Bloomberg BNA

Securities Regulation & Law Report™

FINANCIAL SERVICES

Cybersecurity and Financial Firms: Bracing for the Regulatory Onslaught

By John Reed Stark

I. Introduction

A cyber-crisis can strike a financial firm at any time. The loss of intellectual property and sensitive customer information, disruption of services, and headlines reporting the attack not only shake the confidence of any of a firm's multiple constituencies—especially investors, shareholders, employees, partners and customers—but now more than ever, a cyber-crisis can also trigger the interest (and possibly the wrath) of the Office of Compliance, Inspections and Examinations (OCIE) of the Securities and Exchange Commission (SEC) and, for registered broker-dealers, the Financial Industry Regulatory Authority (FINRA) as well.

John Reed Stark is a Managing Director of Stroz Friedberg, an investigations, intelligence, and risk management company. Formerly, Mr. Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, the last 11 of which as Chief of its Office of Internet Enforcement. He has also served for 15 years as an Adjunct Professor of Law at the Georgetown University Law Center, where he has taught several securities regulation courses, including ''Advanced Securities Regulation'' and ''Securities Law and the Internet.''

Nowadays, when financial firms[1] experience any form of data breach—from the loss or theft of laptops, backup tapes, or hard drives containing sensitive client or customer data, to the compromises of, or intrusions into, a firm's servers, networks and other systems—financial regulators are going to come knocking (or even pounding) on the door.

Regulators such as OCIE and FINRA will also want to know more than just what a firm is doing to detect the origin, nature and extent of the cyber-related incident and what sort of remediation the firm is undertaking; their examiners will also want to understand what sort of cybersecurity preparedness firms undertake to protect their networks and systems together with what plans, policies and procedures firms have established to thwart cyber-intrusions and attacks.

A regulatory cyber-storm is clearly brewing and its onslaught will have a dramatic impact upon how financial firms build, manage and protect their information and trading systems, causing many to redouble their efforts toward enhancing their technological capabilities. Some financial firms may even have to invent a new type of information technology (IT) security department that includes the wherewithal and platforms to enable quick and nimble response to cyber-threats, and the ability to report in real-time a firm's technology-related regulatory compliance, including producing cybersecurity infrastructure, planning and tactics as well as reporting instantaneously the frontline particulars of any actual cyber-incident response.

Even more importantly, SEC and FINRA examination staff will seek to understand a firm's cybersecurity methodologies (i.e. how firms combine both traditional investigative techniques with computer forensics and cyber-crime response to ascertain facts and conclusions

[1] ''Financial firms'' meaning brokerage firms, investment advisers, mutual funds, hedge funds, private equity funds, and other SEC and FINRA-regulated entities; however, the discussions in this article also apply to more traditional institutions that may have operations beyond the scope of SEC jurisdiction, such as banks, insurance companies, 401K plans, etc.

 ISSN 0037-0665

upon which shareholders, customers, board members, corporate officers and IT executives can rely).

For instance, regulatory examiners will expect to find, during both routine and for-cause examinations, the plans financial firms have in place: 1) to assess damage in the aftermath of a cyber-attack; 2) to decide whether to make statutory notifications; 3) to make public statements regarding the type of cyber-intrusion; and 4) to decide whether to report the matter to the SEC, FINRA or other law enforcement or regulatory agency. To help practitioners, in-house counsel, compliance officers, technology personnel and the many other professionals impacted by this recent financial regulatory surge, this article discusses:

- the current regulatory landscape of, and recent increase of regulatory interest in, the cybersecurity policies and practices at financial firms;
- SEC enforcement actions pertaining to cybersecurity;
- the type of cybersecurity information SEC and OCIE examiners may expect to receive during their examinations of SEC-regulated entities;
- recommended technology-related steps for broker-dealers, registered investment advisers, hedge funds, private equity firms, and other financial firms to take in response to increased regulatory focus and new regulatory initiatives, including how financial firms can launch a ''pre-emptive holistic strike'' to counter the anticipated regulatory offensive; and
- suggested guidelines and protocols to successfully manage a data breach after its detection.

II. The Current Regulatory Landscape Relating to Cybersecurity: A Quiet Evolution

The build-up of regulatory interest in the cybersecurity of financial firms has been quiet but steady, with the intensity growing particularly strong at the SEC and FINRA in the past few years.

1. January 2010: Renewed SEC Focus on IT Infrastructure. On Jan. 5, 2010, then-SEC Chairman Mary Schapiro appointed Carlo di Florio to be her director of OCIE. A seasoned risk management and regulatory compliance expert, di Florio made great strides in strengthening the SEC's examination strategy, structure, training programs, processes and systems; in recruiting new examiners with more specialized and technological skill-sets; and in emphasizing the importance of the technological aspects of a financial firm's technological operations. As a result, not only have OCIE's examiners already become far more focused on IT infrastructure[2] but an SEC IT professional sometimes accompanies an examination team for on-site visits (or works behind the scenes providing advice). OCIE staff have also increased their use of an equally beefed-up SEC in-house forensics group to handle large data for examinations, which has led to broader and more invasive requests.

2. October 2011: The SEC Cybersecurity Guidance. On Oct. 13, 2011, the SEC released its first-ever staff guidance pertaining exclusively to the cybersecurity-related disclosure obligations of public companies. The guidance served as a wake-up call for many public companies and an early warning from the SEC that the agency planned to take a strong interest in public companies' manners of handling cybersecurity incidents.[3]

This unique SEC guidance covered a public company's reporting responsibilities both after a cyber-attack as a ''material'' event and beforehand as a ''risk factor.'' From the SEC's perspective, the requirements outlined in the guidance introduced nothing new but, instead, merely clarified the SEC's long-standing requirement that public companies report ''material'' events to their shareholders, i.e. important developments or events that ''a reasonable investor would consider important to an investment decision.''[4]

Precisely *what* renders an event ''material'' has plagued securities lawyers for years and has been the subject of countless judicial decisions, SEC enforcement actions, law review articles, law firm guidance and the like. However, with the ''promulgation'' of this new guidance, the SEC officially (and quite noticeably) added cybersecurity into the mix of disclosure by putting every public company on notice that cyber-attacks and cybersecurity risk fall squarely within a public company's reporting responsibilities.

The guidance was created in May 2011, a few years after Chair Mary Schapiro took over the helm of the SEC, when, at the same time, Chairman of the Senate Commerce Committee Senator Jay Rockefeller (D-W.Va.) and four other U.S. Senators sent a letter to the SEC asking them to clarify corporate disclosure requirements for cybersecurity-related incidents, quoting statistics from a 2009 survey concluding that 38 percent of Fortune 500 companies had made a significant oversight in their public filings by not discussing privacy and data security events.[5]

Apparently pleased with the SEC's guidance, Senator Rockefeller issued a press release stating that the SEC guidance fundamentally changed the future of cybersecurity on Oct. 13, 2011.[6] Yet, almost exactly two years

---

[2] Reviewing of e-mails and other electronic communications, such as postings to social networking sites by registered persons has been a focus of OCIE since 2010, when FINRA released guidelines in this regard. ''Americans are increasingly using social media Web sites, such as blogs and social networking sites, for business and personal communications. Firms have asked FINRA staff how the FINRA rules governing communications with the public apply to social media sites that are sponsored by a firm or its registered representatives. This Notice provides guidance to firms regarding these issues.'' *See* FIN. INDUS. REGULATORY AUTH., REGULATORY NOTICE 10-06 (2010), *available at* http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p120779.pdf

[3] SEC. & EXCH. COMM'N, CF DISCLOSURE GUIDANCE: TOPIC NO. 2 (2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[4] SEC. & EXCH. COMM'N, STAFF ACCOUNTING BULLETIN NO. 99 (1999), *available at* https://www.sec.gov/interps/account/sab99.htm.

