Few topics are as hot as cybersecurity. Recent high-profile data breaches at national retailers have made cybersecurity a frequent topic on Capitol Hill and an issue of growing concern to average Americans. Not surprisingly, securities regulators have also begun to focus on cybersecurity in the financial services industry.¹

On March 26, 2014, the U.S. Securities and Exchange Commission (SEC) held a Cybersecurity Roundtable that gathered representatives from the Department of Treasury, the Department of Homeland Security, self-regulatory organizations (including FINRA and several exchanges), and the private sector to discuss cybersecurity threats and responses with the Commissioners and senior SEC staff members.² More recently, on April 15, the SEC Office of Compliance Inspections and Examinations (OCIE) published a risk alert on cybersecurity.³ The alert announced that as part of a “Cybersecurity Initiative” OCIE will be examining more than 50 registered broker-dealers and investment advisers.⁴ Cybersecurity is also high on FINRA’s agenda. FINRA recently identified cybersecurity as a “priority” in its examination priorities letter for 2014.⁵ Like the SEC, FINRA is also conducting sweep examinations of cybersecurity systems, procedures and practices. This article explores the current cybersecurity regulatory landscape for broker-dealers and investment advisers; the scope of the ongoing SEC and FINRA cybersecurity sweep examinations; relevant enforcement actions brought by the SEC and FINRA; and possible future areas of regulatory and enforcement activity relating to cybersecurity.

1. The Cybersecurity Regulatory Landscape
   a. Regulation S-P

The cornerstone of the cybersecurity regulatory landscape is Regulation S-P. Rule 30 of Regulation S-P (referred to as the “Safeguard Rule”) requires registered broker-dealers, investment advisers and investment companies to establish written policies and procedures reasonably designed to “(a) [i]nsure the security and confidentiality of customer records and information; (b) [p]rotect against any anticipated threats or hazards to the security or integrity of customer records and information; and (c) [p]rotect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.”⁶ In 2008, the SEC proposed amendments to Regulation S-P. Those amendments – which have never been adopted or withdrawn – would require broker-dealers, investment advisers, investment companies and transfers agents to, among other things, “develop, implement, and maintain a comprehensive information security program.”⁷ The comprehensive information security program would have to, among other things, (a) identify reasonably foreseeable internal and external risks to personal information and personal information systems; (b) implement controls against...
those risks; (c) test regularly the effectiveness of those safeguards; (d) respond to unauthorized access of personal information by investigating the nature and scope of the incident and taking steps to contain the incident and prevent further unauthorized access; and (e) notify individuals when their personal information has been accessed or used. While the SEC never adopted these proposed amendments, the proposal nonetheless provides useful guidance on the proper scope of cybersecurity programs.

1. FINRA Rules and Guidance

FINRA reviews broker-dealers’ cybersecurity programs and procedures for compliance with its supervision rules, including NASD Rules 3010 and 3012. NASD Rule 3010 requires member firms to establish, maintain and enforce a supervisory system and written procedures reasonably designed to ensure compliance with applicable securities laws and rules, including Regulation S-P. Pursuant to NASD Rule 3012, each member firm must establish, maintain and enforce a supervisory control system to test and verify that its supervisory procedures are reasonably designed to achieve compliance with applicable securities laws and rules, including Regulation S-P. In July 2005, FINRA (then NASD) issued a notice reminding firms of the risks associated with using technology like wireless fidelity (Wi-Fi) and remote access to firm networks through virtual private networks (VPNs) and other means. The notice instructed firms to consider whether: (a) policies and procedures adequately address the technology used; (b) appropriate technological precautions (including, for example, encryption, firewalls, filters and routers) are being used to protect customer information; (c) employees are being adequately trained about technology and the protection of customer records and information; and (d) periodic audits are or should be conducted to review for potential systems vulnerabilities and to ensure that customer information is, in practice, being protected from unauthorized access.

