June 24, 2015

Cyber-Attacks: Threats, Regulatory Reaction and Practical Proactive Measures to Help Avoid Risks

I. Cybersecurity; Its Importance and Relevance – How We Got to Where We Are Today

In the past few months, the White House, Home Depot, JP Morgan, Hard Rock Hotels, Tesla, the St. Louis Federal Reserve, the Internal Revenue Service and many other institutions have suffered well-publicized cybersecurity breaches.[1] In fact, very recently the Office of Personnel Management — the agency that manages background checks, pension payments and job training for the federal government — announced that it suffered a cyber-attack in which it believes that hackers stole the personal information of more than 4 million federal employees.[2] In a recent survey of more than 800 information technology (IT) security professionals across 19 industries in seven countries, more than half of the respondents said they will "likely" be victim to a successful cyber-attack this year, and almost three quarters of the respondents disclosed that they fell victim to successful cyber-attacks in the prior year.[3] In fact, the Depository Trust and Clearing Corporation recently disclosed in its 2015 *Systemic Risk Barometer Study* that almost half of the respondents listed cybersecurity as their top concern, and more than three quarters listed it among their top five overall concerns.[4]

As a result, it is often said that there are only two types of financial services firms: those that have experienced cybersecurity breaches and addressed them, and those that have experienced cybersecurity breaches and are unaware.[5]

Cybersecurity is multifaceted, and what it entails differs for every financial services firm. The risks of a cybersecurity breach, in addition to significant reputational harm, include loss of proprietary and confidential customer data, trade secrets and employee information; the resulting costs of mitigation (voluntary and as mandated by law); impairment of operations;

---

1 *See* http://thehill.com/policy/cybersecurity/238127-white-house-state-dept-cyberattacks-linked, http://money.cnn.com/2014/09/08/technology/security/home-depot-breach/, http://www.cnbc.com/id/102644470, http://www.bloomberg.com/news/articles/2015-04-25/tesla-hacked-on-twitter-media-relations-e-mail-accounts, http://http://www.nytimes.com/2015/05/20/technology/st-louis-fed-confirms-hacking-attack.html, *see also* infra note 17. Most recently, a popular online dating service has sustained a highly publicized cybersecurity breach, causing an embarrassing disclosure of patrons' sexual proclivities. *See* http://money.cnn.com/2015/05/22/technology/adult-friendfinder-hacked/index.html.

2 *See* http://www.politico.com/story/2015/06/personal-data-of-4-million-federal-employees-hacked-118655.html.

3 *See* "2015 Cyber Threat Defense Report."

4 *See* the 2015 first quarter "Systemic Risk Barometer Results Overview."

5 *See* remarks of Robert S. Mueller, III, Director Federal Bureau of Investigation at the RSA Cyber Security Conference, San Francisco, CA (March 1, 2012), *see also* Bits Blog, "Hacked vs. Hackers: Game On" (Dec. 2, 2014).

For more information, please contact any of the following members of Katten's **Financial Services, Privacy, Data and Cybersecurity,** or **Litigation and Dispute Resolution** practices.

Alan J. Brudner
+1.212.940.6362
alan.brudner@kattenlaw.com

Wendy E. Cohen
+1.212.940.3846
wendy.cohen@kattenlaw.com

Gary DeWaal
+1.212.940.6558
gary.dewaal@kattenlaw.com

David Y. Dickstein
+1.212.940.8506
david.dickstein@kattenlaw.com

Doron S. Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

Dina Wegh
+1.212.940.6704
dina.wegh@kattenlaw.com

and litigation and regulatory actions. Various financial regulators recently have commenced enforcement actions utilizing tangentially related cybersecurity theories of liability. Analyzing some of these actions can give insight into the types of issues concerning financial regulators today.

This Advisory discusses various financial regulators' public views and initiatives relevant to cybersecurity as well as relevant disciplinary actions, and assimilates this information into a checklist of practical steps firms may take to protect themselves against cyber-attacks, as well as to minimize their potential liability. However, it is important to recognize that different measures are appropriate for each firm.

Actions by Industry Regulators in Recent Years

i. SEC

Rule 30 of Securities and Exchange Commission (SEC) Regulation S-P, known as the "Safeguards Rule," mandates that investment advisers, broker-dealers and investment companies create and maintain reasonably designed written policies and procedures to protect the security and confidentiality of customer records and information.[6] Citing Regulation S-P, the SEC has charged brokerage executives with failing to protect confidential information about their customers. In three separate cases, individuals charged under Regulation S-P settled with the SEC and paid fines between $15,000 and $20,000, as well as consented to orders that required them to cease and desist from committing any violations of the provisions charged.[7] The charges included violations of the law by transferring customers' private data without giving the customers a chance to opt out and ignoring red flags from security breaches at the plaintiffs' respective firms.

