Client Alert

January 10, 2014

Broker-Dealer Cybersecurity: Protect Yourself or Pay the Price

By Daniel A. Nathan and Ana-Maria Ignat

In its recently issued 2014 Regulatory and Examination Priorities Letter, FINRA stated that cybersecurity remains a priority given the ongoing cybersecurity issues reported across the financial services industry, including the increasing frequency and sophistication of attacks targeting the nation's largest financial institutions. The securities industry watchdog continues to be concerned with the integrity of firms' infrastructure and the safety and security of sensitive customer data. Broker-dealers are well-advised to ensure that their data security systems and procedures are up-to-date, since the financial and, more important, reputational impacts of adverse examination findings or enforcement actions can be devastating.

THE REGULATION

The applicable regulatory framework governing broker-dealer cybersecurity includes the SEC's Regulation S-P (Privacy of Consumer Financial Information).[1] Specifically, Rule 30 (the so-called Safeguards Rule) requires brokers, dealers, investment companies and investment advisers registered with the Commission to:

- adopt reasonably designed written policies and procedures addressing administrative, technical and physical safeguards for the protection of customer information and records; and
- protect against any anticipated threats or hazards to the security or integrity of customer records and information, and against unauthorized access to or use of customer records or information. [2]

THE EXAM FOCUS

Over the past six years, FINRA's examination priorities have consistently included cybersecurity, data integrity and customer information protection issues. FINRA's examination program looks for potential deficiencies in broker-dealers' procedures in the cybersecurity area, and when an actual breach occurs, FINRA's enforcement program has taken formal disciplinary action, requiring remediation and imposing severe penalties. This year, as in 2013, broker-dealers should expect that FINRA's examiners will focus on the integrity of firms' policies, procedures and controls to protect sensitive customer data, and that findings of significant gaps could lead to investigations or enforcement action.

---

[1] Regulation S-P became effective in November 2000, and compliance with the rules and regulations has been mandatory since July 1, 2001. The requirement that policies and procedures be written has been in place since 2005.

[2] In July 2005, the National Association of Securities Dealers ("NASD"), FINRA's predecessor, reminded its members of their obligations relating to the protection of customer information: www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p014772.pdf. FINRA has also published a list of steps a firm may need to take when it learns that its customers' accounts may have been compromised: http://www.finra.org/industry/issues/customerinformationprotection/p117443

Since 2010, FINRA has conducted thematic reviews in the areas of technology and cybersecurity, and identified these examples of strong controls:

- structured governance over application risk classification and controls;
- robust IT organizations interacting with all areas and facets of the firm;
- full encryption policies and practices for all devices, including those utilized outside the firm;
- independent reviews and testing of operating systems and security; and
- strong user credential requirements and management.

On May 22, 2012, a session of FINRA's annual conference was dedicated to customer protection issues, including a discussion of applicable requirements, recent enforcement activity and industry practices. At the February 25, 2013, meeting of the SRO Subcommittee of the ABA Securities Litigation Committee, FINRA's senior officials Susan Axelrod and Michael Rufino observed that, in the cybersecurity area, FINRA is especially concerned about smaller firms, as exams have shown particular vulnerability in technology systems, with problems that include expired or ineffective anti-viral software. In addition, in the event of a successful cyber-attack, the financial constraints of a small firm may be significant and impair the firm's ability to compensate the victims. In June 2013, during an event hosted by the Insured Retirement Institute, FINRA senior official Daniel Sibears reported that FINRA had seen a proliferation of complaints about cybersecurity breaches at broker-dealer firms, which makes cybersecurity a big issue for FINRA.

Of even greater concern than the potential regulatory penalties and other sanctions that FINRA or the SEC may impose is the potential damage to a broker-dealer's reputation and the loss of client confidence as a result of a data breach.

FINRA ENFORCEMENT ACTIONS

Although FINRA has brought relatively few enforcement actions in the cybersecurity and customer information protection area, the matters it chose to pursue illustrate the focus of its inquiries. FINRA's enforcement actions have found violations in the following areas:

- **Policies and procedures**
    - The failure of a broker-dealer to adopt written procedures setting forth an information security program designed to respond to intrusions;
    - The failure to establish procedures mandating that employees install anti-virus software and other protection on their computers; and
    - The failure to implement procedures for the encryption of laptops or data stored on laptops.
- **Encryption, password protection, and anti-virus and security software**
    - The failure to use a properly configured computer firewall;
    - The failure to audit employee computers to confirm the installation of security software;

- The failure to monitor for potential or actual breaches;
- The failure to enforce the mandated use of strong passwords through validation or periodic password changes and a forced password expiration;
- The failures to employ effective usernames and passwords, or to place controls and procedures on the use and dissemination of the usernames and passwords;
- The failure to review web server logs revealing intrusions;
- The failure to implement appropriate encryption measures;
- Allowing employees to share computer sign-on credentials to access files which contained confidential customer information; and
- Storing a database containing customer information on a computer with a persistently open Internet connection which left the information in the database exposed to the internet.