[5] Letter from Sen. Jay Rockefeller to Mary Schapiro, Chairman, Sec. & Exch. Comm'n (May 11, 2011), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4e21-92c7-a8e1dd5a707e

[6] U.S. SENATE COMM. ON COMMERCE, SCI. & TRANSP., *Rockefeller Says SEC Guidance Fundamentally Changes the Future of Cybersecurity* (Oct. 13, 2011), *available at* http://www.commerce.senate.gov/public/index.cfm?

  SRLR ISSN 0037-0665

later, Senator Rockefeller wrote a second letter to the SEC expressing his concern that public companies were skirting their disclosure responsibilities pertaining to cyber-attacks. Senator Rockefeller specifically requested newly confirmed Chair White to consider releasing more formalized Commission-level guidance to help ensure investors get information they need and to issue that guidance at the Commission (rather than the staff) level.

Senator Rockefeller wrote, ''While the staff guidance has had a positive impact on the information available to investors on these matters, the disclosures are generally still insufficient for investors to discern the true costs and benefits of companies' cybersecurity practices.'' In her response to Senator Rockefeller, Chair White did not comment as to whether the agency would toughen the guidance. Senator Rockefeller even pushed legislation to make the SEC issue stronger guidelines for disclosing risks of cyber-attacks, urging that it be included in cybersecurity legislation in 2012. That measure died in the U.S. Senate. ''It's important for investors to understand whether companies are effectively addressing all forms of risk, from financial and operational to cyber, and this information is a key element in the legislation that the Senate is working on to strengthen our nation's cybersecurity,'' Senator Rockefeller said.[7]

Despite the pressure from Senator Rockefeller, since the issuance of the guidance, enforcement related to it has been quiet (though anecdotal reports indicate that many public companies have increased their attention to disclosure of cyber-related incidents and compliance with the guidelines made cybersecurity-related disclosures an important priority).[8]

According to Bloomberg News, Chair White has stated that the SEC's staff has issued comments related to cybersecurity disclosures to about 50 publicly traded companies, offering one of few glimpses at the number of times SEC corporation finance staff has contacted public companies about the cyber-related disclosures contained in their filings.[9]

Although Chair White told Congress last year that her agency was reviewing whether a more robust disclosure process was needed, she also told reporters last fall that she felt the guidance appeared to be working well and she did not see an immediate need to create a rule mandating public reporting of cyber-attacks.[10]

3. January 2014: Jane Jarcho Speech. On Jan. 30, 2014, during a panel discussion at an OCIE event for financial firm compliance professionals, OCIE announced their intention to ''scrutinize whether asset managers have policies to prevent and detect cyber-attacks and are properly safeguarding against security risks that could arise from vendors having access to their systems.''[11]

According to a Reuter's report of the event, Jane Jarcho, the national associate director for the SEC's investment adviser exam program elaborated: ''We will be looking to see what policies are in place to prevent, detect and respond to cyber-attacks. We will be looking at policies on IT training, vendor access and vendor due diligence, and what information [registered investment advisers] have on any vendors.''[12]

According to Jarcho, the SEC will conduct its upcoming 2014 review of cybersecurity policies for asset managers as part of the agency's routine examinations of investment advisers and investment companies, such as mutual funds. OCIE inspection and examination programs such as the one Jarcho described, can, however, involve any SEC-regulated entity, including broker-dealers, hedge funds, private equity funds, or any other kind of SEC-registered financial firm.

The OCIE anticipated focus, which is a logical addition to the corporation finance staff cybersecurity disclosure guidance, should come as no surprise—especially given the spate of recent cyber-attacks on major U.S. retailers. It is only natural for the SEC staff to jump headfirst into the cyber-fray and use their own statutory and jurisdictional weaponry to join in the global battle against cyber-attacks.

In fact, the SEC on April 15, 2014, very quietly made public its examination ''module''[13] pertaining to cybersecurity—a very rare and unusual disclosure. The SEC also stated in its release of the module, the following: ''Key Takeaways: OCIE will be conducting examinations of more than 50 registered broker-dealers and registered investment advisers, focusing on areas related to cybersecurity. In order to empower compliance professionals with questions and tools they can use to assess their respective firms' cybersecurity preparedness, OCIE has included a sample cybersecurity document request in the Appendix to this Risk Alert.''[14]

4. January 2014: FINRA Cybersecurity Sweep Begins. In January of 2014, FINRA issued the following notice on its website, announcing a cybersecurity ''sweep'' and indicating FINRA's resolve to focus on cybersecurity

---

p=PressReleases&ContentRecord_id=4acbf0d1-7695-4fd8-be64-b950da8f1372&ContentType_id=77eb43da-aa94-497d-a73f-5c951ff72372&Group_id=4b968841-f3e8-49da-a529-7b18e32fd69d&MonthDisplay=10&YearDisplay=2011.

[7] http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51)

[8] *See, e.g.*, Ellen Nakashima & Danielle Douglas, *More companies reporting cybersecurity incidents*, WASH. POST, March 1, 2013, *available at* http://www.washingtonpost.com/world/national-security/more-companies-reporting-cybersecurity-incidents/2013/03/01/f7f7cb68-8293-11e2-8074-b26a871b165a_story.html (" . . . [I]t appears that SEC guidance issued in October 2011 making clear that companies need to report significant computerized theft or disruption, combined with greater public attention to the issue, is forcing more disclosure. Also, the fact that the banks hit by the DDOS attacks have been named in media accounts has made ignoring them more difficult.'')

[9] Chris Strohm, *SEC Chairman Reviewing Cybersecurity Disclosures*, BLOOMBERG NEWS (May 13, 2013), *available at* http://www.bloomberg.com/news/2013-05-13/sec-chairman-reviewing-company-cybersecurity-disclosures.html.

[10] *After retailer breaches, SEC plans roundtable on cybersecurity*, REUTERS (Feb. 14, 2014), *available at* http://www.reuters.com/article/2014/02/14/us-usa-sec-cyber-idUSBREA1D1NM20140214.

[11] Sarah N. Lynch, *SEC examiners to review how asset managers fend off cyber attacks*, REUTERS (Jan. 30, 2014), *available at* http://www.reuters.com/article/2014/01/30/us-sec-cyber-assetmanagers-idUSBREA0T1PJ20140130.

[12] *Id.*

[13] ''Module'' is the term OCIE uses to describe the sort-of questionnaire OCIE examiners use as their initial querying document when examining SEC-regulated entities.

[14] SEC National Exam Program Risk Alert Volume IV, Issue 2, (April 15, 2014), *available at* http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.

policies, practices and procedures implemented in their member firms:

FINRA is conducting an assessment of firms' approaches to managing cyber-security threats. FINRA is conducting this assessment in light of the critical role information technology (IT) plays in the securities industry, the increasing threat to firms' IT systems from a variety of sources, and the potential harm to investors, firms, and the financial system as a whole that these threats pose.