1. Identity Theft Rules

One specific cybersecurity issue – identity theft – has generated additional regulation. The Fair Credit Reporting Act of 1970 (FCRA), as amended in 2003, required multiple federal agencies (including the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation and others but not the SEC) to promulgate joint rules for financial institutions on the detection and prevention of identity theft. Those joint rules were adopted in 2007, and applied to various financial institutions, including broker-dealers, investment advisers and investment companies, although the SEC had no responsibility to enforce these rules. In 2010, the Dodd-Frank Wall Street Reform and Consumer Protection Act amended the FCRA to, among other things, add the SEC to the list of federal agencies that must adopt and enforce identity theft rules. Accordingly, in 2013, the SEC adopted its own identity theft red flags rules, called Regulation S-ID, for entities under its jurisdiction, including registered broker-dealers and investment advisers. The identity theft rules in Regulation S-ID parallel the rules jointly...
adopted by multiple agencies in 2007. Regulation S-ID requires, among other things, that financial institutions have reasonable policies and procedures for (a) “identify[ing] relevant red flags”; (b) detecting those red flags; (c) responding appropriately to red flags once detected; and (d) updating the identity theft program.\textsuperscript{16} Regulation S-ID became effective on November 20, 2013.\textsuperscript{17}

1. State Data Breach and Data Security Laws

No survey of cybersecurity laws would be complete without a discussion of state laws. At present, 47 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, and Guam have some form of data breach notification law.\textsuperscript{18} While these laws vary by jurisdiction, they generally require covered entities (such as broker-dealers and investment advisers) to notify individuals in the event their personal information is compromised. In addition, some laws require covered entities to notify state agencies of data breaches that exceed a specific threshold. For example, California law requires covered entities to notify the Attorney General if a single data breach compromises the personal information of more than 500 residents.\textsuperscript{19} In the event of a cybersecurity breach, broker-dealers and investment advisers should therefore consider whether applicable state laws require customer notification and/or reporting to government agencies.

A few states have established standards for the protection of residents' personal information. For example, Massachusetts requires companies that own or license personal information of its residents to create and maintain a comprehensive information security program that includes a computer security system with user authentication protocols; access control measures; encryption of all data transmitted wirelessly and/or across public networks; monitoring of systems for unauthorized access; encryption of personal information stored on laptops or other portable devices; up-to-date firewall and malware protections; and employee training.\textsuperscript{20} Thus, firms should also consider whether any applicable state laws impose substantive cybersecurity requirements.

1. Cybersecurity Examinations

Both the SEC and FINRA are engaged in active cybersecurity “sweep” examinations. OCIE published a sample cybersecurity examination document request in connection with its recent risk alert.\textsuperscript{21} In so doing, OCIE’s stated intention was that firms could use the document request in evaluating their “level of preparedness.”\textsuperscript{22} The document request addresses various cybersecurity issues, including:

- Cybersecurity governance (including, for example, written policies and procedures; periodic risk assessments of cybersecurity threats and vulnerabilities; cybersecurity insurance; and the allocation and communication of cybersecurity responsibilities to firm personnel);

- Protection of firm networks and information (including, for example, user
access restrictions; system maintenance; data destruction policies; cybersecurity incident response plans; security of removable and portable media; backup system testing; encryption; employee guidance and training; and periodic audits for compliance with information security policies);

• Risks associated with customer on-line account access and email funds transfer requests (including, for example, customer authentication, detection of anomalous trade requests; and protection of stored personal identification numbers);

• Risks associated with vendors and outsourcing (including, for example, how cybersecurity risks are addressed in vendor contracts; vendor training; and cybersecurity risk assessments of vendors);

• Detection of unauthorized activity (including, for example, monitoring for potential cybersecurity incidents; amassing and correlating data on cybersecurity incidents; detecting malware and malicious code on networks and devices; detecting unauthorized users, devices, connections, and software on the firm’s network; and using data loss prevention software); and

• Cybersecurity breaches (including, for example, malware; denial-of-service attacks; unauthorized network access; fraudulent emails attempting to transfer customer funds or securities; software or hardware malfunctions that impair network or web resources; and theft, loss, or unauthorized use or access to customer information) and the firm’s responses thereto.23

FINRA’s cybersecurity sweep examinations cover many of the same issues as the SEC’s examinations, including: information technology risk assessment; business continuity plans in the event of a cyber-incident; organizational structures and reporting lines; sharing and evaluating cyber threat information; cybersecurity breaches in the past years and their consequences; responding to denial of service attacks; cybersecurity training; cybersecurity insurance; and vendor contracts.24 Thus, both regulators appear to be in agreement that these issues represent important cybersecurity considerations.

