination procedures are critical. This is when insiders are most likely to steal company data to use at their next job. This is also the last opportunity to remind departing employees of their postemployment obligations to maintain the secrecy of company data, to return all company data and for the company to inventory the data returned.

Finally, if a breach occurs, it is important to have protocols in place to quickly determine the scope of the breach and the appropriate response. Companies must therefore have in place an overarching plan to investigate suspected breaches and to mobilize internal and external resources.

For a data-compliance program to work consistently, it must be a collaborative effort among all stakeholders and comprehensively focus on mitigating the risks to the company's data from multiple and unexpected sources.


**NICK AKERMAN** *and* **DAN GOLDBERGER** *are partners in the New York office of Dorsey & Whitney. Akerman's practice focuses on the Computer Fraud and Abuse Act and the Racketeer Influenced and Corrupt Organizations Act. Goldberger's practice focuses on financial services, intellectual property, trade secrets and data protection.*

NSCP
THE NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

NOVEMBER 2016 SPECIAL REPRINT
Currents

# CCO Liability: Managing Liability: Navigating Indemnities and Insurance Options

By Janaya Moscony

**Introduction**

This is the third segment in our three-part series focused on Chief Compliance Officer liability, and managing the different sources of risk. In Part I [Dec 15, liability and outsourcing] of our series, we discussed CCO liability and CCO outsourcing including recent enforcement actions, and the benefits and concerns with respect to outsourcing the CCO position. In Part II [Feb 16, liability and outsourcing], we discussed important factors to consider when choosing a CCO, including the candidate's ability to assess the firm's risk and implement corresponding mitigating procedures. In this final installment, we discuss indemnifications and insurance as potential remedies to address the direct financial risks to a CCO.

It is not only investment advisers and fund boards that face regulatory liability; CCOs themselves are increasingly finding themselves in the SEC's crosshairs. Despite all the proper steps a Chief Compliance Officer can take to mitigate compliance risk and avoid an enforcement action, sometimes bad things happen to good people. Defending any regulatory enforcement action can be expensive, and there may be direct financial consequences for the CCO. Having negotiated a solid indemnification with the employer and/or having successfully transferred some or all of the personal financial risk to an insurance underwriter can be an important component to limiting personal financial liability.

In ICI Mutual's 2015 Annual Claims Trends[1], the company noted that 2015 saw an increase in the overall number of claims submitted to them by fund groups under their D&O/E&O policies. Further, ICI Mutual stated that nearly 25% of their insured fund groups submitted at least one claim notice during 2015. Over the five-year period from 2011 to 2015, approximately 50% of their insured fund group submitted at least one claim notice. The increase in claims by fund groups is alarming and highlights the need to ask the right questions when seeking or renewing insurance policies.

When considering insurance, Chief Compliance Officers first and foremost need to understand exactly what risks can be transferred. Careful attention must be given to matching the exact insurance products and riders to the risk sought to be transferred, and knowing where the pitfalls exist which could result in a claim being denied. E&O and D&O coverage have been around for decades and as such, have established standards and terms. However, other types of coverage such as cybersecurity insurance, do not have the same conventions as they are relatively new products. This article will review the three types of insurance many financial services firms consider today to help manage specific business risks.

***Errors & Omissions (E&O)*** policies are widely used throughout the industry to help protect against claims by clients arising out of professional services provided by the insured. ***Directors & Officer Liability (D&O) coverage*** can be added to an E&O policy or purchased separately, to protect the firm as well as the directors, officers, partners and employees of the insured entity for claims arising out of business decisions, not investment decisions. D&O is where you would find coverage for "claims" (including formal regulatory investigations costs) by non-clients such as the SEC and US Department of Labor ("DOL") that are not triggered by a client complaint.

***Side A, Independent Directors Liability ("IDL") Insurance*** typically serves as a supplemental policy to D&O coverage, and would come into play in circumstances where indemnification is not available or is refused. Side A IDL insurance helps fund independent directors mitigate liability and exposure to various risks associated with indemnification (when a fund is legally prohibited from paying for a director/officer's defense); erosion risk (when a D&O policy has exhausted its limits of liability); and coverage risk (when a D&O policy does not provide coverage for the situation). Depending on the indemnifications, CCOs may find themselves in a conflicting situation with their employers who could withhold these protections.