FINRA has four broad goals in performing this assessment:

1. to understand better the types of threats that firms face;

2. to increase our understanding of firms' risk appetite, exposure and major areas of vulnerabilities in their IT systems;

3. to better understand firms' approaches to managing these threats, including through risk assessment processes, IT protocols, application management practices and supervision; and

4. as appropriate, to share observations and findings with firms.

Note: The assessment addresses a number of areas related to cybersecurity, including firms':

- *approaches to information technology risk assessment;*
- *business continuity plans in case of a cyber-attack;*
- *organizational structures and reporting lines;*
- *processes for sharing and obtaining information about cybersecurity threats;*
- *understanding of concerns and threats faced by the industry;*
- *assessment of the impact of cyber-attacks on the firm over the past 12 months;*
- *approaches to handling distributed denial of service attacks;*
- *training programs;*
- *insurance coverage for cybersecurity-related events; and*
- *contractual arrangements with third-party service providers.*[15]

5. March 2014: The SEC Cybersecurity Roundtable. March 26, 2014 marked the first SEC Cybersecurity Roundtable event devoted exclusively to the topic of cybersecurity. Most likely prompted by the recent spate of cyber-attacks on retailers, which has refocused the attention of the business community and policymakers on the area, it was an unprecedented focus on the area of cybersecurity at financial firms and clearly a harbinger of regulatory scrutiny to come.

The roundtable also brought to bear once again Chair White's take on the issue of cybersecurity at financial firms. She noted quite clearly that cyber-attacks ''are of extraordinary and long-term seriousness'' and stressed that the public and private sectors need to be ''riveted in lockstep'' in addressing the complex threats they pose.[16]

At the roundtable, recently appointed OCIE head Andrew Bowden[17] made clear OCIE's intent to focus on the area of cybersecurity in financial firms and his team's resolve to be rigorous in their expectations concerning the protection of not just the assets of their customers and clients, but also their personal identifying information, as well as the intellectual property of financial firms and any information that an intruder could use to gain an unlawful trading advantage.[18]

6. Dodd-Frank SEC Whistle-blower Provisions/FINRA Office of the Whistle-blower. The whistle-blower provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act reward informants who provide actionable information with between 10 and 30 percent of any follow-up SEC recovery over $1,000,000.[19] These relatively new provisions provide a particularly powerful incentive for whistle-blowers with information on potential regulatory violations, including lapses in cybersecurity. No financial firm is immune to the disgruntled employees, unhappy investors or portfolio companies, peeved competitors and the like who are now economically incentivized to report even baseless allegations to the SEC (and send them electronically and anonymously if they so choose).

Similarly, though not offering any sort of reward, FINRA has also formed its own Office of the Whistleblower to expedite ''the review of high-risk tips by FINRA senior staff and ensure a rapid response for tips believed to have merit.'' Led by seasoned regulatory expert and FINRA veteran Cameron Funkhouser, the Office of the Whistleblower enables individuals with evidence of, or material information about, *any* potentially illegal or unethical activity (including cybersecurity breaches) to reach FINRA senior staff, who can quickly assess the level of risk involved and make sure that

---

[15] Fin. Indus. Regulatory Auth., Targeted Examination Letters (Jan. 2014), *available at* http://www.finra.org/Industry/Regulation/Guidance/TargetedExaminationLetters/P443219.

[16] Peter Isajiw, *What Role Should the SEC Play in Cybersecurity*, Law.com (March 28, 2014), *available at* http://www.law.com/sites/peterisajiw/2014/03/28/what-role-should-the-sec-play-in-regulating-cybersecurity/?slreturn=20140230100837. *See also* Matthew P. Allen, *The SEC Speaks 2014—The SEC Reveals Regulatory and Litigation DNA Now Includes Economic Analysis and Technology*, Lexology (Feb. 24th, 2014), *available at* http://www.lexology.com/library/detail.aspx?g=11bdeddb-38b9-4e39-9f17-f4a61deaf53b (''[T]he increased use of technology and data in the capital and financial markets makes them more vulnerable to cyber-attacks and disruptions. So White and other commissioners emphasized the need for increased vigilance on cyber security for all market participants and investors'').

[17] Press Release, Securities and Exchange Commission, SEC Names Andrew Bowden as Director of National Exam Program (May 2, 2013), *available at* http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171514170.

[18] Mark Schoeff Jr., *SEC Searches for Role in Battling Cyber Threats*, Investment News (March 26, 2014), *available at* http://www.investmentnews.com/article/20140326/FREE/140329923; *see also*, Dave Michaels & Chris Strohm, *SEC Probes Threat from Cyber Attacks Against Wall Street*, Bloomberg News (March 26th, 2014), *available at* http://www.bloomberg.com/news/2014-03-25/sec-probes-threat-from-cyber-attacks-against-wall-street.html.

[19] U.S. Securities and Exchange Commission Office of the Whistleblower, http://www.sec.gov/whistleblower.

  SRLR ISSN 0037-0665

each tip is properly evaluated (or referred, if outside of their jurisdiction).[20]

These FINRA and SEC whistle-blower initiatives have, in many instances, transformed how financial firms approach employees who claim to have identified compliance lapses (even if the whistleblower bears a grudge) and empowered even the most low-level IT personnel to report their concerns if they believe their employers are not adequately addressing cybersecurity compliance requirements.

III. SEC Enforcement and Cybersecurity: The Backdrop

When researching SEC enforcement actions involving cybersecurity, the first to find are probably the lengthy string of so-called ''account-takeover'' matters led by the SEC's Office of Internet Enforcement during the late 1990s and the early 2000s. For example, in late 2006 and 2007, the SEC filed civil enforcement actions in federal district court against hackers from Estonia and India who used stolen usernames and passwords to commit securities fraud. In some instances, the perpetrators first purchased thinly traded microcap securities; then they hacked into online brokerage accounts and purchased shares of the same microcap securities in order to drive up the trading price. They then sold the microcap positions in their own accounts, making a quick and substantial profit.[21]

Using sophisticated computer hacking and identity theft techniques to break into the accounts of innocent online brokerage customers, these perpetrators effectively cut out the middleman of the old fashioned pump-and-dump scheme, eliminating phony stock promotions by creating their own artificial trading demand, and consummating their frauds in just a few hours.

These pump-and-dump schemes with a cybersecurity twist are fraudulent market manipulations violating the SEC's frequently used anti-fraud statutory weaponry, but are not necessarily related to what OCIE and FINRA have in mind today when they begin their focus on cybersecurity issues at financial firms.

Historically, the SEC enforcement division has not applied the SEC's antifraud provisions for cybersecurity issues at registered investment advisers, broker-dealers and other financial firms; the SEC enforcement division has instead utilized ''Regulation S-P'' as its basis for addressing cybersecurity lapses. And while not necessarily designed and drafted to directly address cybersecurity, Regulation S-P has provided a sufficient statutory hook for SEC enforcement staff to rely upon.