1. Cybersecurity Enforcement Actions

Both the SEC and FINRA have brought cases against firms for cybersecurity-related failures. As shown below, past cybersecurity enforcement actions involved many of the same issues addressed in the SEC’s and FINRA’s ongoing sweep examinations.

1. Cybersecurity Governance

Securities regulators have taken enforcement actions against firms based on cybersecurity governance failures, including: (i) inadequate written policies and procedures; (ii) failing to enforce written policies and procedures; (iii) failing to
conduct periodic assessments of cybersecurity procedures and measures; and (iv) failing to respond to deficiencies identified through such periodic assessments.

1. **Inadequate Written Cybersecurity Policies and Procedures**

In multiple enforcement actions, the SEC and FINRA have sanctioned firms for having cybersecurity policies and procedures that failed to comply with the Safeguard Rule and other requirements. Specifically, the regulators have found those policies and procedures to be deficient because they:

1. Provided “limited and insufficient” guidance, rather than a “complete set of... policies and procedures addressing administrative, technical and physical safeguards reasonably designed to protect customer records and information”;\(^{25}\)

2. Contained recommendations or suggestions, rather than mandates;\(^{26}\)

3. Were “less than a page long,” “general[,] and vague”;\(^{27}\)

4. Were “generic in that they required employees to secure all non-public financial information”;\(^{28}\)

5. Simply recited the Safeguard Rule and provided examples of safeguards that “may be adopted,” rather than the firm’s actual safeguards;\(^{29}\)

6. Failed to address sufficiently the technology in use because non-public customer information stored on laptops was not protected by encryption or other appropriate technology;\(^{30}\)

7. Failed to instruct registered representatives how to protect customer information and what to do in the event of a breach;\(^{31}\)

8. Failed to ensure that laptops were protected by encryption or other suitable technology;\(^{32}\)

9. Failed to address how to respond to breaches or potential breaches;\(^{33}\)

10. Failed to address the security of the firm’s proprietary trading platform;\(^{34}\)

11. Failed to employ adequate safeguards to detect, review for, and report breaches involving non-public customer information;\(^{35}\)

12. Failed to address how to respond to network intrusions;\(^{36}\)

13. Failed to require the review of web server logs to detect potential
intrusions;\textsuperscript{37}

14. Recommended, but did not require, the installation of antivirus software on computers its registered representatives used to access its clearing firm’s proprietary trading system;\textsuperscript{38}

15. Failed to require reviews of registered representatives’ computer security measures;\textsuperscript{39}

16. Failed to address how to respond or follow up on cybersecurity issues detected through branch audits;\textsuperscript{40} and

17. Failed to require appropriate follow-up on potential cybersecurity issues reported to the firm’s information technology (IT) help desk.\textsuperscript{41}

\begin{itemize}
\item a. Failure to Enforce Cybersecurity Policies and Procedures
\end{itemize}

