STRADLEY RONON ATTORNEYS AT LAW

Adviser Alert

A Publication of the Stradley Ronon
Investment Management Group

WWW.STRADLEY.COM

JULY 2014, NO. 5

Stradley Ronon Stevens & Young, LLP
2005 Market Street, Suite 2600
Philadelphia, PA 19103-7018
215.564.8000 Telephone
215.564.8120 Facsimile
www.stradley.com

With other offices in:
Washington, D.C.
Malvern, Pa.
Harrisburg, Pa.
Wilmington, Del.
Cherry Hill, N.J.
New York, N.Y.

CYBERSECURITY UPDATE: Cybersecurity Troubles at Financial Firms – Seven Regulatory Actions to Consider

By Kenneth L. Greenberg

"Those who do not remember the past are condemned to repeat it." — George Santayana

Frequently in the cybersecurity field, we try to look ahead to anticipate the next threat, that zero-day attack. In this article on cybersecurity, we take a look back and review a handful of regulatory actions initiated by the Securities and Exchange Commission or the Financial Industry Regulatory Authority to glean some lessons learned from cybersecurity vulnerabilities. The SEC is the primary regulator for investment companies, investment advisers and broker-dealers, and FINRA is a self-regulatory organization for broker-dealers.

Regulatory actions initiated by the SEC and FINRA relating to computer/information security are most often grounded in violations of Regulation S-P rather than the SEC's or FINRA's anti-fraud enforcement authority.[1] Rule 30 of Regulation S-P (referred to as the Safeguards Rule), which implemented the privacy provisions in Title V of the Gramm-Leach-Bliley Act of 1999[2] provides:

> Every broker, dealer, and investment company, and every investment adviser registered with the Commission must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. These written policies and procedures must be reasonably designed 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 customer records and information; and
>
> (3) Protect against any unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

The following regulatory actions highlight a number of broad categories of cybersecurity/information security problems, including inadequate policies and procedures, failure to follow up on reported cybersecurity problems and weak computer security/computer password practices, to name a few. Often, inadequate policies and procedures provide poor guidance to employees who, in turn, make poor decisions that result in problematic actions. The facts[3] that led to the regulatory action are summarized

continued on next page

and then followed by bullet points regarding the trouble-causing problems and regulatory sanctions. For each regulatory action, a basic lesson is provided. Additional lessons follow the discussions of the regulatory actions. This article is not intended to be a comprehensive discussion of cybersecurity regulatory actions, but merely highlights a few cases.

Regulatory Actions by the SEC

In the Matter of Marc A. Ellis, Release No. 34-64220 (April 7, 2011)[4]

Basic Lesson No. 1: Financial firms need information security policies and procedures that include some details and do not merely regurgitate the requirements of published regulations.

Facts: Laptop computers belonging to three registered representatives of GunnAllen Financial Inc. were stolen, and the computer password credentials belonging to a fourth registered representative were misappropriated. One of the stolen laptop computers contained names, dates of birth and Social Security numbers of 1,120 of GunnAllen's customers. For the theft involving the computer with customer information, GunnAllen filed a report with the local police but did not take any other steps concerning the theft, and the laptop computer was never recovered. A letter notifying customers of the potential data breach was drafted but never mailed to the affected clients. In addition, a registered representative who was terminated a year earlier had misappropriated another employee's passwords and was monitoring an employee's email. Other than changing the registered representative's password, no other follow-up action was ever taken by compliance. Marc Ellis, GunnAllen's chief compliance officer, was responsible for maintaining GunnAllen's customer information protection procedures.

- Inadequate Policies and Procedures. The policies addressing the protection of customer information contained in GunnAllen's written supervisory procedure manual were "less than a page long" and "general and vague," and they "simply recited the Safeguards Rule" and "provided examples of safeguards that may be adopted but did not specify policies actually adopted." In addition, no procedures existed that addressed what registered representatives should do in the event of a possible data breach such as a stolen laptop computer.

- Failure to Implement Written Policies and Procedures. While GunnAllen's procedures provided for a designated principal who was responsible for monitoring and testing computer safeguards, no one was ever appointed.

If you would like more information, contact Kenneth L. Greenberg at kgreenberg@stradley.com or 215.564.8149.

- Sanctions. Cease and desist order, censure and $15,000 penalty.

In the Matter of J.P. Turner & Company LLC, Release No. ID-395 (May 19, 2010)

Basic Lesson No. 2: Policies and procedures need to have enough detail that employees understand what actions they should and should not take. Training should be provided to reinforce understanding of their responsibilities.

Facts: A registered representative placed records of 5,000 current or former J.P. Turner customers in the curbside trash pickup at his residence. The records included names, addresses, dates of birth, Social Security numbers and bank account numbers. The trash hauler never collected them, and they remained abandoned until J.P. Turner retrieved them, but J.P. Turner was unable to confirm that the records had all been retrieved.

