Westlaw Journal
SECURITIES LITIGATION & REGULATION
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 21, ISSUE 3 / JUNE 11, 2015

EXPERT ANALYSIS

SEC Cybersecurity Investigations: A How-to Guide

By Lisa J. Sotto, Esq., Scott H. Kimpel, Esq., and Matthew P. Bosher, Esq.
Hunton & Williams

With cybersecurity events now considered inevitable, businesses must navigate an increasingly crowded thicket of interested regulators at both the state and federal level.

For many companies subject to the U.S. Securities and Exchange Commission's jurisdiction, it is increasingly clear that the threat of an SEC enforcement investigation must be considered an integral part of cybersecurity planning and compliance efforts.

Being prepared to engage the SEC in a proactive manner is often the best approach.

THE SEC'S ROLE IN CYBERSECURITY REGULATION

The SEC is the nation's primary federal regulator of the U.S. capital markets, securities brokers and other capital market intermediaries, investment managers and funds, and publicly traded companies.

Its stated mission is to protect investors; maintain fair, orderly and efficient markets; and facilitate capital formation.

Against this backdrop, the SEC's regulatory efforts concerning cybersecurity have, so far, focused mainly on maintaining the integrity of the capital markets against malicious intrusions, protecting investor data, and requiring public companies to disclose material information concerning cyberrisks and data breaches.

The agency has not adopted a single, consolidated set of cybersecurity rules applicable to all entities under its jurisdiction. Instead, it has approached cybersecurity in a piecemeal, division-by-division fashion.

For example, the agency's Division of Corporation Finance, which oversees public company disclosure, issued "disclosure guidance" concerning public companies' disclosure obligations related to cybersecurity risks and cyber incidents.[1]

The Division of Investment Management, which regulates the conduct of investment advisers and registered investment companies (including mutual funds), also issued its own cybersecurity guidance. It laid out broad criteria for these firms as they assess risks; design systems to prevent, detect and respond to risks; and implement appropriate policies and procedures to train employees for their compliance strategy.[2]

Not to be outdone, the SEC Office of Compliance Inspections and Examinations issued its own pronouncements on the topic of cybersecurity, many of which overlap with the other divisions' releases.[3]

OCIE is responsible for examining regulated entities such as investment advisers, broker-dealers, transfer agents, clearing agencies, stock exchanges and self-regulatory organizations.

Though not technically part of the SEC, the Financial Industry Regulatory Authority is a self-regulatory organization that shares jurisdiction with the SEC over registered broker-dealers and has released still more cybersecurity guidance of its own.[4]

Other SEC rules of broader application, such as those governing the disclosure of material events, consumer privacy, computer system integrity and internal controls over financial reporting, also may be called into play in the case of a data breach or cybersecurity incident.[5]

OCIE examinations typically conclude with a letter outlining alleged deficiencies and potential opportunities for improvement on the part of the examined entity, but OCIE has no independent authority to initiate actual enforcement proceedings against a registrant.

While FINRA has limited authority to pursue administrative enforcement actions against registered broker-dealers and their employees, both FINRA and OCIE regularly make enforcement referrals to the SEC's Division of Enforcement.

SEC ENFORCEMENT

The SEC has not adopted a single, consolidated set of cybersecurity rules applicable to all entities under its jurisdiction.

The SEC's Division of Enforcement has broad authority to investigate and pursue fraud charges against any person engaged in a device, scheme or artifice to defraud in connection with the offer, purchase or sale of any security. It is also charged with policing alleged violations of the myriad SEC statutes, rules and regulations.

The division pursues investigations based on its own proprietary surveillance of the markets, acts on referrals from other divisions and offices within the SEC, or follows leads generated by other regulators, whistleblowers and the public.

The SEC has historically taken the position that the standard for commencing an inquiry into a potential enforcement matter is the very low threshold of "official curiosity."[6]

Both the Division of Enforcement and FINRA are not hesitant to pursue enforcement actions against regulated financial institutions for cybersecurity-related violations.[7] Some of these cases have involved the simple failure to establish appropriate policies and procedures without any actual data breach.[8]

The SEC has not yet initiated a cybersecurity enforcement action against a public company outside the world of regulated financial institutions, but the Division of Enforcement appears to be exploring several such cases.

The SEC staff seems increasingly concerned that public company disclosures to investors concerning cyberincidents are not as timely or robust as disclosures made in other contexts, such as statements to news media, statements to other regulators and non-SEC disclosure documents.