1. Regulation S-P.

Rule 30(a) of Regulation S-P, commonly referred to as the ''Safeguard Rule,'' requires broker-dealers and SEC-registered investment advisers to adopt written policies and procedures reasonably designed to protect customer information against unauthorized access and use.[22]

Specifically, the Safeguard Rule requires every broker-dealer and investment adviser registered with the SEC to adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information, and that are reasonably designed to: (1) ensure the security and confidentiality of customer 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.[23]

By way of background, Regulation S-P contains the privacy rules promulgated by the SEC under section 504, Subtitle A of Title V of the Gramm-Leach-Blilely Act (GLB). Specifically, section 504 requires the Commission and other federal agencies to adopt rules implementing notice requirements and restrictions on a financial institution's ability to disclose non-public personal information about consumers. Under GLB, a financial institution must provide its customers with a notice of its privacy policies and practices,[24] and must not disclose non-public personal information about a consumer to unaffiliated third parties unless the institution provides certain information to the consumer and the consumer has not elected to opt out of the disclosure.[25]

---

[20] FINRA Office of the Whistleblower, https://www.finra.org/Industry/Whistleblower/

[21] Press Release, Securities and Exchange Commission, SEC Obtains Order Freezing $3 Million in Proceeds of Suspected Foreign-Based Account Intrusion Scheme (March 7, 2007), *available at* http://www.sec.gov/news/press/2007/2007-33.htm; *see also* Thomas O. Gorman, *SEC Continues to Target Account Intrusions*, SEC Actions Blog, *available at* http://www.secactions.com/sec-continues-to-target-account-intrusions/.

[22] Regulation S-P, Privacy of Consumer Financial Information was created on March 2, 2000, when the Commission issued a notice of proposed rulemaking (Proposing Release) (RX 13). Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 12354 (Mar. 8, 2000). On June 22, 2000, the Commission adopted final rules (Adopting Release) (RX 14). Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 40334 (June 29, 2000). Regulation S-P became effective on a voluntary basis as of November 13, 2000, and compliance was mandatory as of July 1, 2001. 17 C.F.R. § 248.18. The Safeguard Rule derives from Subtitle A of Title V of the GLB Act requires the Commission and the other federal regulators to establish standards for financial institutions relating to administrative, technical, and physical safeguards for customer records and information. *See* 15 U.S.C. § 6801(b). As described in Section 501(b) of the GLB Act, the objectives of these standards are to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of those records; and (3) protect against unauthorized access to or use of those records or information which could result in substantial harm or inconvenience to any customer. See 15U.S.C. §§ 6801(b)(1)-(3). The GLB Act does not define the terms ''customer records and information'' and ''substantial harm or inconvenience.'' *See also In re Ellis*, SEC Release 34-64220 (April 7, 2011), *available at* https://www.sec.gov/litigation/admin/2011/34-64220.pdf.

[23] 17 C.F.R. § 248.18.

[24] Regulation S-P does not prescribe any specific format or standardized wording for privacy notices. Instead, financial institutions may design their own notices based on their individual practices, provided they meet the ''clear and conspicuous'' standard in 15 U.S.C. § 6803(a) and 17 C.F.R. § 248.3(c) and furnish the content required by 17 C.F.R. § 248.6.

[25] Congress enacted the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLB Act), Pub. L. No. 106-102, 113 Stat. 1338, in November 1999. Subtitle A of Title V of the GLB Act, captioned *Disclosure of Nonpublic Personal Information*, contains privacy protections

Enforcement of GLB's Subtitle A of Title V rests solely with federal regulators and state insurance authorities with respect to financial institutions and other persons subject to their jurisdiction under applicable laws.[26] Thus, the SEC has the authority to enforce Subtitle A of Title V with respect to brokers, dealers, investment companies, and registered investment advisers under the federal securities laws.[27]

2. Some SEC Enforcement Actions Relating to Cybersecurity.

a. The GunnAllen Matters. On April 7, 2011, the SEC charged three former brokerage executives for failing to protect confidential information about their customers. Specifically, the SEC's investigation found that while Tampa-based GunnAllen Financial Inc. (''GunnAllen'') was winding down its business operations, former President Frederick O. Kraus and former National Sales Manager David C. Levine violated customer privacy rules by improperly transferring customer records to another firm. The SEC also found that former Chief Compliance Officer Mark A. Ellis failed to ensure that the firm's policies and procedures were reasonably designed to safeguard confidential customer information.[28]

The SEC's orders found that all three respondents willfully aided and abetted and caused GunnAllen's violations of Rule 30(a) of Regulation S-P under the Securities Exchange Act of 1934, and that Kraus and Levine willfully aided and abetted the firm's violations of Rules 7(a) and 10(a) of the same regulation.[29]

Without admitting or denying the SEC's findings, the officials each consented to the entry of an SEC order that censured them and required them to cease and desist from committing or causing any violations or future violations of the provisions charged, and to pay penalties ranging from $15,000 to $20,000 each.[30]

The matter was investigated by the SEC enforcement division, but also specifically cited in the press release as in coordination with an examination of the firm conducted by seven members of OCIE.[31]

Eric Bustillo, the head of the SEC's Miami office stated at the time, ''Brokerage customers should be able to trust that sufficient safeguards are in place to protect their private information from unauthorized access and misuse. Protecting confidential customer information is particularly important when a broker-dealer is winding down operations.'' Glenn S. Gordon, associate director of the Miami Regional Office, added, ''GunnAllen did not have adequate policies or procedures in place to safeguard client information, ignoring several red flags from security breaches at the firm in prior years.''[32]

With respect to the security breaches cited by Mr. Gordon, the SEC found that, once aware of the breaches, GunnAllen's CCO failed to direct the firm to: (1) properly assess the risk that these breaches posed to customers; (2) adopt additional written policies and procedures to protect customer information in accordance with the Safeguards Rule; and (3) take remedial steps recommended by employees, such as contacting law enforcement authorities or affected customers. The SEC noted that the data breaches and the firm's limited response to them highlighted the inadequacy of the firm's written policies and procedures for safeguarding information, and that in failing to direct the firm to revise or supplement these policies and procedures, the CCO caused the firm to violate the Safeguards Rule.

The security breaches cited by the SEC did not involve what IT professionals might consider more sophisticated cyber intrusions (such as an Advanced Persistent Threat or APT,[33] SQL Injection,[34] botnet, malware, or other more ''code-generated'' cyber-attacks). Rather, the data breaches at GunnAllen were caused by

---

and related safeguarding measures for consumer financial information. These protections are codified at 15 U.S.C. §§ 6801-6809. The GLB Act declared it to be ''the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.'' 15 U.S.C. § 6801(a). Section 509(4)(A) of the GLB Act defines ''nonpublic personal information'' as ''personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution.'' 15 U.S.C. § 6809(4)(A). The statutory definition excludes publicly available information (unless provided as part of a list, description, or other grouping), as well as any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using nonpublic personal information. 15 U.S.C. §§ 6809(4)(B)-(C). The GLB Act does not define either ''personally identifiable financial information'' or ''publicly available information.'' See also Final Rule, Privacy of Consumer Financial Information, 17 CFR PART 248 , Release Nos. 34-42974, IC-24543, IA-1883; File No. S7-6-00 at http://www.sec.gov/rules/final/34-42974.htm (effective November 13, 2000).

[26] 15 U.S.C. § 6805(a)

[27] 15 U.S.C. §§ 6805(a)(3)(5). N.B. that consumers cannot bring private causes of action against financial institutions that violate the provisions of Subtitle A of Title V. *See Dunmire v. Morgan Stanley DW, Inc.*, 475 F.3d 956, 960 (8th Cir. 2007) (collecting cases).

[28] Press Release, Securities and Exchange Commission, SEC Charges Brokerage Executives With Failing to Protect Confidential Customer Information (April 7, 2011), *available at* https://www.sec.gov/news/press/2011/2011-86.htm.