In additional actions brought by the SEC under Regulation S-P, the SEC found liability where a broker-dealer's written policies and procedures were too short and vague,[8] and only provided limited guidance rather than a "complete set of . . . policies and procedures addressing administrative, technical and physical safeguards reasonably designed to protect customer records and information."[9] In another action, the SEC held a broker-dealer liable where its policies and procedures did not address what to do in the instance of a breach. In that case, the SEC fined the firm's chief compliance officer individually under a theory that he aided and abetted the violation because he did not remedy the inadequate procedures.[10] While the aforementioned actions were brought against broker-dealers, to the extent that they were enforced under Regulation S-P, they apply equally to investment advisers.[11]

To control for cyber-attacks and breaches at the exchange level, the SEC adopted Regulation System Compliance and Integrity (Regulation SCI) to govern the technology infrastructure of most self-regulatory organizations, certain alternative trading systems, plan processors and certain clearing agencies in the United States (collectively, SCI Entities).[12] In the event of a cyber-attack or other disruption, SCI Entities are required to take corrective action, and notify the SEC and affected members or participants.

---

[6] *See* https://www.sec.gov/rules/final/34-42974.htm.

[7] *See* http://www.sec.gov/news/press/2011/2011-86.htm.

[8] Exchange Act Release No. 58515, Admin. Proc. File No. 3-13181, at 4 (Sept. 11, 2008) (finding that the firm violated Regulation S-P), *available at* http://www.sec.gov/litigation/admin/2008/34-58515.pdf.

[9] Exchange Act Release No. 58515, Admin. Proc. File No. 3-13181, at 4 (Sept. 11, 2008) (finding that the firm violated Regulation S-P), *available at* http://www.sec.gov/litigation/admin/2008/34-58515.pdf.

[10] Exchange Act Release No. 64220, Admin. Proc. File No. 3-14328, at 3 (April 7, 2011) (finding that the firm violated Regulation S-P), *available at* http://www.sec.gov/litigation/admin/2011/34-64220.pdf.

[11] In addition to Regulation S-P, the SEC also could bring actions against investment advisers for having inadequate information securities programs based on other federal securities laws including the following: (1) violations of Rule 204A-1 (the Code of Ethics Rule) under the Investment Advisers Act of 1940, as amended (Advisers Act). *See Investment Adviser Codes of Ethics*, Investment Advisers Act Release No. 2256 (July 2, 2004), where the SEC stated that the Code of Ethics Rule will renew investment advisers' "attention to their fiduciary and other legal obligations, and [increase] their vigilance against inappropriate behavior by employees;" (2) breaches of Regulation S-ID: Identity Theft Red Flags rules, *see Identity Theft Red Flag Rules*, Investment Advisers Act Release No. 3582 (April 10, 2013); (3) breaches of an investment advisers' fiduciary duties. *See Compliance Programs of Investment Companies and Investment Advisers*, Investment Company Act Release No. 26299 (Dec. 17, 2003) at n. 22 where the SEC stated an "adviser's fiduciary obligation to its clients includes obligations to its clients from being placed at risk as a result of the adviser's inability to provide advisory services."

[12] *See* http://www.sec.gov/rules/final/2014/34-73639.pdf.

ii. CFTC and NFA

Similar to Regulation S-P above, all National Futures Association (NFA) Members must comply with federal privacy laws and the Commodity Futures Trading Commission's (CFTC) regulations applying those laws to futures firms.[13] Accordingly, and parallel to the Regulation S-P requirements, NFA Members must have written policies and procedures that describe their protections for customer records and information. The procedures must be reasonably designed to "(1) keep customer records and information secure and confidential, (2) protect against any anticipated hazards to the security or integrity of those records and (3) protect against unauthorized access to or use of the records or information."[14]

In *In Re Interbank FX, LLC*, the CFTC sanctioned Interbank for failing to adopt policies and procedures that address the administrative, technical and physical safeguards for the protection of customer records as required under Regulation 160.30 of Title V of the Gramm-Leach-Bliley Act.[15] The sanctions included a fine of $200,000 and an order that Interbank undertake to implement and maintain a comprehensive security program to address the protection of private customer data.

iii. FINRA

National Association of Securities Dealers (NASD) Rule 3010 requires that each Financial Industry Regulatory Authority- (FINRA) regulated firm create and maintain a system with written policies and procedures to supervise the activities of each registered representative or associated person to ensure compliance with applicable securities laws and regulations. Accordingly, FINRA cites Regulation S-P and NASD Rule 3010 to bring enforcement actions against Member firms. In one instance, a Member firm agreed to pay a $150,000 fine for failing to adequately maintain safeguards to detect and report breaches of private customer information.[16]