***Cyber Insurance*** is a type of insurance designed to cover consumers of technology services or products. More specifically, the policies are intended to cover a variety of both liability and property losses that may result when a business engages in various electronic activities. Most notably, but not exclusively, cyber policies cover liability for a data breach in which client information is exposed or stolen by an individual who has gained access to the firm's electronic network. It is another type of insurance policy to consider, however, it has important limitations that you need to keep in mind.

1. ICI Mutual "A Review of Claims in the Mutual Fund Industry (January 2015-March 2016)" Claim Trends, 2015

**About the Author**

Janaya Moscony is President of SEC Compliance Consultants, Inc., www.seccc.com. She can be reached at Janaya@seccc.com.

*Additional Riders*

There are many insurance "riders" that can accompany the policies outlined above. An insurance rider is an available enhancement option that your broker can negotiate to be included in your policy. Riders can help supplement your existing coverage and provide additional benefits. Financial professionals need to understand policy definitions and exclusions, and discuss the various options available with their broker.

We presented several questions applicable to financial services firms to three experts in the insurance field. The questions and responses are below.

**Expert #1 Andy Fotopulos, President at Starkweather & Shepley Insurance Corp. of MA**
(www.starshep.com) (AFotopulos@starshep.com)

*Q: What terms and conditions should Chief Compliance Officers be aware of with respect to insurance policies and riders?*

A: When purchasing or reviewing coverage, CCOs should always be aware of the following:

- Whether the insurance policy is for errors and omission only, or does include directors and officers;
- Whether there is an exclusion in the policy for claims brought by regulators (e.g. E&O vs D&O);
- How the policy defines an "Individual Insured" (i.e. outsourced CCO may not be covered);
- How the policy defines a "claim" and what event(s) trigger coverage. Some policies trigger coverage at the time of a subpoena. Others don't trigger coverage until there is a formal investigation. This is essential to understand because there could be a time period of several months in between a subpoena and formal investigation where there is a gap in coverage; and
- How the policy ensures that when new limits of liability are purchased, claims for past unknown acts are covered under those new limits.

*Q: In order to maximize coverage benefits, what riders and coverage increases are available in the marketplace that firms, directors and officers can obtain for little or no cost?*

A: Here are some things to consider:

- Request broader definitions: Ask an insurer to provide a broader definition of a claim, professional services and other important terms. This can help ensure that when a claim does indeed arise, you have a policy which casts the widest possible net.
- Costs of Corrections: Costs of correction coverage provides for indemnification to an insured company for its costs of correcting situations that, if not corrected, would result in legal liability on the part of the insured company. Additionally, verify that no action or other "claim" is necessary to trigger this coverage. The basic purpose of this coverage is to permit prompt correction by insured companies of operations-based errors so that more expensive problems or litigation can be avoided down the road.
- Pre-Claim Extension coverage: Pre-Claim Extension coverage can help supplement an existing insurance portfolio. For example, if a firm was to receive a subpoena but no individuals are named as being investigated or brought up on charges, many insurance policies are not triggered until such an event occurs or a formal investigation is declared. With 'Pre-Claim Extension' the insured can go back and be reimbursed for expenses that were paid prior to meeting the definition of 'Claim' – thus triggering coverage under the insurance policy. Be aware, however, that the retention amount is typically higher for such situations. Most D&O policies will trigger only after a formal investigation or an allegation of wrongdoing has been presented by a regulatory body. This means that it is likely that all expenses incurred during the audit or informal investigatory stages will be paid by the insured. The take-away is to be sure the firm's D&O policy has been enhanced with Pre-Claim Defense coverage, in order to cover those earlier costs in cases where the audit or investigation turns into a covered claim.

*Q: What are the biggest mistakes a Chief Compliance Officer makes with respect to insurance coverage?*

A: There are 5 typical mistakes CCOs and firms should be sure to avoid when it comes to their liability coverage.