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] So-called APT attacks eschew technical sophistication for careful reconnaissance taking instead a low-and-slow approach that is difficult to detect and has a high likelihood of success. Attackers only need to trick a single employee into opening a piece of malware that exploits a zero-day vulnerability, thus giving them access to not just the employee's PC, but potentially the entire corporate network. *Advanced Persistent Threats Get More Respect*, Information Week (Feb. 9, 2012), *available at* http://www.informationweek.com/government/cybersecurity/advanced-persistent-threats-get-more-respect/d/d-id/1102737?.

[34] Structured Query Language is the programming language used to manage data in a database; more appropriately, relational database management systems (RDBMS). The types of management systems that employ Structured Query Language include Microsoft SQL Database, Oracle, MySQL, PostgreSQL, and others. A so-called SQL injection involves attacking and compromising a database, which is an organized collection of data and supporting data structures. The data can include user names, passwords, text, etc. ''The point of the hack is not just to get information from the target site. Depending on the intention of the malicious hooligans attacking you, it can include to bypass logins, to access data . . . to modify the content of a website as when hackers replace the website with a new front page, or simply shut down the server.'' Gery Menegaz, *SQL Injection Attack: What is it, and how to prevent it*, ZDNet (July 13, 2012), *available at* http://www.zdnet.com/sql-injection-attack-what-is-it-and-how-to-prevent-it-7000000881/

   ISSN 0037-0665

a theft of the laptops of a few registered representatives and a former employee's unauthorized access of a current employee's firm e-mail account.

The GunnAllen settlement marked the first time that the SEC assessed financial penalties against individuals charged solely with violations of Regulation S-P and clearly marked the data breach territory as their own. Moreover, the settlement indicates not only that the SEC is willing to hold senior officers of financial institutions individually liable for their role in violations of Regulation S-P but also that the SEC, when assessing Regulation S-P liability, will consider whether an information security policy is sufficiently comprehensive as well as the effect of a firm's actions upon the privacy rights of customers.

b. The NEXT Financial Group Matter. In 2007, the SEC enforcement division alleged in *In re NEXT Financial Group*, that NEXT violated Regulation S–P by permitting registered representatives who were leaving the firm to take clients' personal financial information and aided and abetted other firms' violations of Regulation S-P by encouraging and assisting newly recruited, registered representatives to bring non-public personal information about their former firm's clients to NEXT. In 2008, an administrative law judge issued an initial decision that imposed a $125,000 fine on NEXT.[35]

The instances center around the methods used by NEXT's ''transition team'' to help bring on new registered representatives. According to the Administrative Order, the transition team assisted new recruits by ''pre-populating'' account transfer documents such as automated customer account transfer forms (ACATS), new account information forms, change of broker-dealer letters, and mailing labels. The team provided all recruits with a sample Excel spreadsheet showing what types of customer information to provide in order to start pre-population.[36]

The Administrative Order also stated that when a registered representative left NEXT, he was allowed to take copies of all his customer files and documents, which included non-public personal information, and to download similar non-public personal information from NEXT's computer system.[37] Further, the Administrative Order asserted that NEXT's transition team sometimes used recruits' user IDs and passwords not only to access recruits' current b/d computer system but also to download non-public personal information used to pre-populate documents, and to access various mutual fund and annuity company websites to extract customer information. In at least one instance, NEXT received non-public client information from a recruit who later decided not to join the firm, yet the customer information was retained in NEXT's computer system.[38]

c. The Commonwealth Equity Matter

The GunnAllen action, though the first of its kind, was not the first time the SEC enforcement division had acted with respect to privacy and information security violations of the Privacy Rule and the Safeguards Rule. For instance, in October 2009, Commonwealth Equity Service LLP, a stock trading firm, similarly settled the SEC's charges that it had violated the SEC's Safeguards Rule.

Specifically, the firm experienced an information security breach when a perpetrator installed a virus on the firm's computers and obtained log-in credentials of the firm's registered representative. The perpetrator used the credentials to access the firm's customer accounts and place unauthorized securities orders in excess of $500,000.

The SEC alleged that the firm violated the Safeguards Rule by: (1) failing to require the firm's registered representatives to maintain antivirus software on their computers; (2) failing to audit computers to determine whether antivirus software had been installed; (3) failing to implement policies and procedures to appropriately review the firm's registered representatives' computer security measures; and (4) failing to implement procedures to track and address information security issues. As a result of these failures, the SEC alleged that , the firm's customer information was left vulnerable to unauthorized access. To settle the SEC's charges, Commonwealth Equity Service paid a penalty of $100,000 and agreed to cease and desist from committing or causing future violations of the Safeguards Rule.[39]

d. The Sydney Mondschein Matter

Somewhat akin to the Next Financial Group matter, and worthy of mention, is the Sydney Mondschein SEC federal action and related administrative proceeding involving a violation of Regulation S-P by a broker who misappropriated from his employer personal identifying information for his own profit.[40]

The Mondschein actions involved allegations by the SEC that between December 2002 and August 2005, Sydney Mondschein, a brokerage firm, was found liable for its registered representative's activities in violation of Regulation S-P by failing to disclose to customers that he intended to, and did sell their personal information to insurance agents. Specifically, the SEC's complaint charged that Mondschein reaped illegal profits by secretly selling the names and other confidential personal information of over 500 of his customers to six different insurance agents.[41]

The final judgment, entered on April 14, 2008, permanently enjoined Mondschein from violating Section 10(b) of the 1934 Exchange Act and Rule 10b-5 there-

---

[35] *In re Next Fin. Grp., Inc.*, Initial Decision Release No. 349, Administrative Proceeding File No. 3-12738. (June 19th, 2008) (Judge James T. Kelly) http://www.sec.gov/litigation/aljdec/2008/id349jtk.pdf; *see also* Before the National Adjudicatory Council Financial Industry Regulatory Authority, *In re Dep't Enforcement vs. Dante J. DiFrancesco*, Croton, NY, Respondent. DECISION - Complaint No. 2007009848801. Dated: December 17, 2010 (FINRA's National Adjudicatory Council affirmed a $10,000 fine and 10-day suspension ordered by a FINRA hearing panel in a contested hearing against a broker for his downloading confidential customer information from his firm's computer system onto a flash drive on his last day of employment and then sharing that information with a new firm. FINRA found the broker's actions prevented his former firm from giving its customers a reasonable opportunity to opt out of the disclosures, as required by Regulation S-P. FINRA also found the broker's misconduct caused his new firm to improperly receive non-public personal information about his former firm's customers.)

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *In re Commonwealth Equity Servs., LLP*, Release Nos. 34-60733 ; 33- 2929 (Sept. 29, 2009), *available at* http://www.sec.gov/litigation/admin/2009/34-60733.pdf.