The SEC and FINRA have also brought cases against firms for failing to follow or enforce their written cybersecurity policies and procedures. In one example, the SEC brought an enforcement action against the former chief compliance officer (CCO) of a now-defunct broker-dealer because, among other things, the firm’s procedures tasked a “Designated Principal” with critical cybersecurity tasks, including monitoring and testing of the firm’s safeguards, but the CCO never named or appointed such a person.\textsuperscript{42} In another case, FINRA charged a broker-dealer with, among other things, violating Rules 3010 and 2110 by failing to comply with its written procedures requiring quarterly reviews of internal computer systems and privacy protections.\textsuperscript{43} In that case, FINRA emphasized that those quarterly reviews, had they been conducted, would have revealed that the firm failed to install “essential monitoring software” on the computers of at least 19 employees.\textsuperscript{44} FINRA also disciplined a firm for failing to enforce its (a) “strong” password requirement through validation; and (b) requirement that passwords be changed every six months through mandatory password changes or expiration.\textsuperscript{45} Thus, firms may be disciplined not only for failing to follow their written cybersecurity procedures, but also for failing to establish appropriate controls to enforce their written cybersecurity procedures.

1. Failure to Conduct Adequate Periodic Cybersecurity Assessments

Regulators have taken enforcement actions against firms for failing to perform sufficient periodic assessments of cybersecurity procedures and measures. In a settled administrative proceeding, the SEC found that a registered broker-dealer, investment adviser and transfer agent failed to assess the security of its proprietary trading system, despite conducting vulnerability testing of other systems and despite experiencing a data breach.\textsuperscript{46} In another example, FINRA found that a firm’s periodic audits were inadequate because they did not review laptops to ensure they were protected by appropriate technology.\textsuperscript{47} Therefore, when firms conduct cybersecurity assessments, they may want to review both the technology in use and the means available to monitor and protect that
1. Failure to Respond to Cybersecurity Deficiencies

Several cases demonstrate that when cybersecurity deficiencies are detected, firms may be sanctioned if they fail to take timely corrective action. The SEC brought an enforcement action based, in part, on a firm’s failure to take corrective action in response to an internal audit report finding deficiencies in the firm’s password requirements and system inactivity parameters for its proprietary trading system. The SEC seemed particularly troubled by the firm’s failure to act, even though the internal auditors emphasized that these deficiencies posed an increased risk of account intrusions and unauthorized access to non-public customer information. In another case, the SEC found that a dually registered broker-dealer and investment adviser violated the Safeguard Rule by, among other things, failing to respond to cybersecurity issues detected through branch audits or reported to the firm’s IT help desk. FINRA has also disciplined firms on this basis. In one settlement, FINRA charged a broker-dealer for failing to adopt a recommendation by an independent auditor and outside security consultant that the firm implement an intrusion detection system. Thus, firms may be found liable if they fail to address any cybersecurity deficiencies detected through internal reviews, internal processes (such as through help desks), and external reviews.

1. Protection of Firm Networks and Customer Information

Firms have also drawn regulatory ire by failing to protect networks and non-public customer information with appropriate technology (including encryption, antivirus software and firewalls) and reasonable procedures (including user access restrictions).

1. Encryption

FINRA has brought disciplinary action against two firms for, among other things, failing to encrypt non-public customer information and thus exposing such information to the risk of unauthorized access. In a case involving a stolen firm laptop, FINRA charged the firm for failing to encrypt “sensitive” customer information stored on the laptop (which included, among other things, social security numbers and customer bank account numbers). In another case, FINRA sanctioned a firm for, among other things, failing to encrypt a database containing non-public customer information, even though it was exposed to the Internet via a persistent Internet connection. Although the regulators have yet to proclaim that encryption is a universal requirement, these disciplinary actions suggest that FINRA may view encryption as necessary to protect non-public customer information under certain facts and circumstances.

1. Antivirus Software

The SEC and FINRA have focused on the protection of registered
representatives’ computers with antivirus software. Relevant cases include:

- The SEC charged a dually registered broker-dealer and investment adviser because, among other things, its procedures recommended – but did not require – that its registered persons install antivirus software on their computers;  

- FINRA disciplined a member firm based, in part, on its failure to implement its written procedures requiring quarterly reviews of internal computer systems, when such reviews would have detected the firm’s failure to install “essential monitoring software” on the computers of at least 19 employees;  

- FINRA disciplined another firm for, among other things, failing to (1) mandate that field representatives install antivirus software on representative-owned computers used to conduct firm business; and (b) review such computers to verify that the antivirus software had, in fact, been installed.  