1. Be very careful with joint policies. With a joint policy that includes an insured fund, board and adviser, one aggregate limit can be exhausted by a claim thus leaving nothing for the Chief Compliance Officer. For example, if the fund, adviser, administrator and CCO all are all being sued, the limits might not be enough. Often a joint policy is purchased when the adviser and fund complex are under common control. Independent directors often buy their own separate policies.
2. The obligation for an entity to indemnify a CCO depends on the state of incorporation so it matters whether or not the CCO is recognized as a "corporate officer" of the insured entity. Some states require that the CCOs are appointed in the bylaws of the insured entity as a corporate officer. Moreover, other states might require that the CCO also be appointed as a corporate officer in state filings. Of course, as the CCO, you believe you are covered under your firm's D&O, but have you verified this? A majority of CCOs are not subject to indemnification unless designated in the by-laws as a corporate officer or have a stand-alone agreement in writing guaranteeing indemnification. The take-away is that CCOs should review the state by-laws to make sure they are covered, as the title of Chief Compliance Officer alone doesn't mean he or she is a corporate officer of the firm for insurance coverage purposes.
3. Know the difference between E&O and D&O. The intent of an E&O policy is to cover claims by clients arising out of the firm's "professional services". The intent of D&O is to protect the insured entity as well as its directors, officers, partners and employees, against litigation arising out of business decisions. This is typically where to find coverage for the CCO for claims, including investigations by regulators. But just because an E&O policy may define an "insured" to include the Chief Compliance Officer, that doesn't mean they're covered for their professional services as CCO. The CCO needs to understand what they are covered for and what triggers coverage. In other words, consider who needs to bring the claim in order to have coverage. Quite a

few E&O policies will only cover the expense of a formal regulatory investigation against a CCO if the investigation is initiated due to a client complaint. The take-away is to ensure that D&O/E&O policy does not contain an exclusion for "claims brought by regulators."

4. The CCO may be in conflict with their firm at some point, and he or she may withhold indemnification. For example, if a CCO is terminated and brings an employment practices claim, the firm could retaliate and bring a defamation suit against the CCO. How would the CCO's legal expenses be covered? In another scenario, the employer may want to move on by settling a claim while the CCO is fighting to maintain his or her professional reputation and future employment. How will the insurance policy respond to such conflict between insured parties?
5. If the individual is an "outsourced" CCO or independent contractor, he or she needs to be sure that the insurance policy's definition of an individual insured is broad enough to include a non-W2 Employee.

*Q: How much coverage is enough?*

A: Ideally, the right coverage amount should equal the amount of a claim. In other words, there is no set rule, but one needs to remember that although fines and penalties are not covered under an insurance policy, legal defense costs can run much higher and should be covered with proper liability coverage. Insureds should request to receive proper benchmarking based on their particular niche of the investment industry from their insurance professional before obtaining any policy and/or rider.

*Q: Are CCOs still covered once they leave a firm?*

A: Most policies from leading insurers cover any past, present of future directors, officers, partners and employees. However, low cost insurance policies may not. A strong recommendation would be to negotiate such tail coverage in advance of placing the insurance policy as it will be far more reasonable if negotiated in advance of placing coverage. If the firm waits until a litigation action is eminent, the availability for tail coverage may be limited or cost prohibitive.

Finally, firms should not open themselves up to the prior exposure of firms they may be acquiring. The best defense against this exposure is to ensure that the acquired firm purchases its own policy which extends coverage to match the various state statutes of limitations for bringing a claim.

**Expert #2 Stephen T. Cohen, Partner at Dechert LLP (www.dechert.com) (stephen.cohen@dechert.com)**
Given Mr. Cohen's experience with registered funds, our focus shifted to liability specifically associated with overseeing these products.

*Q: When can registered fund assets be used to cover legal expenses for the board and officers?*

A: A fund generally can cover the members of its board and its officers for all expenses reasonably incurred or paid by him or her in connection with any claim, action, suit or proceeding in which he or she becomes involved as a party, or otherwise by virtue of his or her being or having been a member of the board or an officer. The members of the board and officers would only be covered to the extent that the fund has sufficient assets to reimburse or pay the expenses incurred with respect to a claim. Similarly, if a claim involves a particular fund that is one of several series of a corporation or trust, the assets of only that fund may be used to provide indemnification.

Under federal law, a member of the board or an officer who has been adjudicated by a court to be liable (or, in some cases, determined by the board as likely to be liable) to the fund or its shareholders by reason of willful misfeasance, bad faith, gross negligence or reckless disregard of the duties involved in the conduct of his or her office is not entitled to such indemnification. State law also may prohibit indemnification under similar circumstances.

*Q: How are fund directors and officers covered against personal liability for official actions?*

A: Fund directors and officers generally have two sources of coverage to protect themselves from personal liability for actions taken in their official capacity. First, funds generally provide their directors and officers with indemnification, which typically allows directors and officers to be reimbursed from fund assets for liabilities (including legal expenses) incurred by them as defendants or witnesses in fund-related actions, subject to certain limitations. A fund's indemnification protections are set forth in the fund's organizational documents and often times, provide directors and officers with the maximum indemnification permitted under state and federal law.