Market practice is quickly evolving in this respect. With these developments in mind, it is only a matter of time before the SEC brings a "message case" for disclosure violations by a well-known public company that suffered a data breach.

The director of the SEC's Chicago regional office told attendees at the annual SEC Speaks conference in February that cybersecurity "is an area where we have not brought a significant number of cases yet, but is high on our radar screen."[9]

SEC Chair Mary Jo White's vision statement for enforcement underscores the belief that the Enforcement Division will not sit on the sidelines for long.

"One of our goals is to see that the SEC's enforcement program is — and is perceived to be — everywhere, pursuing all types of violations of our federal securities laws, big and small," she said.[10]

© 2015 Thomson Reuters

THE SEC INVESTIGATIVE PROCESS

SEC investigations generally proceed in four phases: informal inquiry, formal investigation, the so-called Wells process and enforcement action.

Informal inquiries typically begin with a letter or call from an SEC enforcement lawyer requesting that the company voluntarily provide documents, data or information. The staff may also ask the company to take steps to preserve all relevant information at this stage.

While the staff generally requests only voluntary cooperation during an informal inquiry, most companies comply with the requests, at least to some extent, with the hope of avoiding a formal investigation.

A formal investigation begins when the SEC or its staff, acting by delegated authority, issues a formal order of investigation. The formal order identifies — at a very high level — the conduct and subjects under investigation, and it authorizes the staff to serve subpoenas and compel sworn testimony, among other activities.[11]

Anyone compelled to provide documents or testimony pursuant to a formal order may review the order and, in some instances, receive a copy.

In the early part of a formal investigation, the staff may focus on documents, including documents subpoenaed from third parties. After the staff digests the documentary record — which often consists of millions of pages and gigabytes of data — the staff will call witnesses to testify.

Testimony, like a deposition in a civil case, is taken under penalty of perjury and transcribed by a court reporter. It is different from a deposition, however, in that, at least in the staff's view, the questions are not limited by concepts like relevance, factual foundations and clarity.

In other words, the staff generally takes the position that they can ask about essentially anything in whatever manner they want.

In addition to collecting documents and taking testimony during the formal investigation phase, the staff may enter into cooperation agreements with some witnesses, work with experts or work with other agencies to develop a case.

It is not unusual for the informal inquiry and formal investigation phases of an SEC investigation to last years.[12]

If the staff believes a securities law violation occurred, it will it typically will provide a "Wells notice" to the alleged violators after its preliminary review of documentary evidence and testimony.[13]

The Wells notice provides a formal indication that the staff is considering recommending that the five SEC commissioners vote to approve the filing of a case. The notice usually includes the staff's view as to why it believes a violation occurred and appropriate remedies.[14]

A Wells notice recipient may provide a Wells response, which the staff and commissioners will review if the staff recommends commencement of an enforcement action.

During this process, Wells recipients have the opportunity to access some of the staff's investigative files, and the staff generally is willing to meet with Wells recipients to discuss the merits of the matter.

In some cases, Wells recipients convinced the staff or even the SEC to drop the matter without enforcement action. The vast majority of cases involving a Wells notice, however, result in a settled enforcement action or litigation.

The final stage of an SEC investigation is an enforcement action. The SEC files cases in federal district court or administratively before an in-house administrative law judge.

The agency can seek a broad array of remedies, including injunctive relief; civil monetary penalties; disgorgement of ill-gotten gains; and bars from participating in the securities industry, serving as an officer or a director of a public company, and appearing before the SEC as an accountant or attorney.

The SEC has not yet initiated a cybersecurity enforcement action against a public company outside the world of regulated financial institutions, but the Division of Enforcement appears to be exploring several such cases.

© 2015 Thomson Reuters

Anyone compelled to provide documents or testimony pursuant to a formal order may review the order and, in some instances, receive a copy.

ENGAGING SEC STAFF

In many contexts outside of data breach, whether to self-report a potential violation of the federal securities laws to the SEC can be the subject of considerable debate.

Indeed, the SEC encourages voluntary self-reporting of violations and may give favorable cooperation credit to corporate defendants that elect to self-report.[15]

A significant difference between a matter involving cybersecurity compliance and other areas of the federal securities laws, however, is that a company responding to a significant data breach may have separate legal obligations to notify affected individuals or other regulators.

At that point, there may no longer be any advantage to keeping the SEC in the dark, particularly when a company intends to contact law enforcement or other regulatory agencies.