Thus, firms should consider requiring installation of antivirus software on registered representatives’ computers and monitoring (likely through internal audits) to ensure the installation has been completed.

1. **Firewalls**

FINRA disciplined a firm, in part, because it improperly configured its firewall such that unauthorized persons could attempt to access its fax server, which housed faxes transmitted from field representatives to the firm’s home office, many of which contained non-public customer information. As a result, FINRA found that the firm violated the Safeguard Rule and NASD Rule 3010. Thus, regulators may view an improperly configured firewall as a violation of the Safeguard Rule.

1. **User Access Restrictions**

Securities regulators have been very active in sanctioning firms for failing to implement adequate password requirements. The failures range from failing to require any password to failing to require a “strong” password. The regulators have found the following practices to be violative:

- Failing to require a password to access a firm database containing non-public customer information, even though the database was connected to the Internet via a persistent connection;  

- Using a generic user name (“Administrator”) and password (“password”) to access a firm database containing non-public customer information;  

- Failing to protect sufficiently the firm’s electronic portfolio management
system by (a) allowing employees to share login credentials; (b) failing to track who accessed the system and when; (c) failing to require that user names and passwords be changed on a regular basis; and (d) failing to disable user names or passwords after employees left the firm;60

• Failing to take adequate corrective measures in response to an internal audit identifying as deficiencies the firm’s failure to require “strong” passwords for its proprietary trading system because the firm did not require (a) a minimum password length; (b) a complex password involving an alphanumeric/special character combination; (c) expiration of passwords after a certain time period; and (d) automatic lockout after failed login attempts;61 and

• Requiring “strong” passwords to be changed every six months to access firm laptops, but failing to enforce those requirements through validation or mandatory password expiration.62

Thus, regulators apparently believe that appropriate user access restrictions for certain firm systems containing non-public customer information should include, at a minimum: (a) requiring that passwords exceed a specific length and include an alphanumeric/special character combination; (b) setting passwords to expire after a set period of time and requiring a password change; (c) prohibiting sharing of user names and passwords; (d) locking out a user after a set number of unsuccessful logins; and (e) disabling user names and passwords after employees or registered persons leave the firm.

1. Cybersecurity Issues Associated with Vendors and Outsourcing

Regulators have also shown interest in cybersecurity risks involving vendors and outsourcing relationships. In particular, regulators are concerned about the protection of non-public customer information shared with third-party vendors. For example, FINRA brought a case against a firm that shared confidential customer information with a third-party vendor without first providing opt-out notices to the affected customers, when the vendor accidentally posted some non-public customer information on the Internet.63 The firm’s procedures permitted disclosure of non-public customer information to non-affiliated third parties (such as vendors) only when (a) the information was necessary to perform services for the firm; (b) the vendor was contractually required to maintain confidentiality of such information; and (c) the customer was given an opportunity to opt out from the disclosure.64 FINRA cited the firm for failing to ensure adherence to these procedures and failing to monitor and detect when third parties are in possession of non-public customer information.65 In another case, FINRA disciplined a firm for, among other things, “fail[ing] to establish policies and procedures that address and review the administrative, technical, and physical safeguards for the protection of customer records and information involved in” its outsourcing relationship with a non-affiliate that provided compliance and operations functions (including storing documents containing
non-public customer information) for the firm.\textsuperscript{66}

1. Inadequate Responses to Cybersecurity Breaches

Firms have been sanctioned for failing to respond adequately to cybersecurity breaches. Examples include:

- A registered broker-dealer, investment adviser and transfer agent failed to implement enhanced security measures and procedures, despite experiencing a series of “hacking” incidents;\textsuperscript{67}

- A registered broker-dealer failed to employ adequate safeguards to ensure that data breaches involving confidential customer information were reported to the Compliance Department and Privacy Officer, as required by the firm’s procedures;\textsuperscript{68}

- A registered broker-dealer failed to investigate a data breach and sent inaccurate notifications to customers and registered representatives concerning the data breach;\textsuperscript{69} and

- The CCO of a broker-dealer failed to enhance cybersecurity policies and procedures, despite being aware of three stolen laptop computers (one of which contained confidential customer information) and a representative’s misappropriated email access credentials.\textsuperscript{70}

Regulators therefore appear to be paying close attention to how firms respond to data breaches, including how firms improve their systems and procedures with a view towards preventing the recurrence of similar data breaches.