The other source of coverage is through insurance. Although there is no legal requirement that they do so, most funds arrange to purchase such insurance. A directors and officers/errors and omission ("D&O/E&O") insurance policy typically provides coverage for liabilities, including legal expenses, resulting from negligence or breach of duty by directors or officers in performance of their duties (though not for liabilities resulting from their fraud, dishonesty, or similar misconduct). It is common for D&O/E&O insurance policies to require a retention (or deductible) before the insurance policy will begin to cover claims, although certain types of coverage for directors and officers will respond without a retention.

*Q: What costs and conduct are typically covered under fund indemnification and insurance arrangements?*

A: Although indemnification and insurance arrangements generally cover personal liability and costs incurred in defense of fund directors and officers, such as legal or other defense costs, there are certain limitations to the amounts of coverage available to fund directors and officers, as well as the types of claims that will be covered by a fund's indemnification and insurance arrangements. For example, indemnification would be limited to the amount of fund assets available, and insurance would be subject to the maximum amount of coverage in the policy itself. In addition, as already mentioned, a fund's indemnification and insurance arrangement generally would not cover disabling conduct that may arise from bad faith, willful misfeasance or other similar types of misconduct in their official capacity and may be subject to certain other conditions. In fact, the federal securities laws expressly preclude such coverage.

*Q: What factors may a board wish to consider in connection with approving or renewing a D&O/E&O insurance policy?*

A: It is important for boards to consider appropriate factors and information in connection with approving or renewing a fund's D&O/E&O insurance policy. Certain relevant factors and information generally would be common to all funds, such as

the cost of the coverage, the parties covered as insureds, the amount of fund assets, the types of strategies pursued and the reputation of the insurance carrier(s). In addition, fund boards may wish to consider the evolution of regulatory and legal risks and exposures applicable to fund directors and officers generally, as well as the particular funds overseen by the board. For example, a board may wish to take into account evolving risks, such as cybersecurity risks, or changes in regulatory initiatives and the focus of the plaintiffs' bar in determining whether to increase the level of coverage. Boards may also wish to take into account whether a stand-alone or joint policy is preferable; that is whether the policy covers only a fund and its directors and officers or whether it extends to service providers, including the fund's adviser. If the full limit of liability is available to the fund and its directors and officers, the adviser would need to arrange and maintain its own insurance.

*Q: Will D&O/E&O insurance policy assets be utilized before Fund assets?*

A: Generally, a D&O/E&O insurance policy serves as the second line of defense after indemnification, and the typical sequence involves the fund initially providing indemnification for covered expenses and the insurance policy compensating the fund for those expenses, subject to a deductible (or retention). Although this is typically the sequence, a D&O/E&O insurance policy also may advance covered expenses to a member of the Board or an officer, under certain circumstances.

*Q: What are the most common situations when Fund Directors/Officers need to tap into insurance/fund assets?*

Typical claims include, among others, allegations by shareholders of a fund that members of the board or officers breached their duties to the fund or mismanaged the fund, allegations of material misrepresentations in a fund's prospectus, and allegations of failure to appropriately supervise a service provider to a fund.

*Q: What are the protections/defenses in place for fund directors? Are CCOs afforded the same protections? Also, is outside counsel ever subject to potential liability?*

A: Provided they have exercised reasonable care and are reasonably informed, and have acted under the reasonable belief that their actions are in the best interest of a fund, the members of the board and officers generally will not be responsible or liable for the outcome of their acts or omissions or negligence or wrongdoing. CCOs, however, are subject to certain responsibilities under the federal securities laws that may not afford them the same level of protections for their actions. Outside counsel is subject to potential liability arising from negligent acts or omissions that sufficiently prove legal malpractice that causes harm, in this case, to the fund and shareholders. Outside counsel commonly purchase insurance coverage for claims of legal malpractice.

*Q: Are Fund Directors ever found personally liable or are they covered by fund assets and/or D&O/E&O insurance policies?*

A: As a result of limitations of liability under law and charter documents as well as the protections afforded under indemnification and D&O/E&O insurance policies, it is rare for a member of the board to be personally liable in connection with actions taken in his or her capacity as such. In almost all instances, a board member is covered by fund assets and/or D&O/E&O insurance policies.