[40] *SEC v. Mondschein*, Civil Action No. C-07-6178 SI (N.D. Cal., Dec. 6, 2007) Litigation Release No. 20386, *available at* http://www.sec.gov/litigation/litreleases/2007/lr20386.htm

[41] *Id.*

under, and from aiding and abetting any violations of Rules 4(a), 5(a), and 10(a)(1) of Regulation S-P. The final judgment also ordered Mondschein to disgorge all of his ill-gotten gains of approximately $53,000, plus prejudgment interest of approximately $4,680, and to pay a penalty of $45,000.[42]

In the separate related administrative action, the SEC issued an order barring Mondschein from associating with any broker or dealer, with a right to reapply after five years. In the district court action, the SEC's complaint alleged that Mondschein, a former Antioch, California stockbroker, sold his customers' personal information as sales ''leads'' solely to enable insurance agents to solicit these customers, many of whom had already purchased fixed or equity-indexed annuity products, to buy additional annuity products.[43]

IV. What Will OCIE Demand from SEC Regulated Entities About Cybersecurity?

Based on recent reports regarding the latest OCIE module, financial firms regulated by the SEC should expect thoughtful, meticulous, robust and exhaustive inquisitions into their overall cybersecurity.[44] Areas of operation that will experience severe probing by the SEC examination staff will likely include:

1. *Identification of Risks/Cybersecurity Governance* (e.g. security of physical devices and software platforms; network resources; connectivity platforms; protection priorities; written cybersecurity policies; risk assessment results (for both physical and IT); organizational charts and reporting lines for cybersecurity personnel; cybersecurity testing; cybersecurity training; cybersecurity insurance; data destruction practices; encryption procedures; back-up system protocols; etc.);

2. *Risks Associated With Remote Customer Access, Funds Transfer Requests and Vendors* (e.g. online access security for customers and employees; vendor security training, protocols and procedures; authentication procedures; contracting requirements; segregation and security of firm data; etc.);

3. *Detection of Unauthorized Activity* (i.e. fortressing, testing, detecting, reporting, analyzing, etc. of all suspicious unauthorized cyber-related activity, including insider threats as well as cyber threats from offshore attackers); and

4. *Intrusion Event History* (i.e. full descriptions of all intrusion-related incidents and the firm's response to the events, including malware identification and reverse engineering, phishing attempts and APT; loss calculations; notifications; forensic review methodologies; preservation techniques; logging analysis; law enforcement and/or regulatory liaison or reporting; etc.).

1. A Note Regarding Regulation S-ID. The OCIE examiners will also likely inquire if a financial firm has updated its written supervisory procedures to reflect the *Identity Theft Red Flags Rules*, which went into effect in 2013.[45] Adopted jointly with the Commodity and Futures Trading Commission (CFTC), Regulation S-ID is a comprehensive set of rules requiring the entities it regulates to adopt written identity theft prevention policies and procedures that:

- implement reasonable policies and procedures to detect, prevent, and mitigate the risk of identity theft;
- are updated periodically to reflect different types of changes in identity theft-related risks;
- senior management reviews and approves;
- provide training on relevant risks and program implementation; and
- allow for oversight of service providers.

The prevention program must involve the board of directors (or committee thereof) or a designated senior manager in the approval, oversight, development, implementation and administration of the program.[46]

These ''Red Flags'' rules only apply to SEC-regulated entities that meet the definition of ''financial institution'' or ''creditor'' under the Fair Credit Reporting Act (FCRA),[47] and are very similar to the red flags rules adopted by the U.S. Federal Trade Commission.[48]

The program must also provide for the exercise of ''appropriate and effective oversight'' over vendors and the training of employees, and must provide for annual updates to be given to the board of directors, appropriate committee, or designated senior manager.[49]

---

[42] Press Release, Securities and Exchange Commission, Final Judgment Entered Against Former San Francisco-Area Stockbroker Concerning Fraudulent Scheme That Violated the Privacy Rights of His Elderly Customers (April 17, 2008), *available at* https://www.sec.gov/litigation/litreleases/2008/lr20531.htm.

[43] *In re Mondschein*, *supra* note 39.

[44] See also earlier discussion in section II (3) and footnote 14 regarding the new 2014 OCIE module pertaining to cybersecurity.

[45] 17 CFR § 248—Subpart C—Regulation S-ID, *available at* http://www.sec.gov/rules/final/2013/34-69359.pdf

[46] Commodity Futures Trading Comm'n & Sec. & Exch. Comm'n, Identity Theft Red Flags Rules, *available at* http://www.sec.gov/rules/final/2013/34-69359.pdf.

[47] The final rule defines the term ''financial institution'' in the final rules by reference to the definition of the term in section 603(t) of the FCRA. That section defines a financial institution as including certain banks and credit unions, and ''any other person that, directly or indirectly, holds a transaction account (as defined in section 19(b) of the Federal Reserve Act) belonging to a consumer.'' Section 19(b) of the Federal Reserve Act defines ''transaction account'' to include an ''account on which the . . . account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payment or transfers to third persons or others.'' Section 603(c) of the FCRA defines ''consumer'' as an individual; thus, to qualify as a financial institution, an entity must hold a transaction account belonging to an individual. The FCRA defines ''creditor,'' by reference to the Equal Credit Opportunity Act (ECOA), as a person that regularly extends, renews or continues credit, or makes those arrangements that ''regularly and in the course of business . . . advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person.'' The FCRA excludes from this definition a creditor that ''advance[s] funds on behalf of a person for expenses incidental to a service provided by the creditor to that person . . .''

[48] *Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business*, Bureau of Consumer Prot., *available at* http://www.business.ftc.gov/documents/bus23-fighting-identity-theft-red-flags-rule-how-guide-business.

[49] Identity Theft Red Flags Rules, *supra* note 45.

   ISSN 0037-0665

V. Tackling Regulatory Cybersecurity Initiatives: A Holistic Preemptive Strike

To plan for the impending increased regulatory scrutiny for cybersecurity, financial firms should take a more holistic approach to the challenge, beginning a broad range of their own initiatives, which could include the following recommendations set forth below.

1. Review Overall Cybersecurity Policies. An easy place to begin an analysis of a financial firm's adequacy with respect to cybersecurity is with a broad examination of cybersecurity policies and procedures. In light of FINRA's examination module, framework and expectations concerning cybersecurity,[50] financial firms should consider the following questions cited below, which apply to any financial firm's cybersecurity approach (including non-FINRA regulated entities such as investment advisers, hedge funds, private equity firms and the like):[51]

a. overall approach to information technology risk and cybersecurity (Is there a commitment from the top down, both culturally and financially, to rigorous cybersecurity?);

b. business continuity plans in case of a cyber-attack (Has the financial firm properly evaluated the effectiveness of their response plan? Is the same person handling cyber-defense as the one who reports up the chain of command about breaches?);

c. organizational structures and reporting lines (Do current reporting lines make sense, given the responsibilities and accountability needed to execute the plan?);

d. processes for sharing and obtaining information about cybersecurity threats (How will the firm deal with the competing constituencies? On one hand, there are the FBI, Secret Service, and other law enforcement agencies who want to help find the intruders, and on the other hand, there are the myriad attorneys general and other state regulatory agencies who will be issuing requests and demanding answers about the safety of the personally identifiable information of their respective citizenries?);

e. understanding of concerns and threats faced by the industry (What steps does the firm undertake in the realm of security science to stay current about the latest cybersecurity intrusion modus operandi, cybersecurity-related software patches, data breach trends, etc.?);

f. assessment of the impact of cyber-attacks on the firm over the past 12 months (How often does the firm visit and revisit their own cybersecurity policies, and make changes to counter burgeoning or newly identified threats?);

g. approaches to handling distributed denial of service (DOS) attacks (How many DOS attacks has the firm experienced and what are the specifics in deterring them?);

h. training programs (How often and how effective are the firms' cyber-safety training programs, if any?);

i. insurance coverage for cybersecurity-related events (What sort of cybersecurity insurance does the firm have? Does that insurance pay for forensics and malware reverse-engineering expertise – the experts who investigate, identify, and repair the data breach?); and

j. contractual arrangements with third-party service providers (What sort of protections does the firm contractually require its third-party vendors to employ to deter cyber-attacks?).