1. Future Cybersecurity Regulatory and Enforcement Activity

All signals indicate that additional cybersecurity regulation and increased cybersecurity-related enforcement actions are on the horizon. Chief among those signals are statements made by representatives of the SEC and FINRA at the recent Cybersecurity Roundtable. SEC Commissioner Luis Aguilar stated that he expected the SEC would consider the information gathered at the Roundtable, and then “with appropriate haste, [would] consider what additional steps the Commission should take to address cyber-threats.”\textsuperscript{71} In addition, the Roundtable concluded with David Grim, Deputy Director of the Division of Investment Management, asking participants in the Broker-Dealers, Investment Advisers and Transfer Agents panel what actions the SEC should take in this area. The panelists urged the SEC that any cybersecurity regulation should be principles-based, rather than prescriptive, and should take into account variables such as firm size and business model. It remains to be seen whether the SEC will heed this advice. However, it seems likely that the SEC will issue cybersecurity regulation or guidance in the near future.

The Roundtable also provided insight into FINRA’s possible approach
to cybersecurity regulation. Daniel Sibears, Executive Vice President of FINRA, stated that FINRA intends to use the information it gleans from its cybersecurity sweep examinations to publish “best practices” guidance. This guidance should be helpful to firms struggling with how to identify and implement cybersecurity systems and procedures that will pass regulator muster.

The best predictor of future cybersecurity enforcement activity is past enforcement activity. Several lessons emerge from a review of past cybersecurity enforcement actions. These lessons provide insight into the potential nature and scope of future enforcement actions in this area. The following are possible avenues the SEC and FINRA may take when they bring enforcement actions:

• Future SEC and FINRA cybersecurity enforcement actions may be based on violations of the Safeguard Rule. Among the specific issues the regulators are likely to focus on are: adequacy of cybersecurity policies, procedures and controls; a firm’s compliance with its cybersecurity policies and procedures; adequacy of periodic assessments of cybersecurity policies, procedures and controls; responding appropriately and promptly to any cybersecurity deficiencies detected; protecting non-public customer information with suitable technology and strong user access restrictions; protecting non-public customer information shared with vendors; and responding appropriately to data breaches.

• Many future cybersecurity enforcement actions will likely be based on actual data breaches. Of the past enforcement actions discussed in this article, seven of 11 (or 64%) involved actual data breaches, rather than just vulnerabilities that could have resulted in breaches. In this regard, the regulators may assert that a firm that experiences an actual data breach failed, by definition, to comply with the Safeguard Rule.

• Actual customer harm is not required, however, the regulators may still bring enforcement actions in cases where non-public customer information has been exposed to unauthorized access, even if the information was not actually misused.

• Responding promptly and appropriately to cybersecurity breaches may not be enough to prevent an enforcement action. However, regulators should consider remedial efforts in assessing sanctions.

• Future cybersecurity enforcement actions may result in significant fines. The fines imposed against broker-dealers and investment advisers in the cases examined in this article range from low-to-mid six figures (specifically, $100,000 to $450,000). The only exception is a $27,500 fine imposed against a small firm (with only five registered persons and five associated persons) for a procedural violation without any customer harm.

In addition to Regulation S-P violations, the SEC will also likely be
reviewing identity theft procedures and practices in the near future, which could lead to enforcement activity. As discussed above, Regulation S-ID recently became effective.