In another example, in March 2015, citing NASD Rule 3010, FINRA fined a Member firm, OptionsXpress, $150,000 for permitting an identity thief to illicitly transfer funds.[17] FINRA held OptionsXpress liable because its written supervisory policies and procedures to review transfers of funds from customer accounts to outside bank accounts were deemed inadequate.[18] FINRA charged OptionsXpress for not sufficiently following up on red flags in connection with transactions that appeared on an internal exception report that identified potentially suspicious conduct. As a result of the unauthorized activity, in March and April 2012, the relevant customer sustained losses totaling $443,000 that the firm ultimately reimbursed. Among the ignored red flags, the identity thief, pretending to be the OX customer, (i) contacted the OX customer service center and was not able to correctly answer security questions; (ii) called the OX customer service center using Skype, evidencing a heavy Eastern European accent, and did not appear to understand English, even though the actual customer lived in Illinois; and (iii) repeatedly accessed the customer's account from a Texas IP address (when the customer was living in Illinois) with numerous failed efforts to reset the account security personal identification number.

On May 5, 2015, citing Regulation S-P and NASD Rule 3010, FINRA fined a Member firm $225,000 when one of its employees left his unencrypted work computer in a public restroom and private customer information was placed at risk. The firm's policies and procedures did not provide for the encryption of laptops because firm management believed that, due to the low number of issued work computers, encryption was not necessary.[19]

iv. FTC

Rule 314 of the Federal Trade Commission (FTC) rules (FTC Safeguards Rule) also requires financial institutions to adopt comprehensive information security programs to protect customer information. While Rule 30 of Regulation S-P governs protection

---

[13] *See* infra note 35.

[14] *See* https://www.nfa.futures.org/NFA-compliance/publication-library/regulatory-requirements-guide.pdf.

[15] *In re Interbank FX, LLC*, CFTC Docket No. 09-11 (CFTC filed June 29, 2009).

[16] Letter of Acceptance, Waiver and Consent No. 2010022554701, at 2, 5 (April 9, 2012), *available at* http://disciplinaryactions.finra.org/Search/ViewDocument/31594.

[17] Approximately 100,000 taxpayers recently were subject to a similar identity theft fraud perpetrated by criminals on the US Internal Revenue Service. *See* http://www.nytimes.com/2015/05/28/business/irs-data-breach-may-be-sign-of-more-personalized-schemes.html.

[18] *See* http://disciplinaryactions.finra.org/Search/ViewDocument/38882.

[19] *See* http://disciplinaryactions.finra.org/Search/ViewDocument/51064.

of individual "customer" privacy data, the FTC Safeguards Rule is the federal information security protection regulation that requires private investment fund advisers to adopt procedures to protect the information of private investment fund investors.[20] Private investment funds, but not their underlying investors, are deemed "clients" under the Advisers Act. Since the funds are not individuals, Rule 30 does not apply. Conversely, the FTC Safeguards Rule applies to "customers" of *financial institutions*. The FTC could view the individual investors in such funds as "customers" of the funds. Consequently, the FTC's enforcement of the FTC Safeguards Rule is relevant to private investment fund managers. The FTC has brought numerous cases to enforce the FTC Safeguards Rule, and could try to bring similar actions against private investment funds for information security breaches.[21]

v. State Requirements

In addition to federal law and regulations, to date, 47 states and the District of Columbia, Puerto Rico, Guam and the US Virgin Islands have privacy laws, which require entities to promptly notify individuals whose information was compromised or thought to be compromised, and the majority of them provide a private right of action.[22]

vi. DOJ

In April 2015, the US Department of Justice (DOJ) released a 15-page document titled "Best Practices for Victim Response and Reporting of Cyber Incidents."[23] In addition to practical advice about incident response planning, the DOJ suggests notifying the relevant authorities promptly in the event of a breach because, among other things, the knowledge and experience of agencies such as the DOJ and FBI in dealing with particular types of breaches and particular criminal parties may be valuable in getting more quickly and accurately to the bottom of what happened in a particular instance.

