KING & SPALDING

Client Alert

Securities Enforcement and Data, Privacy & Security Practice Groups

February 6, 2015

SEC Releases Results of Financial Industry Examination Sweep Regarding Cybersecurity

The publications highlight the SEC's continuing focus on cybersecurity and data privacy issues.

On February 3, 2015, the U.S. Securities and Exchange Commission ("SEC") staff released two publications: the results of an examination sweep of 57 registered broker-dealers and 49 registered investment advisers, and guidance for investors on how to best protect their online brokerage accounts from fraud. These two publications represent the latest in a string of attempts by the SEC to encourage the companies it regulates to prepare for, defend against, and respond to cyber-attacks. The SEC's focus on cybersecurity likewise occurs within the context of calls for greater regulatory action in both the securities and financial institutions field and across the U.S. economy as a whole.

I. Background: The SEC's Authority to Regulate Cybersecurity

The SEC's authority with respect to cybersecurity and data privacy stems from two sources.

First, the SEC has broad and overarching power to ensure transparency and full disclosure in the securities marketplace, and it has wielded that power to require securities issuers to disclose any cybersecurity-related risks or events that a reasonable investor would consider material to an investment decision. To this end, the SEC issued guidance in 2011 to help issuers determine whether they needed to disclose certain cyber-vulnerabilities, past cyber-attacks, and other cybersecurity matters (available here).[1] Companies typically fulfill their duties to disclose cyber-deficiencies by, when necessary, including cybersecurity-related risk factors in their public filings or by describing in their public filings cybersecurity breaches that result in material costs or consequences to the company.

Second, and more specifically relevant to financial institutions, Rule 30 of Regulation S-P requires registered brokers, dealers, investment companies, and investment advisors to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."[2] These policies and procedures must be designed to: "(1) Insure the security and confidentiality of customer

For more information, contact:

Dixie L. Johnson
+1 202 626 8984
djohnson@kslaw.com

Gary G. Grindler
+1 202 626 5509
ggrindler@kslaw.com

J. C. Boggs
+1 202 626 2383
jboggs@kslaw.com

Christopher C. Burris
+1 404 572 4708
cburris@kslaw.com

Matthew H. Baughman
+1 404 572 4751
mbaughman@kslaw.com

Alex K. Haas
+1 202 626 5502
ahaas@kslaw.com

James L. Michaels
+1 404 572 2809
jmichaels@kslaw.com

King & Spalding
Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

www.kslaw.com

records and information; (2) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."[3] The duties mandated by Rule 30 include the duty to safeguard all digital customer information. The SEC—as well as the Financial Industry Regulatory Authority ("FINRA")—has brought enforcement actions to address and correct cybersecurity deficiencies at financial institutions.

II. The SEC's Recent Actions - The Cybersecurity Examination Sweep Summary

The SEC's *Cybersecurity Examination Sweep Summary* (available here) paints a sobering picture of the current state of cybersecurity compliance at American financial institutions and also provides guidance as to areas that the SEC may consider when contemplating enforcement actions.[4]

In April 2014, the SEC's Office of Compliance Inspections and Examinations ("OCIE") announced that it would conduct cybersecurity preparedness examinations of dozens of registered broker-dealers and investment advisors (a discussion of the announcement from April 2014 and a sample list of examination questions is here). Over the past year, OCIE examined 57 broker-dealers and 49 investment advisors with the stated aim of "better understand[ing] how broker-dealers and investment advisors address the legal, regulatory, and compliance issues associated with cybersecurity."[5] In the course of its inspections, OCIE gathered data relating to many facets of cybersecurity, from firms' abilities to identify cybersecurity risks and to create policies and procedures to address those risks, to the more concrete areas of steps taken to protect firms' computer networks and efforts to deal with cyber risks related to clients and vendors. The areas upon which OCIE focused, and the related commentary, shed light upon the cybersecurity measures that the SEC deems most important. Some of the highlights (and lowlights) of the OCIE survey are discussed below.