**Expert #3 Michael Brice, Co-Founder BW Cyber Services**
(www.bwcyberservices.com)
(michael@bwcyberservices.com)

As cybersecurity insurance has begun saturating the market, advisers should understand the options. Advisers need to be aware of their specific cyber risks and how their cyber policies mitigate those risks.

*Q: What is the biggest misconception about cyber insurance?*

A: The biggest misconception is that cyber insurance will transfer cyber risk, and is an alternative to having a strong cyber program. Many advisers (and investors) are under the impression that a cyber insurance policy will mitigate their lack of cyber controls or lack of in-house competency with respect to cybersecurity. If anything, it's the exact opposite situation. The policy will only go into effect once a certain minimum level of cyber competence has been met. While not comprehensive, some requirements of cyber competence include:

- Executive understanding (e.g., signature on a policy statement) and oversight (e.g., annual review of the policy) of a formal cyber program;
- Certain industry best practices are considered standard operating procedures these days such as: firewall, AV & Malware with periodic scans, timely software updates & patches, password policy and basic encryption of data. There is no specific framework, but these are some of the basic controls an insurer wants to see is in place.
    - Cyber Risk Assessment and implementation of corresponding controls to address the highest risks
    - A breach response process;
    - Security training for all employees;
    - Documented policies related to the above items and supporting evidence that the policies are reviewed and enforced;
    - Some basic control testing like a penetration and vulnerability testing - especially if a client has a webpage or web portal, and;
    - An understanding of the amount of PII and where/how it might reside and be protected.

**Conclusion**

Boards and CCOs should always consult with experienced insurance brokers, compliance consultants and fund counsel to ask the right questions and work to ensure they have the best coverage in the event of a legal or regulatory issue. It is essential to understanding the available protections. It is rare for a CCO or member of the board to be personally liable in connection with actions taken in his or her capacity as such. In almost all cases the director or officer exercises sound judgment, indemnities assets or D&O/E&O insurance policies will cover those confronted with legal issues. ★

THE NATIONAL LAW JOURNAL
JUNE 30, 2014
An ALM Publication

THE PRACTICE

# SEC Playing Bigger Role in Cybersecurity

Besides clarifying disclosure requirements, the agency is prompting companies to take proactive steps.

BY NICK AKERMAN
AND PARKER SCHWEICH


Cybersecurity threats have reached a point where they cannot go ignored by any government agency, even the U.S. Securities and Exchange Commission. Although an agency that is tasked with protecting investors is not one that typically comes to mind in the battle against cyberthreats, the SEC does maintain jurisdiction over cybersecurity issues for public companies, broker-dealers and investment advisers, due to its responsibilities for ensuring the disclosure of material information, integrity of market systems and customer data protection.

The SEC began focusing on cybersecurity issues in October 2011 by issuing guidance for public companies on disclosing risks and incidents within the already existing framework of public company disclosure requirements. The SEC's guidance clarified the material information regarding cybersecurity risks and incidents that requires disclosure. Since then, the number of disclosures about data breach incidents, risk factors, trends and uncertainties, and legal proceedings related to cybersecurity threats has grown.

Although requiring this enhanced disclosure regarding cybersecurity issues is intended to protect investors and provide greater information to those with national security responsibilities, it is providing collateral benefits as well. In order to avoid securities law liability for material omissions or misstatements in their public filings, public companies are finding that they must pay closer attention to their policies, procedures and compliance systems in the area of cybersecurity. One area public companies should revisit is their disclosure controls and procedures to ensure that those procedures adequately address reporting up cybersecurity risks and incidents. In addition, many public company boards of directors are starting to rethink risk oversight in this area and, as companies seek new directors to join their boards, experience in overseeing cybersecurity risks may become a highly sought attribute. Companies that want to ensure better cybersecurity risk

oversight at the board level should consider revising their annual board evaluations and director questionnaires in this regard.

The SEC rules, like many other federal and state laws, mandate the disclosure of past failures to protect data. Forty-seven states require notification to consumers if there is a reason to believe that their personal information has been the subject of an unauthorized breach. The federal Health Information Technology for Economic and Clinical Health (HITECH) Act requires similar notifications for the breach of personal health related information. The trend, however, has moved away from the emphasis on the reactive response to data breaches to proactive measures to protect data in the first instance. This proactive approach is embodied in a compliance program consistent with the Federal Sentencing Guidelines requiring computer security policies, the appointment of a security coordinator, training the workforce on protecting company data, periodic auditing of the viability of the program, enforcing its policies, and promptly responding to policy violations.