Companies that reach out to the SEC frequently find the staff on a steep learning curve in matters concerning cybersecurity. A company can therefore use this opportunity to describe the nature of the breach, share any preliminary assessments as to its cause and scope, and frame possible legal issues with the SEC staff.

That dialogue also often includes:

- Insights from the staff regarding the staff's potential areas of interest.
- Opportunities for counsel to correct the factual record if there are any basic misunderstandings.
- A discussion on the scope of the company's obligation to preserve documents and data.
- A discussion of the company's proposed and ongoing remedial efforts.

If the staff desires to review documents or interview witnesses, counsel also may propose a timeline for producing that evidence.

Opening up an early dialogue with the staff may help avoid a more comprehensive SEC investigation and, at the very least, enable a company to gauge the size of a potential problem.

The staff also may view a company's proactive efforts as good corporate citizenry.

OTHER TIPS

The prospect of an informal or a formal investigation remains even if a company self-reports a cybersecurity event to the SEC.

Although no two SEC investigations are alike, companies should consider the following steps when facing an investigation:

- Upon receipt of an informal inquiry or subpoena, react swiftly. The staff will attach significance to the timing and attentiveness of a company's response, and that response likely will color the staff's view of the substance of the investigation — particularly if the company previously has not self-reported.
- Take reasonable steps to preserve documents and information after hearing from the staff. The surest way to make an SEC investigation worse than it needs to be is by failing to preserve documents or information the staff may deem relevant to the investigation.
- Request access to and a copy of any subpoena or formal order.
- Consider whether to disclose the investigation to investors. There is no standard answer to whether or when an investigation must be disclosed publicly to investors pursuant to the federal securities laws, but thoughtfully consider the question in light of the facts and circumstances of their specific matter.

© 2015 Thomson Reuters

- Remain mindful of the attorney-client privilege and, in almost all cases, protect it. The SEC generally does not ask companies to waive the privilege, and companies should be careful to not do so inadvertently when providing documents and information.

- Ask to see the staff's investigative file when there is a Wells notice. While the staff's response to such a request is case-by-case, in some instances, the staff will allow companies' counsel to review key nonprivileged documents and even testimony provided by other parties. The staff's reaction to a request for access to records will depend on many factors, but it will likely help if counsel and the staff maintained a constructive dialogue during the investigation.

- During the Wells process, request to meet with enforcement staff senior leadership, meaning those senior to the staff running the investigation day-to-day. In those meetings, draw out the senior staff on theories of potential liability and make their best case for why an investigation should be dropped without enforcement action.

If a member of the Enforcement Division's trial unit is assigned to a case, outreach to the trial lawyer (which is almost always a different person than the attorney investigating the case) also can be productive.

CONCLUSION

The SEC is rapidly expanding its oversight of cybersecurity matters and actively enforcing the federal securities laws in connection with these issues.

Enforcement may address more than the data breach itself. It also could cover the more basic failure to establish and implement an appropriate information security program.

In light of today's perilous environment and the likelihood of a significant cybersecurity event occurring, companies subject to the SEC's jurisdiction should be sure to include the prospect of interacting with that agency as part of any cybersecurity incident response plan. 1

NOTES

[1] Sec. & Exch. Comm'n, Div. of Corp. Finance, Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011), *available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[2] Sec. & Exch. Comm'n, Div. of Inv. Mgmt., IM Guidance Update: Cybersecurity Guidance (April 2015), *available at* http://www.sec.gov/investment/im-guidance-2015-02.pdf.

[3] *See, e.g.*, Sec. & Exch. Comm'n, Office of Compliance Inspections and Examinations, *National Exam Program Risk Alert: OCIE Cybersecurity Initiative* (Apr. 15, 2014), *available at* http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf; Sec. & Exch. Comm'n, Office of Compliance Inspections and Examinations, National Exam Program Examination Priorities for 2015 (Jan. 13, 2015), *available at* http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2015.pdf; Sec. & Exch. Comm'n, Office of Compliance Inspections and Examinations, National Exam Program Risk Alert: Cybersecurity Examination Sweep Summary (Feb. 3, 2015), *available at* http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

[4] *See, e.g.*, Fin. Indus. Regulatory Auth., Report on Cybersecurity Practices (February 2015), *available at* https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

[5] *See, e.g.*, Regulation S-ID, 17 CFR Part 248, Subpart C (identity theft); Regulation S-P, 17 CFR Part 248, Subpart A (privacy of consumer information); Regulation SCI, 17 CFR § 242.1000 (systems compliance and integrity).

[6] *See United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950).

