The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 1, Number 1 April 8, 2015

SEC ENFORCEMENT

The SEC's Two Primary Theories in Cybersecurity Enforcement Actions

By Daniel F. Schubert, Jonathan G. Cedarbaum and Leah Schloss
WilmerHale

Cyber attacks are increasingly common and affect all sectors of the economy, from retail and financial services, to health care and education. The types of attackers and their goals are just as varied as the targets, with criminals, foreign governments and so-called "hacktivists" attacking companies to steal money or personal information, engage in corporate espionage and tarnish reputations.

When a data security incident has been identified, a company's initial priorities include understanding, containing and remedying the vulnerabilities. In the aftermath of a data security incident, however, companies often have to focus nearly as quickly on responding to inquiries from an expanding array of federal, state, and local regulators and law enforcement agencies. State attorneys general have been active in this field for some time, bringing enforcement actions under various state consumer protection, data security and privacy laws. At the federal level, the Federal Trade Commission (FTC) has pursued more than 50 data security investigations over the last decade and a half, relying on the prohibition on unfair and deceptive trade practices in Section 5 of the FTC Act.

The Securities and Exchange Commission (SEC) is a more recent entrant into the cybersecurity enforcement arena. It has dramatically increased its focus on these issues in the last four years, and it has signaled an intent to continue to expand its efforts. This is true not only for financial institutions subject to extensive SEC oversight—such as broker-dealers and investment advisers—but for all publicly-traded companies.

The SEC's Initial Involvement: Encouraging Disclosures

The SEC visibly entered the cybersecurity arena in 2011, initially in a non-enforcement context. Responding to concerns that public companies may not have been providing adequate disclosures about cyber incidents, the SEC's Division of Corporation Finance issued guidance in October 2011 about when disclosure could be required, both in the wake of a cybersecurity event and in general risk factor disclosures in securities filings.

While the guidance was issued, at least in part, in response to the urging of Senator Rockefeller (D-WV),[1] the Division of Corporation Finance quickly made clear that it would take the issue of cybersecurity disclosures seriously. In the first year and half after the guidance was issued, the SEC sent comment letters to approximately 50 public companies, requesting information about cyber incidents and information security.[2] These comment letters effectively required companies to commit to disclosing the fact of past incidents, though disclosure of particular details and circumstances may not be required. In the wake of the SEC guidance and these comment letters, companies are increasingly including general discussions of cybersecurity risks in their corporate risk disclosures.

From Comment Letters to Enforcement

The SEC has quickly moved from comment letters to enforcement investigations and currently has multiple active enforcement investigations involving data breach events. The SEC's New York Regional Office has been

particularly active in this space, although other offices are also getting involved and have active enforcement investigations. In late February 2015 at the annual "SEC Speaks" conference, for example, David Glockner, the Director of the SEC's Chicago Regional Office, said that cybersecurity is "high on [the SEC's] radar."[3]

Glockner's comment is just the latest in a series of statements by high-ranking SEC officials signaling the SEC's increased focus on cybersecurity enforcement. SEC Chair Mary Jo White emphasized the importance of responding to threats posed by cybersecurity in the securities sector at a March 2014 Cybersecurity Roundtable, and described the SEC's role with regard to cybersecurity as focusing on disclosure of material information, and the protection of market-related systems, investors, and customer data.

Commissioner Luis Aguilar made similar remarks during a June 2014 conference hosted by the New York Stock Exchange, expressing concern over the severe impact that the increasing frequency and cost of cyber attacks could have on the integrity of the capital markets, on public companies, and on investors.

Although there have not yet been any publicly-resolved matters, consistent with these remarks, recent SEC cyber-related enforcement actions appear to rely on two main theories: (1) disclosures and (2) controls.

Enforcement Theory #1: Disclosures

The SEC's interest in cyber-related disclosures falls broadly into two categories.