1. Conclusion

Cybersecurity is and will continue to be a “hot” regulatory issue for the foreseeable future. The threat of cyber attacks is rising, not diminishing. As the threat grows, regulatory interest is likely to expand. In addition, as data breaches continue to generate headlines, regulators will likely face mounting pressure from Congress and the public to act in this area. Future regulatory and enforcement actions are therefore anticipated. Make sure your seat belt and cyber belt are securely fastened.

---

1The regulators have also been forced to focus on their own conduct. For example, on April 17, 2014, the U.S. Governmental Accountability Office issued a report about the SEC’s need to improve controls over financial systems and data. http://www.gao.gov/products/GAO-14-419. A few years ago, at NASD’s Boca Raton district office, 10 laptop computers were stolen, “rais[ing] questions about how financial regulators protect customer data.” http://www.investmentnews.com/article/20060706/REG/607060707#.


4Id. at 2.


617 C.F.R. § 248.30(a) (2014).


8Id. at 94-98

9NASD Rule 3010 will be superseded by FINRA Rule 3110 effective December 1, 2014. Like NASD Rule 3010, FINRA Rule 3110 will require firms to, among other things, establish, maintain and enforce systems and procedures reasonably designed to achieve compliance with applicable securities laws and rules, including Regulation S-P. FINRA Regulatory Notice 14-10: SEC Approves New Supervision Rules; Effective Date: December 1, 2014, at 1-2, 4 (March 2014), available at http://finra.complinet.com/en/display/display.html?rbid=2403&element_id=11470.

10NASD Rule 3012 will be superseded by FINRA Rule 3120 effective December 1, 2014. Like NASD Rule 3012, FINRA Rule 3120 will require firms to, among other things, test and verify that their written procedures are reasonably designed to achieve compliance with applicable securities laws and rules, including Regulation S-P. FINRA Regulatory Notice 14-10, supra note 6, at 15.

11NASD Notice to Members 05-49: Safeguarding Confidential Customer Information, at 2-3 (July 2005), available at
Legal Alert: Cybersecurity Issues in the Financial Services Industry: Fasten your cyber belts, it's going to be a bumpy night

continued


12Id. at 4.


14Id. at 5.

15Id. at 7.

16Id. at 30-31.

17Id. at 2.


19Cal. Civil Code § 1798.29(e).

20201 CMR §§ 17.03-17.04.

21OCIE National Exam Program Risk Alert, supra note 2, at 2.

22Id.

23Id. at 3-7.


32Letter of Acceptance, Waiver and Consent No. 2009019893801, at 10 (Nov. 21, 2011) (finding that the firm


35 Letter of Acceptance, Waiver and Consent No. 2010022554701, at 2, 5 (Apr. 9, 2012) (finding that the firm violated the Safeguard Rule and NASD Rules 3010(a) and (b)), available at http://disciplinaryactions.finra.org/.

36 FINRA Letter of Acceptance, Waiver and Consent No. 2008015299801, at 2-3 (Apr. 9, 2010) (finding that the firm violated the Safeguard Rule and NASD Rules 3010(a) and (b)), available at http://disciplinaryactions.finra.org/.

37 FINRA Letter of Acceptance, Waiver and Consent No. 2008015299801, at 2-3 (Apr. 9, 2010) (finding that the firm violated the Safeguard Rule and NASD Rules 3010(a) and (b)), available at http://disciplinaryactions.finra.org/.


44 Id.


63Id. at 3.

64Id.


68FINRA Letter of Acceptance, Waiver and Consent No. 2007009780901, at 5-7 (Apr. 28, 2009), available at http://disciplinaryactions.finra.org/. The AWC mentions that state law required notification, but does not say the firm violated state law.

69Commissioner Luis Aguilar, The Commission’s Role in Addressing the Growing Cyber-Threat (March 26, 2014), continued
Legal Alert: Cybersecurity Issues in the Financial Services Industry: Fasten your cyber belts, it’s going to be a bumpy night

available at http://www.sec.gov/News/PublicStmtDetail/PublicStmt/1370541287184#.U0MNFRjD_IU.