II. Cybersecurity – The Current Regulatory Environment

Background

As a result of the increased volume and scope of cyber-attacks in recent years, various regulators and even the President of the United States,[24] have published cybersecurity "best practices." While the SEC, FINRA, CFTC and NFA have yet to enact specific regulations imposing cybersecurity requirements (other than Regulation SCI in the securities industry), cybersecurity is a growing concern of each of these regulatory bodies and, as elaborated below, more regulatory initiatives likely are forthcoming.[25] Additionally, the National Institute of Standards and Technology (NIST), a non-regulatory agency of the US Department of Commerce with a mission to promote industrial innovation and competitiveness, developed a cybersecurity framework that includes "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[26] The framework, which all firms, including financial services firms, are strongly encouraged to use,[27] provides a structure to create, guide, assess and/or improve comprehensive cybersecurity programs, and is a helpful tool for

---

[20] *See* 16 CFR part 314, *Standards for Safeguarding Customer Information*.

[21] *See* e.g., In the Matter of Nationwide Mortgage Group Inc., (finding that Nationwide Mortgage Group violated the safeguards rule by failing to conduct privacy risk assessments), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2005/04/050415do09319.pdf.

[22] *See* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[23] *See* http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf.

[24] *See* Executive Order 13636.

[25] The NFA is expected to enact requirements regarding cybersecurity for Members by the end of 2015, *see* "Testimony of Daniel J. Roth, President and CEO of the NFA before the Subcommittee on Commodity Exchanges, Energy, and Credit of the Committee on Agriculture of the U.S. House of Representatives." Additionally, the CFTC has incorporated cyber concerns into its regulations and is looking at private companies that run major exchanges and clearinghouses to determine if they are adequately testing their cyber protections, *see* "Testimony of Chairman Timothy G. Massad before the U.S. Senate Committee on Appropriations, Subcommittee on Financial Services and General Government."

[26] *See* "Framework for Improving Critical Infrastructure Cybersecurity."

[27] *See* https://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework, http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf, http://www.natlawreview.com/article/where-are-we-now-nist-cybersecurity-framework-one-year-later.

firms in developing their cybersecurity policies. Moreover, the federal government as well as a majority of states have enacted cybersecurity laws.[28]

i. The SEC Makes Cybersecurity a Priority

In 2014 and 2015, the SEC's Office of Compliance Inspections and Examinations (OCIE) included cybersecurity in its examination priorities. In 2014, OCIE listed "information technology" as an area that would continue to be examined, and included "cybersecurity" in a list of items on which its staff would focus with respect to the core risks of trading.[29] In 2015, OCIE's examination priorities include cybersecurity as a market-wide risk that will be scrutinized by the SEC.[30]

A few months after OCIE released its 2014 exam priorities, the SEC hosted a roundtable on cybersecurity.[31] In her opening remarks at the roundtable, SEC Chairman Mary Jo White opined that the threats on cybersecurity are global and pose a grave risk to our economy. Chairman White also stated that such risks are "first on the Division of Intelligence's list of global threats, even surpassing terrorism."[32] Panelists at the roundtable included government officials, service providers, investors and academics, all of whom shared their perspective on evaluating and addressing cybersecurity challenges.[33] Many of the panelists referenced the utility of the NIST framework,[34] but cautioned that the framework should not be viewed as a one-size-fits-all approach for dealing with cybersecurity risks.

At the SEC roundtable, cyber-attack perpetrators were categorized as follows:

- those seeking to steal national security secrets or intellectual property;
- organized criminals seeking to steal people's identity and money;
- terrorists desiring to attack a firm's infrastructure;
- "hacktivists" attempting to make a social statement by stealing information and publishing it to embarrass organizations or extort them; and
- insiders or people whose employment was terminated on bad terms.

The roundtable also identified the primary methods used to carry out cyber-attacks, including:

- the destruction of data or hardware;
- denial of service;
- theft of information, money or identity; and
- ransomware, which encrypts files until a ransom is paid.

ii. The CFTC Makes Cybersecurity a Priority

On February 26, 2014, the CFTC's Division of Swap Dealer and Intermediary Oversight issued recommended best practices for futures commission merchants, commodity trading advisors, commodity pool operators, introducing brokers, retail foreign exchange dealers, swap dealers and major swap participants.[35] The best practices highlight the steps registrants should take to secure the financial information of their customers in compliance with rules regarding customers' privacy, security and confidentiality under the Gramm-Leach-Bliley Act.

---

[28] *See* supra note 22, see also *Federal Information Security Modernization Act of 2014*.

[29] OCIE, "Examination Priorities for 2014" (Jan. 9, 2014).

[30] OCIE, "Examination Priorities for 2015" (Jan. 13, 2015).

[31] *See* a transcript of the Cybersecurity Roundtable.

[32] *Id.*

[33] SEC Press Release, "SEC Announces Agenda, Panelists for Cybersecurity Roundtable."

[34] *See* Supra note 26.

[35] Division of Swap Dealer and Intermediary Oversight, "Gramm-Leach-Bliley Act Security Safeguards" (Feb. 26, 2014).