Disclosures Following an Incident

First, the SEC is actively examining corporate disclosures made in the wake of a cyber attack. The SEC is looking to understand how the issuer evaluated whether the incident was or should have been considered material and whether any disclosures that were made about the incident were timely, complete and accurate. A related theory, also within the scope of the SEC's authority, rests on Regulation FD, which, broadly speaking, prohibits issuers from selectively disclosing material non-public information to third parties, and instead generally requires simultaneous disclosure to the market at large.[4]

Ongoing Disclosures

Second, the SEC has expressed interest in whether issuers' risk factor disclosures, located in their regular filings, contain sufficiently robust disclosures around the cyber risks facing the issuer. Among other things, the SEC is interested in whether the issuer has been subjected to prior cyber attacks, the detail and completeness of its disclosures in relation to those attacks and whether they accurately reflect the nature and severity of the cyber risks facing the issuer.

Although, as noted, there have not yet been any publicly-resolved matters, these disclosure themes can be seen in the SEC's 2011 cybersecurity disclosure guidance itself, which noted (among other things) that:

> Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents. . . .
>
> In addition, material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading.

The guidance thus stressed that "registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents." The guidance effectively put reporting companies on notice to pay closer attention to their cybersecurity disclosures, and many companies have, in the years since, revamped their standard risk factor disclosures to include cybersecurity risks.

In light of this guidance and enforcement trends, companies experiencing a cybersecurity incident should carefully review the facts of the incident to

determine whether the event is material such as to require disclosure. Factors to consider in determining whether an incident is material include the magnitude of the incident, the type of data subject to the incident, and the potential impact of the incident on the company's business (including, for example, costs and other consequences arising from contractual obligations, remediation costs, litigation and damage to the company's business opportunities or relationships).

Any statement about an incident must also be accurate. This means that substantive statements about an incident should either be avoided until information has been verified or otherwise appropriately caveated. That said, the significance of a breach should not be downplayed. Past disclosures, including cyber risk factors, should also be reviewed after an incident to determine whether updating is required. For example, the risk factors may discuss the risk of a cyber attack in hypothetical terms (i.e., attacks could happen), whereas post-attack the risk factors may more appropriately discuss such attacks in actual terms (i.e., attacks do happen) or identify the type of event that occurred if it is not covered under the prior disclosures.

Enforcement Theory #2: Controls

The second area of focus for the SEC is cyber-related controls. While, here too, no resolutions have been publicly disclosed, the SEC's interest appears to fall broadly into two categories.

SEC-Registered Financial Institutions

First, SEC-registered entities, such as broker-dealers and investment advisers, are subject to controls-related requirements under Regulation SP.[5] This regulation requires brokers, dealers, and investment companies, as well as registered investment advisers, to adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information.[6] These procedures must be reasonably designed to ensure the security and confidentiality of customer information, protect customer records from anticipated threats or hazards to their security or integrity and protect against unauthorized access to or use of customer records that could result in substantial harm or inconvenience.[7] Consistent with these requirements, the SEC has shown investigative interest in the impact of data breach incidents on customers of regulated entities and likely views this as a key jurisdictional hook for enforcement actions.

In keeping with this interest, on February 3, 2015, the SEC's Office of Compliance, Inspections and Examinations released a Risk Alert summarizing the results of a cybersecurity examination sweep it had conducted since April 2014.[8] The sweep covered more than 100 registered broker-dealers and investment advisers, based on a long questionnaire addressing topics such as risk assessment, corporate governance, intrusion detection, vendor management and funds transfer fraud detection.[9] The questionnaire also asked registered entities for a detailed list of data security incidents they had experienced since 2013, ranging from incidents involving malware and network breaches to hardware/software malfunctions and other security incidents.[10]

Speaking at the February 2015 SIFMA/FISMA Cybersecurity Conference the following day, Vincente Martinez, Chief of the Office of Market Intelligence in the SEC's Division of Enforcement, confirmed that, relying in part on the information in the Risk Alert, the SEC is actively examining both how its existing authorities can be used to bring more enforcement actions when firms fail to provide sufficient protection for the confidentiality and integrity of customer information and how those authorities might be broadened and strengthened. Martinez stressed that the Risk Alert is not intended as a best practices guide, but instead as a resource for the SEC to inform its enforcement efforts and development of policy.