2. Eliminate Red Flags. Not only are there now more OCIE examiners than ever before, but the examiners are also much better trained to identify IT-related red flags, which can prompt and expand a regulatory examination or inquiry.[52] Such red flags could include:

a. failure to implement an information security policy that outlines the layers of security in place – from technology and authentication protocols to restricting access and password requirements (this should also include physical security which is inexorably linked to IT security);

b. failure to create an incident response plan in order to have some degree of preparation should a security breach or cyber-attack occur;

c. failure to train employees on information security awareness, because a firm's security strategy will only work if employees are properly trained on it;

d. failure to conduct due diligence on service providers who can create unexpected risks;

e. weak internal controls and protocols regarding handling identity theft;

f. failure to employ systems and procedures to identify, address, and remediate suspicious activity registered in system log files (especially resulting from an active intrusion detection system (or IDS);

g. inadequate cybersecurity protections and systems relating to the activities of employees (especially registered persons) working at home;

h. too much cost-cutting related to IT and cybersecurity (which often go hand-in-hand), and a lack of independence and objectivity of any third-party review of cybersecurity;

i. poor integration of IT cybersecurity after a merger, acquisition, or other transformative corporate event;

j. compliance staff who lack a sophisticated understanding of IT and cybersecurity;

---

[50] Targeted Examination Letters, *supra* note 14.

[51] *Id.*

[52] For example, today's examiners would likely dig further if they found an antiquated dot matrix printer like the one used for client statements by Bernard Madoff in perpetrating his Ponzi scheme. Along those lines, OCIE just posted for a Senior Officer to lead its Technology Controls Program (TCP), which presently conducts examinations of the technology related controls at exchanges and clearing agencies. (The program was formerly known as ARP and used to report into the Division of Trading and Markets, but moved into OCIE at the beginning of this year.) OCIE intends to grow the TCP and to expand the types of registrants it examines to include investment advisers, investment companies, broker-dealers, and others. *See*, USAJOBS posting *available at* https://www.usajobs.gov/GetJob/ViewDetails/362038500.

k. inadequately documented or otherwise weak privacy protections and policies for protecting internal or outsourced data;

l. inability to capture, maintain, and reproduce electronic data (including cybersecurity-related log files) on a timely basis in a user-friendly format;

m. inadequate monitoring and supervision of communications (including emails, instant messaging, and social networking sites) among traders, analysts, and other employees;

n. inadequate IT barriers to prevent unlawful insider trading, including deficient systems identifying and monitoring traders who use both proprietary and client accounts and have knowledge of customer-pending orders; and

o. poor electronic documentation of annual and periodic reviews.

3. Create the Team. To handle this new and daunting regulatory initiative, if it has not done so already, financial firms should consider forming a cyber-incident management team. The members of the team could include employees from all the relevant c-levels of a company's organization chart, including from information technology, investor relations, public relations, legal, and other important operational departments.

A financial firm should also do its best to to have a technical incident response team available, and may need to engage a third-party expert to fill this role and conduct the investigation of the attack, performing tasks such as data preservation, malware analysis, digital forensic analysis, network log analysis, reverse engineering, remediation, and other investigative tasks.

The value of hiring an independent expert cannot be overstated. Internal IT security teams may have the expertise to perform the investigation, but many times they lack the objectivity needed for the findings to be deemed credible. A third-party digital forensics team can surround the cyber-attack scene with virtual ''yellow police tape,'' which can prove valuable during the investigation and provide added credibility and neutrality to the ultimate disclosure of the event. Moreover, leaving pristine in the short-term any potential evidence left by a cyber-attack until after the execution of a forensic identification, preservation, and analysis, can save time, money and headaches in the long-term. Cyber-attack internal probes can be compromised when, for example, critical logs, back-up tapes, hard drives, or other data become corrupted or overwritten by inexperienced investigators.

4. Protect Against Identity Theft. Regulators are going to expect financial firms to implement external data protection protocols and systems that evidence a strong commitment to protect its clients from identity theft.[53] For instance, an investment adviser or broker-dealer should also draft a well-crafted protocol to preserve data and respond to any attack on customers' PII, also known within financial institutions as non-public personal information (NPI).

Identity theft affects thousands of individuals every year. From stolen credit card numbers and bank account information to social security numbers and passwords, PII is increasingly sold on the black market for fraud and profit. Drafting a protocol to defend against online scams is not easy because scams come in a variety of forms: phishing (where e-mails seemingly sent from legitimate organizations dupe users into surrendering PII), pharming (where poisoned Domain Name System (DNS) servers seamlessly redirect a user's browsing activity to criminally controlled sites for PII harvests) and IP spoofing (where hackers modify message packet headers to mirror trusted host IP addresses and thereby gain unauthorized access to company computers to harvest PII).

When hit by identity theft schemes, financial firms not only incur the wrath of their customers and employees who may have suffered compromised PII, they also suffer lost revenue, productivity, reputational value and the faith of their investors. Consequently, when struck by an incident of possible identity theft, financial firms should do their best, in particular, to:

a. rapidly respond to remediate existing vulnerabilities and implement processes designed to proactively prevent future theft;

b. employ suspect identification methods through packet header analysis, anomalous DNS pattern detection and the use of other robust Internet investigative methodologies;

c. employ network and systems analysis to define the universe of PII victims and the extent of PII stolen; and

d. initiate a post-incident IT infrastructure security review, design security applications to detect new intruders or anomalies, and warn customers of potential security risks and vulnerabilities.

5. Get Private. As the regulatory protections afforded PII continue to expand, so do the risks in acquiring, storing and transmitting such information. Credit card numbers, social security numbers, birthdays, medical records, and other identifying information can be housed on servers, laptops, backup tapes, cell phones, and removable media. When such devices or the data on them are misplaced, stolen, or hacked, a financial firm's exposure can be enormous. Costs can cover lost customers, forensic damage assessments, individual notifications, fines and credit monitoring services. Inadequate privacy protections are particularly important to regulatory examiners who will be looking carefully for any potential network vulnerabilities, especially if the examiners identify a failure to adopt policies and procedures that are reasonably designed to ensure the security and confidentiality of customer information.

Handling offshore data can be even more perilous. Today's financial firms travel to, and handle electronically stored information (ESI) in, the far reaches of the world, where the violation of a privacy law can result in serious sanctions and border-crossing issues. Therefore, firms should employ data experts with expertise in preparing protocols consistent with European Union or other ESI privacy standards and can work to address privacy issues. Who actually ''owns'' the data contained in a mobile telephone, or desktop/laptop computer of an employee (e.g. an Investment Adviser or its employee), is not always clear and can prompt privacy inquiries and concerns.

For instance, as one of its basic principles, the European Union data protection directive, which compels

[53] *See also*, discussion in Section IV(1) discussing Regulation S-ID.

   ISSN 0037-0665

member nations to enact national data protection laws, prohibits the processing of PII without notice to and consent of the data subject. This could arguably include the data on a cell phone or laptop computer even if that device is owned by a person's employer. Even in the United States, the law is evolving over whether a user's personal data contained on a company computer or network is protected (no matter what sort of disclaimer a company requires its employees to sign or accept as a condition of employment).