A. Sweep Summary Results - The Good

The examinations revealed that nearly all of the inspected financial institutions have taken steps to mitigate their risks from cyber-attacks. The vast majority of both broker-dealers (93%) and investment advisors (83%) have written information security policies, and conduct periodic risk assessments on a firm-wide basis to identify cybersecurity threats and vulnerabilities (93% for broker-dealers, 79% for investment advisors). Most examined firms also make use of encryption in some form.

A majority of firms (88% of broker-dealers, 53% of investment advisors) model their information security procedures on published, third-party standards, such as the 2014 cybersecurity framework published by the National Institute for Standards and Technology ("NIST"). Many broker-dealers (47%) reported that they were members of industry groups focused on sharing information regarding cybersecurity and identifying controls to mitigate harm from cyber-attacks. One industry group, the Financial Services Information Sharing and Analysis Center ("FS-ISAC") was highlighted as being particularly useful.

Finally, the majority of firms that allow clients online access to their accounts also provide their clients with information about steps they can take to reduce cybersecurity risks.

B. Sweep Summary Results - The Bad

Although a number of firms have made efforts to improve their cyber resilience, many of those same firms expose themselves to vulnerabilities by doing business with other companies that do not maintain effective cybersecurity procedures. While 84% of broker-dealers require cybersecurity risk assessments of vendors that have access to the firms' networks, only 32% of investment advisers conduct the same assessments of vendors. Furthermore, while 72% of broker-dealers incorporate cybersecurity requirements into contracts with vendors and partners, only 24% of investment advisors do, and although 54% of broker-dealers provide security training to vendors and partners, only 13% of advisors do. The recent Target data breach—which reports indicate was caused by a cybersecurity lapse by a Target vendor who had access to Target's network for billing and project management purposes[6]—illustrates the need to ensure that others with access to a company's network must have effective cybersecurity programs. The cybersecurity chain is only as strong as its weakest link and all companies, including those in the financial services industry, must examine their supply chain, vendors, and network partners to ensure that they are not exposing themselves to weaknesses through their relationships with other companies.

C. Sweep Summary Results - The Ugly

Considering the risk climate in which financial institutions operate, it is unsurprising that the vast majority of examined firms (88% of broker-dealers and 74% of advisors) have been the subject of some form of cyber-related incident. These incidents include the receipt of fraudulent emails asking for client funds to be transferred (of which 54% of broker-dealers and 43% investment advisors report receiving), employees failing to abide by their firms' identity authentication procedures (25% of broker-dealers reported this issue), and even employees or other authorized users misappropriating funds, securities, or sensitive information (11% of broker-dealers and 4% of investment advisors faced this problem). When problems arise and client money is lost, most firms (70% of broker-dealers and 87% of advisors) do not have written policies addressing how to determine whether the firm or the customer is responsible; even fewer firms (only 15% of broker-dealers and 9% of advisors) offer guarantees against cyber-related losses.

D. Sweep Summary Results - Conclusion

The OCIE examination results show that many financial institutions have taken substantial steps toward mitigating risks from cyber-attacks, but that there are still important areas, like vendor compliance, where firms could strengthen their cybersecurity efforts. While the OCIE report did not expressly state that deficiencies in any of the examined areas would lead it to refer a matter to the SEC's Division of Enforcement, the fact that OCIE decided to zero in on specific cybersecurity issues suggests that it believes those issues represent the most significant, or vulnerable, aspects of financial institution cybersecurity. And given the intense focus on cybersecurity issues by a broad spectrum of federal regulators—and the near-weekly data breaches being reported in the news—SEC investigations and enforcement actions remain a potential risk.

In that vein, OCIE's examination report suggests that the SEC staff is focusing on the areas identified by NIST in its *Framework for Improving Critical Infrastructure Cybersecurity* (available here) as important when considering recommended or required cybersecurity measures for financial institutions (the SEC staff's reliance on NIST was expressly apparent in the sample list of questions that accompanied the April 2014 announcement that OCIE would be conducting the examinations, where OCIE stated that some of its questions would be based on the NIST framework).

The NIST Framework is intended to enable organizations "to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure [such as cybersecurity infrastructure]" and provides, in its *Framework Core*, five key functions or activities that organizations should look to when assessing cybersecurity procedures: Identify, Protect, Detect, Respond, and Recover. OCIE's areas of examination focused on the first three functions, which can be considered the prophylactic aspects of the NIST framework.