In a related development, the SEC has also recently adopted rules relating to the integrity and resilience of systems supporting securities trading, order routing, market regulation and certain other key market functions operated by or on behalf of certain

securities exchanges, clearing agencies and alternative trading systems. In November 2014, the SEC unanimously approved Regulation Systems Compliance and Integrity, or "Regulation SCI."[11] This new regulation is intended "to strengthen the technology infrastructure of the U.S. securities markets, to improve its resilience, and to enhance the [SEC's] ability to oversee it,"[12] including by addressing the increased potential for technological problems with high-speed, automated trading on national securities exchanges and alternative trading systems.

Regulation SCI places various obligations on covered entities, including requirements to (1) adopt standards that result in the design, development, testing, maintenance, operation and surveillance of covered systems to facilitate the successful collection, processing and dissemination of market data,[13] and (2) monitor relevant systems to identify potential "SCI events,"[14] including "system intrusions" (defined as an "unauthorized entry" into an SCI system).[15] In other words, the regulation places specific obligations to detect, and prevent covered systems from, unauthorized intrusions, such as cyber attacks.

At the recent SIFMA/FISMA Cybersecurity Conference, Martinez pointed to the new Regulation SCI as an example of sources of authorities the SEC may rely upon to exercise a heightened data security enforcement role and suggested that the SEC is considering developing an analogue of the rule for broker-dealers.

Finally, the Dodd-Frank Act transferred some of the FTC's authorities over the "Red Flag" identity-theft rules to the SEC.[16] These rules require covered entities (generally, broker-dealers, investment companies, and investment advisers) to adopt and implement an identity-theft program, designed to identify, detect and respond to signs of identity theft.[17] The SEC could perhaps use this authority as a jurisdictional hook for enforcement following a breach of a covered entity that failed to implement sufficient controls to detect and prevent identity theft.

Thus, at least with respect to SEC-registered financial institutions and other key market players, the SEC has made clear that it is willing to use both its existing regulations and the adoption of new regulations as a basis for cybersecurity enforcement to protect customer data and market integrity.

SEC Reporting Companies Generally

In addition to the IT security practices of SEC-regulated financial institutions and key market players, the SEC has recently begun to explore its authority over the IT controls of publicly-traded companies in two areas.

First, the SEC has expressed enforcement interest in controls around systems that contain financial reporting data. This theory appears to be based on Section 404 of the Sarbanes-Oxley Act of 2002 (SOX) and implementing regulations, which generally require publicly-traded companies to maintain a system of internal control over financial reporting (ICFR).[18] SEC guidance has stated that the "[m]anagement's evaluation of the risk of misstatement should include consideration of the vulnerability of the entity to fraudulent activity (for example, fraudulent financial reporting, misappropriation of assets and corruption), and whether any such exposure could result in a material misstatement of the financial statements."[19]

Placed in the context of a cyber breach, the SEC's theory appears to be that cybersecurity is relevant to ICFR insofar as security breaches could allow an intruder to tamper with the financial statements or underlying financial data or records.[20] That said, the language of SEC rules suggests that safeguarding of assets is relevant to ICFR only to the extent that control failures with respect to safeguarding could have a material impact on financial statements.[21]

Second, the SEC has expressed interest in finding a broader controls-related theory, under which controls around additional systems could potentially be subject to jurisdiction. It is not clear that there is any legal

basis for such a theory, but it would perhaps rest on a combination of the SOX and Foreign Corrupt Practices Act's internal controls provisions.