6. Choose the Right Monitoring Technologies. Financial regulators will expect firms to employ the right technologies to monitor risks associated with employees, such as a robust system to monitor, supervise, and warehouse all electronic communications of traders, analysts, and other employees (including emails, instant messages, and social networking sites). These information-reporting systems should gel nicely with SEC and other regulatory systems and allow for real-time responses to regulatory inquiries. Firms should also strive to employ the right technology to construct meaningful and effective whistleblower programs and policies, thereby preventing a small inquiry from turning into an arguably retaliatory investigation.

7. Watch Out for 'Bad Leavers' and 'Bad Stayers.' Not every data breach is the result of an unlawful intruder, some data breaches are perpetrated by insiders, which is why data breach response should avoid, if possible, drawing conclusions too quickly, and make efforts to take a more holistic approach to its investigation. Internal privacy safeguards and protocols can protect a firm and its clients against so-called ''bad leavers'' (departing employees who may cause mischief such as stealing information relating to the firm, its employees, its partners, its clients, etc.)[54] Such safeguards can also protect against rogue employees (so-called ''bad stayers''). These safeguards can include technological solutions to maintain access to traders' personal trading accounts and appropriate technological barriers to ensure that ''inside information'' is maintained in a secure and confidential manner.

8. Consider CyberInsurance. While a discussion of cyber-insurance is a large subject in and of itself, and beyond the scope of this article, the notion of cyber-insurance remains worthy of mention. Cyber-insurance can mitigate the costs of everything from hiring forensic investigators and specialized attorneys to shelling out ransoms to cyber-extortionists. In particular, as boards of directors have become increasingly concerned about exposure to cybersecurity risks, cyber-insurance is becoming more prevalent, especially among financial firms.

Just like flood, fire, and auto insurance, the idea behind cyber-insurance is to mitigate the risk and cost of a cybersecurity incident, covering issues relating to: reputation; extortion; data leakage; intrusions; breach notification and remediation; lost revenue; replacing destroyed or damaged data; the selection of an incident response firm; and a range of other business-related issues.

Indeed, the SEC's 2011 cybersecurity disclosure guidance even went so far as to advise companies regarding disclosure of cyber-insurance to shareholders, stating: ''Depending on the registrant's particular facts and circumstances, and to the extent material, appropriate disclosures may include . . . [a] description of relevant insurance coverage.''[55]

In the least, simply obtaining cyber-insurance can have beneficial consequences. For instance, before agreeing to insure a given financial firm, insurance companies typically launch an underwriting process that scrutinizes an organization's network security, privacy policies, password protection, intrusion detection, vulnerability scanning, incident response procedures, and more. Thus, the mere process of becoming cyber-insured can render a financial firm better prepared to deal with a cybersecurity incident.

9. At the First Sign of Trouble, Investigate. Prudent financial firms often hire independent consultants to conduct thorough internal investigations at the first sign of a problem, on a real-time basis (while the ability to address them internally still exists). This not only allows the firm to get its arms around a problem quickly, but it may also allow for rapid reporting of the conduct to the SEC and other regulators and law enforcement (ahead of whistle-blowers), which will put a firm in the best position to argue for leniency or no sanction at all. A policy of conducting independent investigations should also satisfy regulatory examiners who will not only ask specifically about complaints from clients and employees but also about the policies and procedures in place to address those complaints.

VI. Some Investigative Tips: Identify, Preserve, Assess, Search and Remediate

A cybersecurity investigation consists of a very technically minded iterative process, with an eye toward complete discovery of the scope of any computer compromise. Full-scope discovery means identifying all of the compromised accounts, computer systems, and information stores. Failure to identify full-scope could dramatically affect the firm's ability to make informed decisions about notification, disclosure and remediation, in addition to potentially leaving the systems vulnerable to a follow-on breach.

This iterative process consists of the following five sequential actions: Identify, Preserve, Assess, Search and Remediate.

1. Identify: The investigation may have sprouted from a customer who complained that his or her data was used for a fraud or maybe a computer system was found to be communicating with an unscrupulous internet address. Either way, this initial information should be used to identify the likely locations of evidence. Time will be saved in this phase if the investigator is already familiar with the computer network and has an accurate map of the systems and what they store. An investigator should consider all computer devices as likely locations to target for investigation. These devices should include:

a. company laptops and workstations;

[54] The term ''bad leaver'' likely comes from Great Britain, where my British colleagues have handled so many of these insider threat-related situations, that they coined a term for them.

[55] CF Disclosure Guidance, *supra* note 3.

b. network storage servers;

c. firewalls;

d. intrusion detection systems (IDS);

e. webservers;

f. customer databases; and

g. e-mail servers.

2. Preserve: Once the location of potential evidence is determined, preservation can begin. Computer systems will likely need full ''bit-for-bit'' forensic images collected.[56] Other systems (such as firewalls and IDS systems) will need their logs collected. Financial firms in particular should try to be comprehensive when preserving potentially relevant data, especially given that a failure to preserve data later deemed relevant could result in heightened scrutiny (or even skepticism) by regulators and law enforcement. In an abundance of caution, the team may want to lean toward ''over-preservation,'' even if the data is likely never to be analyzed.

3. Assess: Forensic analysis of the preserved data should be performed to assess what data may have been compromised. In addition, forensic analysis can determine the existence of additional data artifacts, remnants, and fragments that can prove relevant in the search phase. These artifacts can include:

a. internet addresses;

b. computer names;

c. malicious file names;

d. system registry data;

e. user account names; and

f. network protocols.

4. Search: Digital forensic investigators can then use the data artifacts found relevant to a breach to identify further locations within the firm's computer system that may contain additional relevant data. Investigators can identify and locate this data through inspection of network devices, logs and scanning of hosts. If the searching yields additional systems, the team needs to return to the preservation phase. Once the search determines no additional potential systems, the team can turn toward full analysis and remediation.

5. Remediate: Remediation can mean rebuilding compromised systems; implementing patches; resetting compromised user accounts; and enforcing targeted employee education. Remediation is a continual process and investigators can perform remediation as they identify further vulnerabilities. The more informed about the scope of compromise, the better the team can perform effective remediation actions; however, delaying remediation can look suspicious, so the team should not to wait too long before taking action to enhance the security of the firm's customer data

VII. Conclusion

The time is now. Not just for financial firms to assess their cybersecurity capabilities, but also for them to organize, prepare, initiate and/or refresh cybersecurity plans, practices, procedures and capabilities. Now more than ever, financial firms need to answer to a new era of increased regulation, unprecedented regulatory scrutiny, and a more powerful, better-organized and well-equipped SEC enforcement division and FINRA enforcement department.

Firms inclined to take a wait-and-see approach to the upcoming cybersecurity regulatory onslaught should reconsider; by lingering and failing to make changes, financial firms not only place their enterprises at risk of unlawful infiltration and exfiltration, but also risk:

- prompting an OCIE or FINRA enforcement referral, leading to an SEC or FINRA enforcement investigation;
- stifling the attraction of new investors; and/or
- causing existing investors to flee.

Without a doubt, the havoc wreaked upon a financial firm by a cyber-attack is bad enough without the additional strain of a regulatory deficiency letter regarding cybersecurity, or even worse, a string of federal or regulatory subpoenas probing cyber-preparedness and response.

[56] It is important to note that the concept of ''materiality'' does not apply in digital forensics. The slightest amount of data can have huge importance, hence the need for comprehensive forensic preservation.

   ISSN 0037-0665