1Letter of Acceptance, Waiver and Consent No. 2010022554701, at 3-5 (Apr. 9, 2012) (two customers given online viewing access to accounts of unrelated customers and one customer sent account statements for unrelated accounts); Letter of Acceptance, Waiver and Consent No. 2009019893801, at 9-10 (Nov. 21, 2011) (laptop containing non-public information for 37,864 customers stolen from an employee’s car); FINRA Letter of Acceptance, Waiver and Consent No. 2008015299801, at 3 (Apr. 9, 2010) (hacker accessed non-public customer information for 192,000 customers and attempted to blackmail the firm); Exchange Act Release No. 60733, Admin. Proc. File No. 3-13631, at 2 (Sept. 29, 2009) (hacker accessed 368 customer accounts and entered trades in eight customer accounts); FINRA Letter of Acceptance, Waiver and Consent No. 2007009780901, at 2 (Apr. 28, 2009) (firm’s failure to protect its fax server allowed a hacker to use the server to host a phishing scheme); Exchange Act Release No. 58515, Admin. Proc. File No. 3-13181, at 3 (Sept. 11, 2008) (unauthorized persons gained access to the firm’s proprietary trading platform and attempted to place 209 unauthorized trades in 68 customer accounts).

2But see FINRA Letter of Acceptance, Waiver and Consent No. 2009015980301, at 6 (Dec. 14, 2012) (firm failed to comply with its written procedures requiring quarterly reviews of computer systems and privacy protections); FINRA Letter of Acceptance, Waiver and Consent No. 20100239953, at 3-4 (Sept. 13, 2012) (firm’s vendor inadvertently posted customers’ non-public information on the Internet, but no evidence that identify theft or other customer harm resulted); FINRA Letter of Acceptance, Waiver and Consent No. 2009018720501, at 4-5 (Feb. 16, 2011) (firm’s system containing customer account information was put “at risk,” but an outside consultant found no evidence of an actual breach); FINRA Letter of Acceptance, Waiver and Consent No. 2009016196001, at 4 (Feb. 18, 2010) (firm failed to protect non-public customer information shared in connection with an outsourcing relationship).

3FINRA Letter of Acceptance, Waiver and Consent No. 2010022554701, at 3-5 (Apr. 9, 2012) (customers given unauthorized access to the accounts of other customers, but information apparently not misused); FINRA Letter of Acceptance, Waiver and Consent No. 20100239953, at 3-4 (Sept. 13, 2012) (vendor inadvertently posted non-public customer information on the Internet, but no customers suffered identity theft or other actual harm as a result); Letter of Acceptance, Waiver and Consent No. 2009019893801, at 9-10 (Nov. 21, 2011) (non-public customer information put “at risk,” but not misused, when a laptop was stolen from an employee’s car); FINRA Letter of Acceptance, Waiver and Consent No. 2009018720501, at 4-5 (Feb. 16, 2011) (firm’s system containing customer account information put “at risk,” but an outside consultant found no evidence of an actual breach).

4FINRA fined firm $375,000 where a hacker downloaded confidential information for 192,000 customers and attempted to extort the firm – even though no customer was actually harmed as a result – and the firm reported the incident to law enforcement and cooperated in the subsequent investigation that led to multiple indictments; notified impacted customers and offered them free credit monitoring; settled a related class action suit; hired an outside firm to advise on cybersecurity; imposed an additional firewall, added intrusion prevention software; and upgraded the relevant server to the latest encryption software); Exchange Act Release No. 60733, Admin. Proc. File No. 3-13631, at 2-6 (Sept. 29, 2009) (SEC imposed a $100,000 civil money penalty on dually registered broker-dealer and investment adviser that responded to a hacker viewing non-public customer information for 368 accounts and executing 18 unauthorized trades in eight customer accounts by cancelling the unauthorized trades, absorbing the resulting loss, notifying the affected accountholders, and self-reporting the breach to the SEC).


If you have any questions about this Legal Alert, please feel free to contact any of the attorneys listed under ‘Related People/Contributors’ or the Sutherland
attorney with whom you regularly work.