Another Possible Enforcement Theory?

While disclosures and controls have been the two primary theories that the SEC has been exploring in recent enforcement actions, other theories are likely on the horizon as the SEC continues to seek to broaden its enforcement efforts. For example, a recent report by cybersecurity firm FireEye has highlighted a hacking group targeting information about mergers and acquisitions (and other sensitive non-public information) that could perhaps be used for insider-trading.[22] Pursuant to its authorities to protect market integrity and prevent insider trading, the SEC may try to use the breach of non-public deal information as a jurisdictional hook.

Daniel Schubert is a partner in WilmerHale's Securities and Litigation/Controversy Departments. His practice focuses on securities litigation and enforcement matters, including advising clients on cybersecurity disclosures and investigations.

Jonathan Cedarbaum is a partner in WilmerHale's Government and Regulatory Litigation and Cybersecurity, Privacy, and Communications Groups. He counsels clients and represents them before administrative agencies and congressional committees on a wide array of data security and privacy issues.

Leah Schloss is an associate in WilmerHale's Defense, National Security, and Government Contracts Group. She focuses primarily on advising clients on data security and cybersecurity matters, including data breach preparedness, investigations and response.

[1] See Letter from Senator John D. Rockefeller IV, Chairman, Senate Commerce, Sci., & Transp. Comm., et al. to Mary Schapiro, Chairman, Sec. & Exch. Comm'n (May 11, 2011).
[2] See Letter from Mary Schapiro, Chairman, Sec. & Exch. Comm'n, to Senator John D. Rockefeller IV, Chairman, Senate Commerce, Sci., & Transp. Comm. (May 1, 2013).
[3] Sarah N. Lynch, SEC on the prowl for cyber security cases: official, Reuters (Feb. 20, 2015).
[4] 17 C.F.R. § 243.100. This regulation does not apply to SEC reporting companies that are foreign private issuers (as defined in SEC Rule 405 and under the Securities Act of 1933).
[5] 17 C.F.R. Part 248 Subpart A.
[6] Id. § 248.30(a).
[7] Id.
[8] SEC Office of Compliance Inspections and Examination, National Exam Program Risk Alert: Cybersecurity Examination Sweep Summary, Vol. IV, Iss. 4 (Feb. 3, 2015).
[9] Id.; Office of Compliance Inspections and Examination, National Exam Program Risk Alert: OCIE Cybersecurity Initiative Appendix, Vol. IV, Iss. 2 (Apr. 15, 2014).
[10] Id.
[11] Regulation Systems Compliance and Integrity, 79 Fed. Reg. 72252 (Dec. 5, 2014) (incorporated at 17 C.F.R. § 242.1000 et seq.).
[12] Mary Jo White, Chairman, Sec. & Exch. Comm'n, Statement at Open Meeting on Regulation SCI (Nov. 19, 2014).
[13] 17 C.F.R. § 242.1001(a)(2)(vi).
[14] Id. § 242.1001(a)(2)(vii).
[15] Id. § 242.1000.
[16] 15 U.S.C. § 1681m(e)(1).
[17] Id. §§ 162.30(d)(2), 248.201(d)(2).
[18] 15 U.S.C. § 7262; 17 C.F.R. §§ 240.13a-14, 240.13a-15, 229.308, 229.601(31)(i).
[19] Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934, Release No. 33-8810 at 14 (Jun. 27, 2007).
[20] Auditors are also looking at this issue, such that shortcomings in controls with respect to cybersecurity could result in an auditor finding of a significant deficiency or material control weakness.
[21] 17 C.F.R. § 240.13a-15(f) (defining "internal control over financial reporting" to include "a process . . . to provide reasonable assurance regarding the reliability of financial reporting . . . that (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of issuer's assets that could have a material effect on the financial statements." (emphasis added)).
[22] FireEye, Hacking the Street? FIN4 Likely Playing the Market (2014).