Compliance programs, if designed properly, can be used to protect shareholder value. The loss of competitively sensitive data can obviously have an adverse impact on shareholder value. The breach of personal customer information that can be used to perpetrate identity theft can be just as harmful. Press reports surrounding the theft of personal data, as recently occurred with Target Corp., can result in devastating publicity undermining customer and shareholder confidence.

The trend is clearly in the direction of making data protection an integral part of a company compliance program. For example, in 2010 Massachusetts began requiring any company that owns, licenses, stores or maintains personal information of a Massachusetts resident to implement a comprehensive written security program for personal information. While there is no foolproof means of stopping cyberattacks, a well-designed compliance program can minimize the potential risks.

Cyberattacks on the infrastructure underlying capital markets have been on the rise too and, as a result, the SEC is paying close attention to cybersecurity for self-regulated organizations and large alternative trading systems. The SEC has issued proposed rules on regulation systems, compliance and integrity, which would require stock exchanges and the like to test their automated systems for vulnerabilities, test their business continuity and disaster-recovery plans, notify the SEC of computer intrusions and recover their clearing and trading operations within specified time frames.

Stock exchanges also have begun taking their own steps to ensure listed companies have cybersecurity protections in place. The New York Stock Exchange has compliance rules that require listed companies to "adopt and disclose a code of business conduct" that includes the protection of confidential information "that might be of use to competitors, or harmful to the company or its customers, if disclosed."

As cyberattacks on financial institutions have become more frequent and sophisticated, the SEC also has focused on cybersecurity risk issues for broker-dealers and investment advisors. In April 2013, the SEC adopted Regulation S-ID, which requires certain regulated financial institutions and creditors to adopt and implement identity-theft programs and which builds upon the SEC's existing rules for protecting customer data such as Regulation S-P.

In light of the risks posed by cyberthreats, all public companies should do the following: Review the corporate compliance program to ensure it adequately covers the prevention and detection of cyberthreats; if one doesn't exist, create a compliance program for the protection of data; update company policies and agreements to adequately protect competitively sensitive and personal data; and institute procedures for effectively reporting to the public cybersecurity risks and breaches.

**NICK AKERMAN** *and* **PARKER SCHWEICH** *are partners at Dorsey & Whitney. Akerman who practices in the New York office, focuses on cases involving the Computer Fraud and Abuse Act and the Racketeer Influenced and Corrupt Organizations Act. Schweich, in Costa Mesa, Calif., heads the firm's Southern California corporate practice group.*

**Nick Akerman, *Partner, Dorsey & Whitney LLP***

Nick Akerman helps clients navigate the judicial system in dealing with complex civil and criminal issues and government investigations with an emphasis on computer technology, the computer fraud and abuse act, the economic espionage act, racketeer influenced and corrupt organizations statute, the foreign corrupt practices act, securities fraud, state and federal trade secret laws and post employments restrictive covenants.

Prior to private practice Nick served as a federal prosecutor. He was an Assistant United States Attorney in the Southern District of New York, where he prosecuted a wide array of white collar criminal matters, including bank frauds, bankruptcy frauds, stock frauds, complex financial frauds, environmental and tax crimes. Nick was also an Assistant Special Watergate Prosecutor with the Watergate Special Prosecution Force under Archibald Cox and Leon Jaworski. Nick has over 30 years of experience in helping clients respond to government investigations and prosecutions and assisting corporate clients prevent and respond to internal thefts and outside hackers. He is a nationally recognized expert on computer crime and the protection of competitively sensitive information and computer data. Nick regularly obtains injunctions for his clients under the federal Computer Fraud and Abuse Act and trade secret laws in various federal courts around the country requiring computer thieves to return stolen computer data and prohibiting the dissemination of the data to competitors. He also guides clients in developing systems, policies and protocols to protect computer data. Nick speaks and writes regularly on protecting computer data, including in his regular computer data column for the National Law Journal. He has been a featured quoted expert on computer fraud and computer security issues in the New York Times, USA Today, the San Jose Mercury News, the Boston Globe, the St. Louis Dispatch, the Sacramento Bee, Forbes, ComputerWorld, CFO Magazine, CNET, CNET Japan, ZDNet, MSN, Internet Week and the Weekly Homeland Security Newsletter. His blog can be found at http://computerfraud.us.