III. The SEC's Recent Actions - Investor Bulletin: Protecting Your Online Brokerage Accounts from Fraud

The SEC staff also provided guidance to investors (available here) which gives steps that investors can take to avoid cybersecurity risks. These steps are, for the most part, in accordance with current best practices in consumer-level cybersecurity. The staff recommended, among other things, that investors: use "strong" passwords, which are passwords that are "not easy to guess," use eight or more characters, and include symbols, numbers, and both capital and lowercase letters; use two-step verification systems, which usually send a unique code to the investor's phone or email account when he or she attempts to log in; use different passwords for different online accounts; avoid accessing accounts on public computers; and exercise caution with wireless connections and mobile devices.

IV. The SEC's Focus on Cybersecurity Continues the General Trend Toward More Regulation of Cybersecurity In The Financial Industry And Elsewhere

As cyber-attacks become more sophisticated and pervasive, there has been an increased focus on these issues, both by regulatory and oversight authorities as well as within the regulated industries themselves. This trend within the financial industry mirrors what has been occurring throughout the U.S. economy.

The recent publications are not the SEC's first foray into cybersecurity regulation of financial institutions. As mentioned above, the SEC guidance regarding disclosure applies to financial institutions (as well as all publicly traded companies). Furthermore, at a roundtable event in March 2014 (available here), Commissioner Luis Aguilar noted that the SEC will regulate in the cybersecurity sphere; however, at that point—and continuing to today—the SEC's exact role is far from clear. Industry commenters have urged the SEC to adopt principles-based guidance as opposed to prescriptive regulations which could be rendered ineffective by constantly-evolving cyber-threats.

Following up on the roundtable, the Securities Industry and Financial Markets Association ("SIFMA") urged greater action in this area in October 2014 by releasing a list of ten cybersecurity principles (available here) that it hoped would guide regulators as they craft new cybersecurity principles or rules. The principles are broad and, for the most part, do not provide specific "granular" advice to companies as they grapple with ways to implement cybersecurity measures, but the messages provided by many of the principles—such as "Information Sharing is Foundational to Protection," "Crisis Response is an Essential Component to an Effective Cybersecurity Program," and "The Management of Cybersecurity at Critical Third Parties is Essential for Firms"—are entirely consistent with other cybersecurity frameworks and with the topics discussed in the OCIE examination report.

FINRA has also become more involved in cybersecurity efforts. The same day that the SEC released the OCIE examination results and the investor bulletin, FINRA released two similar—but more detailed—publications. FINRA's *Report on Cybersecurity Practices* (available here) contains the results of its 2014 cybersecurity-focused FINRA survey of members and guidance about how to institute robust cybersecurity programs; FINRA's *Cybersecurity and Your Brokerage Firm* Investor Alert (available here) provides advice to brokerage clients about

how to best ensure that they are not effected by cybersecurity problems. The *Report* contains detailed guidance regarding the overarching principles and specific cybersecurity practices that FINRA believes are necessary for its members to consider and implement. Furthermore, FINRA concluded its report by stating that it expects member firms to consider those principles and practices and to devote sufficient resources to understanding cybersecurity threats. Cybersecurity is by no means a new issue for FINRA: the National Association of Securities Dealers, FINRA's predecessor organization, issued a Notice to Members in 2005 reminding members of their obligations under Regulation S-P while noting "numerous technological advancements and other changes in the workplace [] may raise concerns regarding the safeguarding of customer information."[7]

The importance of cybersecurity in financial institutions has also piqued the attention of the U.S. Senate. In October 2014, former Senate Banking Committee Chairman Tim Johnson (D-SD) and former Ranking Member Mike Crapo (R-ID) sent a letter to a group of financial regulators (available here) noting that the finance industry "probably wins the cybersecurity threat award… because [it is] where the money is." In their letter, the Senators asked the banking and finance regulators for information about how they acquired information about cyber threats, how they coordinated with each other, their roles in monitoring cybersecurity risks, and how they planned to help address cybersecurity gaps.