[7] *See, e.g.*, LPL Financial Corp. Release 34-58515, Admin. Proc. File No 3-13181 (Sept. 11, 2008) (registered broker-dealer, investment adviser and transfer agent firm violated the Gramm-Leach-Bliley Act's Safeguards Rule in failing to implement adequate controls and information security measures that facilitated the compromise of customer accounts); Commonwealth Equity Services LLP, Release 34-60733, Admin. Proc. File No 3-13631 (Sept. 29, 2009) (registered broker-dealer and investment adviser violated GLB's Safeguards Rule in failing to implement adequate data security measures that facilitated the compromise of customer accounts); D.A. Davidson & Co., FINRA Letter of Acceptance, Waiver and Consent No. 2008015299801 (Apr. 9, 2010) (broker-dealer's failure to implement adequate information security controls facilitated the compromise of customer accounts).

© 2015 Thomson Reuters

[8] *See, e.g.*, Marc A. Ellis, Release 34-64220, Admin. Proc. File No 3-14328 (Apr. 7, 2011) (chief compliance officer of registered broker-dealer aided and abetted violation of GLB's Safeguards Rule by failing to revise or supplement policies and procedures for protecting customer information after theft of laptops and passwords); Tradewire Securities LLC, FINRA Letter of Acceptance, Waiver and Consent No. 2009015980301 (Dec. 14, 2012) (involving broker-dealer's failure to enforce written supervisory procedures, including procedures requiring reviews of internal computer systems and privacy protections).

[9] Sarah Lynch, *U.S. SEC on the prowl for cyber security cases: official*, Reuters (Feb. 20, 2015), http://www.reuters.com/article/2015/02/20/us-sec-cyber-idUSKBN0LO28H20150220.

[10] Mary Jo White, Chair, Sec. & Exch. Comm'n, *Remarks at the Securities Enforcement Forum* (Oct. 9, 2013), *available at* http://www.sec.gov/News/Speech/Detail/Speech/1370539872100.

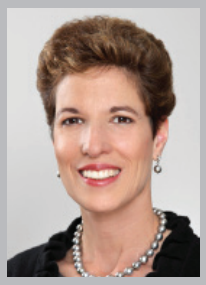
[11] Since 2009, enforcement attorneys can obtain subpoenas through an expedited internal process that no longer requires approval of any of the five SEC commissioners. SEC Release 34-60448, Delegation of Authority to Director of Division of Enforcement (Aug. 5, 2009).

[12] Some SEC investigations bypass the formal investigation stage and proceed directly from informal inquiry to litigation. On the other hand, many investigations that reach the formal stage never result in litigation.

[13] A "Wells notice" is a communication from the staff to the target of an investigation that informs the subject the staff is considering recommending that the SEC file an action or institute a proceeding against it, identifies the securities law violations that the staff has preliminarily determined to include in the recommendation; and provides notice that the subject may make a submission to the SEC in defense of the proposed recommendation. It takes its name from recommendations submitted by the SEC's 1972 Advisory Committee on Enforcement Policies and Practices, which is better known as the Wells Committee after its chairman, John A. Wells.

[14] Under the SEC's internal protocols, a majority of the five commissioners must vote to approve any litigation. Thus, the final decision as to whether to bring a case rests with the commissioners, not the attorneys investigating a case or senior leadership in the Enforcement Division.

[15] *See, e.g.*, Sec. & Exch. Comm'n, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions, Release No. 34-44969 (Oct. 23, 2001), *available at* http://www.sec.gov/litigation/investreport/34-44969.htm.



Lisa J. Sotto (L) is a partner and chair of the global privacy and cybersecurity practice at **Hunton & Williams** in New York. She assists clients in identifying, evaluating and managing risks associated with privacy and information security issues. **Scott H. Kimpel** (C) is a partner in the firm's corporate finance and board advisory practice in Washington, and he previously served on the executive staff of the Securities and Exchange Commission. He regularly represents clients on matters involving complex compliance issues arising under the federal securities laws. **Matthew P. Bosher** (R) is a partner in the firm's corporate and securities litigation practice and regularly advises companies in SEC investigations. He also defends companies, executives and accountants in disputes related to financial reporting and corporate governance. He works out of the firm's Richmond, Va., and Washington offices.

©2015 Thomson Reuters. This publication was created to provide you with accurate and authoritative information concerning the subject matter covered, however it may not necessarily have been prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional. For subscription information, please visit www.West.Thomson.com.

© 2015 Thomson Reuters