The Investment Lawyer
Covering Legal and Regulatory Issues of Asset Management
VOL. 22, NO. 4 • APRIL 2015

REGULATORY MONITOR

SEC Update

Wilmer Cutler Pickering Hale and Dorr LLP
Washington, DC

—By Jonathan G. Cedarbaum, Yoon-Young Lee, Matthew Chambers, and Benjamin A. Powell

The SEC and FINRA Increase Scrutiny of Regulated Firms' Cybersecurity

Continuing their heightened focus on the information security practices of regulated firms, both the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) released reports on February 3, 2015, summarizing the results of cybersecurity examination sweeps they had conducted since last year.[1] Speaking at the SIFMA/FINRA Cybersecurity Conference the following day in New York, Vincente Martinez, the Chief of the Office of Market Intelligence in the SEC's Enforcement Division confirmed that, relying in part on the information in the reports, 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. FINRA, too, can be expected to increase its scrutiny of firms' data security practices. The sweeps reports offer firms glimpses of the SEC's and FINRA's likely enforcement priorities and confirm that cybersecurity should be a high priority for investment advisers in 2015.

SEC Risk Alert

The SEC's cybersecurity risk alert reports the results of examinations of 57 registered broker-dealers and 49 registered investment advisers undertaken since April 2014. The examinations were based on a long questionnaire addressing topics such as risk assessment, corporate governance, intrusion detection, vendor management, and funds transfer fraud detection.[2] The questionnaire also asked registered entities for a detailed list of data security incidents they had experienced since January 1, 2013, ranging from incidents involving malware and network breaches to hardware/software malfunctions and other security incidents. For each incident, the entity was asked to explain if it reported the incident to law enforcement, the Financial Crimes Enforcement Network (FinCEN) (through the filing of a Suspicious Activity Report), FINRA, a state or federal regulatory agency, or an industry or public-private organization facilitating the exchange of information about cybersecurity incidents and risks.

At the SIFMA/FINRA Cybersecurity Conference, Martinez stressed that the alert is not intended

as a best practices guide, but instead as a resource for the SEC to inform its enforcement efforts and policy development. It therefore may provide some insight into SEC priorities. Martinez identified as particularly notable the variation seen in policies and practices concerning vendor management and other third-party relationships and in fraud avoidance and loss allocation policies with respect to funds transfers. Those areas thus may attract particular attention from the SEC.

In many of the areas scrutinized in the sweep, significantly higher percentages of broker-dealers than investment advisers had desired policies in place. Nearly all the broker-dealers surveyed (93 percent), for example, conduct periodic risk assessments on a firm-wide basis to identify cybersecurity risks, vulnerabilities, and potential business consequences, while only 79 percent of investment-advisers do. A substantial majority of broker-dealers (84 percent) require vendors to undertake such risk assessments, but only 32 percent of advisers do. Similarly, nearly nine in ten (88 percent) of broker-dealers reported relying on external standards, such as the National Institute of Standards (NIST) Cybersecurity Framework, in developing their information security processes, but only about half (53 percent) of advisers did.[3] Perhaps most striking, 72 percent of broker-dealers incorporate provisions relating to cybersecurity risk into their contracts with vendors and business partners, while only 24 percent of advisers surveyed do the same. Whether these contrasts will lead the SEC to pay particularly close attention to investment advisers' data security practices remains to be seen.

FINRA Report

The FINRA report, unlike the SEC risk alert, not only describes the results of FINRA's 2014-2015 sweep (as well as of a sweep undertaken in 2011), but also offers an array of "principles and effective practices" that provide a guide for regulated firms to use in assessing and improving their own information security activities. Those principles include:

- Governance and risk management: "establish[ing] and implement[ing] a cybersecurity governance framework that supports informed decision making and escalation within the organization to identify and manage cybersecurity risks," including engaging the board and senior management;
- Risk assessment: undertaking regular, enterprise-wide assessments of assets and threats, with an eye toward prioritizing remediation efforts;
- Technical controls, such as identity and access management, encryption, and penetration testing, creating a defense-in-depth strategy:
- Incident response planning: establishing policies and procedures and defining roles and responsibilities for a coordinated, firm-wide response to data security breaches;
- Vendor management: ensuring careful lifecycle scrutiny of vendors' cybersecurity practices;
- Training: carrying out regular training of staff on cybersecurity "hygiene," that is, day-to-day habits that are essential to protecting information systems;
- Cyber intelligence and information-sharing, including participating in information-sharing forums such as the Financial Services Information Sharing and Analysis Center (FS-ISAC); and
- Cybersecurity insurance: evaluating the utility of cyber insurance as a way to transfer some of the risk of cyber incidents.

The report notes that while sophisticated threats are becoming more frequent, "most successful attacks take advantage of fairly basic control weaknesses." It emphasizes that "[w]hat is required is rigorous attention to detail and execution." FINRA, the report explains, "expects that firm management will make cybersecurity a priority" and will "review this report to assess what aspects of the principles and effective practices … could help them build or improve their cybersecurity readiness." The report also holds up the NIST Cybersecurity Framework as an essential guide.

Further Initiatives

These SEC and FINRA reports—and the examination sweeps behind them—are just the latest steps in what will undoubtedly be both bodies' ongoing increased attention to regulated firms' information security practices. At the SIFMA/FINRA Cybersecurity Conference, Martinez echoed statements by SEC Chair Mary Jo White at the SEC's March 2014 cybersecurity roundtable that the SEC views information security as crucial to protecting market-related systems and thus investors. In addition to Regulation S-P and FINRA Rule 2010, he identified several other sources of authorities the SEC and FINRA may rely on in order to exercise a heightened data security enforcement role, including the recently issued Regulation SCI, which he said the SEC is considering developing an analogue of for broker-dealers; Investment Advisers Act Regulation 206(4), and Securities Exchange Act § 15B as a basis for scrutinizing credit rating agencies.[4]

With the increasing importance of and regulatory attention to data security, financial institutions can expect the pace of regulatory—and perhaps even legislative—activity to continue to increase. Regulated firms, for example, also need to ensure that they are complying with their obligation—under the Fair Credit Reporting Act, as amended, and its implementing "red flag" rules and guidelines—to have a board-approved identity theft program in place. The Dodd-Frank Act moved responsibility for enforcement of these obligations for broker-dealers, investment advisers, and investment companies to the SEC, which (in collaboration with the Commodity Futures Trading Commission) promulgated new rules and guidance in 2013.[5]

On February 13, 2015, President Obama convened a White House Cybersecurity Summit at Stanford University. He is pressing for a package of laws designed to encourage cybersecurity information-sharing, to establish a uniform federal standard for data breach notification, and to strengthen law enforcement tools against cyber criminals. In just the last six months he has issued two executive orders addressing aspects of the cybersecurity landscape, and more presidential directives can be expected. President Obama has repeatedly described cyber threats as "one of the most serious economic [and] national security challenges that we face as a nation."[6]

Regulatory attention to data security is increasing almost as rapidly as the threat environment is evolving. Investment advisory firms would be wise to make cybersecurity one of their highest priorities in 2015.

NOTES

1 The SEC report and a related investor bulletin are available at: *http://www.sec.gov/news/pressrelease/2015-20.html#.VOyKBvnF9AA.* The FINRA report is available at: *http://www.finra.org/Newsroom/NewsReleases/2015/P602385*.

2 The questionnaire is available at: *http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf*. Our earlier alert discussing the sweep is available at: *https://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=17179872201*.

3 The NIST Cybersecurity Framework is available at: *http://www.nist.gov/cyberframework/*.

4 Our earlier alert on Regulation SCI can be found at: *https://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=17179875980*.

5 Our earlier alert describing those rules and guidance can be found at: *https://www.wilmerhale.com/uploadedFiles/Shared_Content/Editorial/Publications/WH_Publications/Client_Alert_PDfs/Securities%20Alert_04%2025%2013.pdf*.

6 Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), available at: *http://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit*.