Even a brief review of the relevant legal news and commentary shows that cybersecurity issues have impacted companies across industries in the U.S. and elsewhere. Just as the SEC and FINRA have been increasing their focus in these areas, so too have other regulators. For example, the Federal Communications Commission recently imposed a ten million dollar fine against two companies because they stored their customers' Social Security numbers, names, addresses, and driver's license information on a publicly accessible database, in violation of the Communications Act's requirement that telecommunications carriers protect their customers' "proprietary information" (see here for more information). The Federal Trade Commission has recently attempted to expand the definition of "unfair and deceptive trade practices" to include companies' failures to implement reasonable data security programs, and is embroiled in litigation with Wyndham Worldwide Corporation over the issue (see here for more information about the FTC's data security measures and the *Wyndham* suit). Even the Food and Drug Administration has become more attuned to this area, recently issuing guidance based on the NIST framework to guide medical device manufacturers (see here for information about the FDA's guidance and here for more information about medical devices and cybersecurity risks).

V. Conclusion

Two key conclusions can be drawn from the SEC's release of the OCIE examination report at a time when cybersecurity breaches and related rulemaking and litigation are on the rise: *first*, the SEC is attempting to highlight aspects of cybersecurity to which the companies it regulates should be especially sensitive; and *second*, many of the examined companies' cybersecurity procedures fall below the standards that the SEC considers ideal. Financial institutions should heed the SEC's implicit advice and draft, revise, and enforce cybersecurity policies and protocols that mitigate the risks discussed by the SEC in the OCIE examination report.

* * *

King & Spalding's strengths in securities enforcement and data privacy and security put it in a unique position to assist financial institutions facing data security issues—especially in crisis situations or when the SEC, CFTC, DOJ,

or other regulators are involved. King & Spalding has significant experience in the assessment, creation, and implementation of corporate compliance and cybersecurity programs across industries and subject areas, and in assessing, auditing, and revising pre-existing cybersecurity measures to ensure that they do not expose our clients to threats due to internal, vendor, or partner vulnerabilities.

King & Spalding's Securities Enforcement and Regulation Practice

King & Spalding represents companies and individuals in all aspects of federal securities law enforcement. Our team of over 60 lawyers appears regularly before the Securities and Exchange Commission, Commodity Futures Trading Commission, Department of Justice, Financial Industry Regulatory Authority, Public Company Accounting Oversight Board, the Financial Conduct Authority, and other federal, state, and international enforcement organizations. We track their priorities and train our teams accordingly.

To meet growing client needs in this area, King & Spalding bolstered its extensive existing SEC enforcement and regulation practice during the first quarter of 2014 and is now a powerhouse in SEC enforcement matters. Our team of former SEC and DOJ officials, former federal and state prosecutors, and experienced SEC enforcement practitioners has handled many of the most challenging securities enforcement matters in recent decades. Often, our matters do not become known to the public because they are resolved without government action against our clients.

We help our clients navigate government investigations and manage crises while minimizing unnecessary distractions on officers and employees, who have other work to do. We also conduct internal investigations and due diligence, and we help our clients strengthen their policies and procedures to minimize the risk of future violations.

King & Spalding's Data, Privacy, and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Data, Privacy & Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 30 Data, Privacy & Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigations, e-discovery / e-disclosure, government investigations, government advocacy, insurance recovery, and public policy.

[1] *CF Disclosure Guidance: Topic No. 2 Cybersecurity*, U.S. Securities and Exchange Commission, Division of Corporation Finance (Oct. 13, 2011), available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
[2] 17 C.F.R. § 248.30.
[3] *Id*.
[4] *Cybersecurity Examination Sweep Summary*, U.S. Securities and Exchange Commission, NATIONAL EXAM PROGRAM RISK ALERT, Vol. 4, Issue 4 (Feb. 2, 2015), available at http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.
[5] *Id*.
[6] *Target Hackers Broke in Via HVAC Company*, KREBS ON SECURITY (Feb. 5, 2014), available at http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.
[7] *Safeguarding Confidential Customer Information*, National Association of Securities Dealers, Notice to Members 05-49 (July 2005), available at http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p014772.pdf.