**Janaya P. Moscony, *President, SEC Compliance Consultants***

As a former Securities and Exchange Commission ("SEC") regulator, Janaya has significant experience in the examination, implementation and enforcement of securities regulations. Having worked in private practice as a compliance officer and as a consultant, Janaya is able to provide practical guidance to clients to assist in bridging the gap between the regulatory requirements and business needs. Janaya is a recognized industry expert regularly quoted in the financial press, has appeared on industry television such as CNBC, and is a regular speaker at industry conferences including GAIM-Ops. Janaya routinely assists companies faced with multiple regulators both within the US and internationally including, but not limited to, Canada, South America, Europe and Asia.

Prior to incorporating SEC3 in 2003, Janaya served as Vice President of Bank of Hawaii's Asset Management Group where she advised and implemented the bank's regulatory compliance program. Prior to the Bank of Hawaii, Janayawas employed as a regulatory consultant by BISYS Professional Services ("BISYS"), where she managed numerous client engagements for banks, mutual funds, investment advisers and broker-dealers. Prior to BISYS, Janaya worked as an examiner for the Philadelphia District office of the SEC for 5 years where she worked on routine and “for-cause” examinations and enforcement cases on behalf of a broad range of financial entities. She routinely liaised with other regulatory entities including the NASD, NYSE and state regulators. Janaya also led numerous staff training sessions while at the SEC and BISYS.

Janaya received her Chartered Financial Analyst (“CFA”) designation 1999 and she earned a B.A. in Economics and Spanish from Rutgers University in 1995.

**Suzan Rose, *Chief Compliance Officer, Marshall Wace North America L.P.***

Ms. Rose joined Marshall Wace North America L.P. in October 2004 as Chief Compliance Officer; she was part of the core team that built and launched the business. She is responsible for ensuring that the firm's activities satisfy all regulatory and legal requirements in the US and abroad. As part of a global team, Ms. Rose also works on behalf of the firm’s affiliated investment advisers in London and Hong Kong to fulfill their respective US requirements.

During nearly 25 years in the investment industry, Ms. Rose previously held a variety of senior compliance and management roles in the equity and fixed income areas of several prominent financial firms, such as Goldman Sachs, Credit Suisse, Citigroup, and Lehman Brothers.

Ms. Rose has a B.A. in Communications from Hofstra University, is an active member of a number of industry groups, and lectures in the industry on regulatory topics. She also is a member of the advisory board of Pencils of Promise and the US board of ARK.

### Edward M. Stroz, *Co- President, Stroz Friedberg*

Ed Stroz is the founder and Co-President of Stroz Friedberg, an Aon company and global leader in investigations, intelligence and risk management. Ed oversees the firm's growth and client development, while ensuring the maintenance of its distinctive culture. He also provides hands on strategic consulting in investigations, intelligence and due diligence, plus cyber and physical security. Before starting the firm, Ed was a Special Agent with the FBI where he formed their computer crime squad in New York.

Trained as a Certified Public Accountant, Ed has extensive experience in investigations of white-collar crime including bank fraud and securities fraud, and has testified in court numerous times as an expert witness.

Ed is a trustee of Fordham University, his alma mater, and serves as an advisor to the Center on Law and Information Policy (CLIP) at Fordham Law School. Ed sits on the Board of Directors of the Crime Commission of New York City, an independent non-profit organization focused on criminal justice and public safety policies and practices, and is a member of the Association of Former Intelligence Officers (AFIO). He served on the New York State Courts System E-Discovery Working Group, established to provide ongoing support and expertise to the New York State Judiciary in the area of e-discovery.

As a member of the National Association of Corporate Directors (NACD), in 2017 he earned the CERT Certificate in Cybersecurity Oversight from Carnegie Mellon University.

### Tom Weston, Partner, Hakluyt

Tom heads Hakluyt Cyber in North America. Tom joined Hakluyt and Company's strategy consulting practice in London in 2009, spent 2012-15 running Pelorus Research, our group's tailored service for public market investors, and subsequently joined our Cyber practice. Before Hakluyt, Tom spent nine years at McKinsey & Company. He was variously based in London, Hong Kong and South Africa, and served both public and private sector clients across a broad range of industries. He is a graduate of the University of Oxford, and has an MBA from Stanford University.