- **Training, audits and consultant recommendations**
  - The failure to perform sufficiently broad periodic audits to protect customer records and other sensitive information from unauthorized access;
  - The failure of a firm to carry out the security recommendations of independent auditors and outside security consultants for an intrusion detection system; and
  - The failure to provide adequate training to employees regarding customer breaches, leading to the failure of certain employees to recognize that an unauthorized customer account data breach had occurred and that the breach had to be reported to the firm's compliance department and privacy officer.
- **Customer notifications**
  - The failure to provide customers with an opt-out notice prior to disclosing their information to the nonaffiliated third party; and
  - Sending misleading notification letters to affected customers and their brokers.

Significantly, in all of these cases, FINRA imposed relatively high penalties – between $150,000 and $450,000 – and required extensive and often expensive remedial measures, including making needed hardware and software upgrades, revising written supervisory procedures, implementing data security policies and various related protocols, engaging third-party consultants to review information security systems, providing notifications to customers, offering customers the services of a nationally-recognized credit monitoring service free of charge, and resolving related class action litigation.

Some of these cases are instructive.

In one case, a firm used a public-facing computer web server that also housed a database containing confidential customer information. The database was stored in a computer with a persistent Internet connection, which left the customer information in the database exposed to the internet. In addition, the firm failed to encrypt the database or activate a password, and the lack of encryption in the database exacerbated the vulnerability of the confidential customer information. The firm's failure to adequately secure customer information ultimately led to actual customer harm when a third party downloaded the confidential customer information through a sophisticated network intrusion. The firm only learned of the breach through an email sent by the hacker. Although the attacks were visible on web server logs, the firm failed to review those logs. The firm did not have any written procedures for the review of web server logs, nor an intrusion detection system. Even if it had detected the intrusion, the firm did not have written procedures setting forth an information security program designed to respond to intrusions. The firm also failed to carry out the recommendation of independent auditors and outside security consultants that it implement an intrusion detection system. FINRA concluded that the firm's systems and procedures were not reasonably designed to safeguard customer records and information, in contravention of Regulation S-P, supervisory deficiencies which ultimately contributed to the hacker's ability to obtain the confidential customer information of approximately 92,000 firm customers. FINRA required the firm to take numerous remedial steps after the intrusion, including taking down its website, reporting the incident to law enforcement, providing written notice to affected customers and voluntarily offering affected customers a subscription to a credit-monitoring service for two years at a cost of $1.3 million to the firm. The firm also paid a $375,000 fine.

In another case, FINRA found that for seven years a broker-dealer failed to adequately protect customer records and information in the firm's electronic portfolio management system by allowing certain employees to share computer sign-on credentials to access files which contained confidential customer information. The firm failed to place controls and procedures on the use and dissemination of the usernames and passwords, thus allowing potential access to the customer information outside of its control and management. The firm was also unable to determine which or how many employees had been given access to the common usernames and passwords, and did not have procedures to disable or change usernames and passwords on a recurring basis, or even after a home office employee was terminated or otherwise no longer associated with the firm. The firm also failed to establish procedures mandating that its representatives in the field install anti-virus software and other protection on their computers used to conduct LFS-related business away from the home office, and to audit the representative-owned computers to confirm the installation of security software or to monitor for potential or actual breaches. The firm was found to have violated Rule 30 of Regulation S-P and failed to adequately supervise its personnel, and paid a $450,000 fine.

SEC ENFORCEMENT

The SEC has also been fairly active in enforcing the Safeguards Rule in the cybersecurity area. Deficiencies identified by the SEC at firms included:

- The failure of a firm to have customer information policies and procedures for its employees and branch-registered representatives describing its overall program that was reasonably designed to protect customer records and information as required by the Safeguards Rule;
- The distribution of limited and insufficient written materials, which included suggestions rather than mandates, regarding safeguarding customer information;

- The lack of written procedures to follow up on potential computer security issues uncovered during branch audits, reported by registered representatives to the help desk, or identified as a result of breaches or potential breaches of customer information;
- The failure to mandate that the firm's registered representatives maintain antivirus software on their computers used to access customer account information on the firm's intranet and trading platform, thus leaving the information vulnerable to unauthorized access; and
- The failure to implement adequate controls, including some security measures, to safeguard customer information maintained in a proprietary trading platform, thus leaving the information vulnerable to unauthorized access.

In these cases, the SEC imposed substantial penalties from $100,000 to $275,000.

RECOMMENDATIONS

Broker-dealers should be mindful of FINRA's focus on cybersecurity issues, and should ensure that their policies, procedures and practices are compliant with existing guidance and teachings stemming from FINRA and SEC's enforcement efforts in the area. Attorneys and consultants expert in customer data security and privacy can assist broker-dealers in identifying gaps in their policies and procedures and, should a firm encounter a data breach or account intrusion, they can assist in damage control and mitigate the reputational impact of such an event.

Contact:

Daniel A. Nathan
(202) 887-1687
dnathan@mofo.com

Hillel T. Cohn
(213) 892-5251
hcohn@mofo.com

Ana-Maria Ignat
(202) 887-1561
aignat@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 10 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.