- Inadequate Policies and Procedures. Manuals for the main office, registered representatives and branch managers simply restated the objectives of the Safeguards Rule, mandated that firm records be locked in file cabinets and be subject to random spot checks, and delegated to the chief compliance officer the responsibility to ensure compliance. There were no other policies that addressed the administrative, technical or physical safeguards for protecting customer records or properly disposing of them when they were no longer needed.

- Inadequate Training. Although J.P. Turner's chief compliance officer emailed an NASD webcast to employees regarding customer data protection, the effectiveness of training provided by NASD webcast was weakened by instructions to viewers to review their company's procedures, of which there were none.

- Sanctions. Cease and desist order and $65,000 penalty.

continued on next page

In the Matter of Commonwealth Equity Services LLP, Release Nos. 34-60733 and IA-2929 (Sept. 29, 2009)

Basic Lesson No. 3: Compliance policies and procedures work best when employees are required to follow them as opposed to recommendations that they can choose to ignore. Also, it is not good enough to know that a problem exists, a process must be in place to ensure that the problem is remediated.

Facts: An unauthorized individual obtained the login credentials of one of Commonwealth's registered representatives through the use of a malware/keystroke logger virus. The virus was placed on a computer that did not have anti-virus software. Using the registered representative's login credentials, the intruder entered Commonwealth's intranet site, learned how to execute trades, and then launched a search query for customer accounts that generated a list of 368 accounts and provided personally identifiable information, including account name, account number, cash balance and last four digits of a customer's Social Security number. The intruder placed 18 unauthorized purchase orders in eight accounts totaling over $523,000. Commonwealth's clearing broker detected the activities, and the intruder was blocked from further trading. Commonwealth immediately canceled the unauthorized purchases and transferred them into its error account, which ultimately cost Commonwealth $8,000. Commonwealth reported the incident to the Commission and notified its clients.

- Inadequate Policies and Procedures. Commonwealth policies recommended as best practices for its registered representatives the use of anti-virus software on branch office computers but did not mandate such use.

- Failure to Follow Up on Computer Security Issues. Prior to the intrusion, Commonwealth's IT help desk received several calls from the same registered representative whose computer had been hacked and whose computer was compromised by a software virus. The IT help desk recommended the purchase of anti-virus software, but did not follow up to confirm whether anti-virus software was purchased. In addition, Commonwealth had no written procedures that addressed follow-up regarding computer security issues reported to the IT help desk or uncovered in branch audits.

- Sanctions. Cease and desist order, censure and $100,000 penalty.

FINRA Regulatory Actions

Wells Investment Securities Inc., Letter of Acceptance, Waiver and Consent No. 2009019893801 (Nov. 21, 2011)

Basic Lesson No. 4: Encrypt confidential information on mobile devices or, at a minimum, have the ability to wipe remotely the device. A company must verify that its policies and procedures are being followed by its employees.

Facts: Among other compliance issues, the FINRA letter notes that a laptop computer containing names, account numbers, Social Security numbers, addresses, telephone numbers and other investment data of over 37,000 customers was stolen from the car of an employee. The letter also noted that the employee who lost the laptop computer continued to have access to customer information after he was terminated by the firm but employed by an affiliate.

- Inadequate Policies and Procedures Regarding Encryption. Written procedures regarding Regulation S-P were generic as they required employees to secure all nonpublic financial information. The firm's encryption policy required that only nonpublic financial information communicated to third parties be encrypted. There was no requirement that data contained on a firm laptop computer or confidential customer information shared with an affiliate be encrypted. Regular computer system audits did not include laptop computer security.

- Weak Password Protocols. There was no enforcement of the use of strong passwords through periodic password changes or forced password expiration.

- Sanctions. Censure and $300,000 fine.

In the Matter of Department of Enforcement vs. Dante J. DiFrancesco, Complaint No. 2007009848801 (Dec. 17, 2010)

Basic Lesson No. 5: Employees need to understand that confidential client information is not theirs to take to a new employer. Privacy regulations require, among other things, that before any nonpublic personal information of a client is disclosed to a non-affiliated third party (like a new employer), a client must be provided with a reasonable opportunity to opt out of the disclosure.

continued on next page

Facts: Mr. DiFrancesco, prior to terminating his employment with Banc of America Investment Services Inc. (BAIS) and without authorization from BAIS or its customers, downloaded onto a flash drive in excess of 36,000 customer names, account numbers and telephone numbers, and forwarded the information to his new employer. He had intended to download only his approximately 200 clients.[5]

- Downloading and Transmission of Customer Personal Information to Competitor Triggers Privacy Violations. DiFrancesco violated Regulation S-P by downloading and sending to a nonaffiliated third party nonpublic personal information. Regulation S-P, among other things, requires broker-dealers to provide consumers the reasonable opportunity before any nonpublic personal information is disclosed to a nonaffiliated third party to opt out of the disclosure.

- Sanctions. Fined $10,000 and suspended for 10 business days in all capacities.

D.A. Davidson & Co., FINRA Letter of Acceptance, Waiver and Consent No. 200815299801, (Apr. 9, 2010)

Basic Lesson No. 6: Consider defense in depth for confidential information — encryption, password protection and segregation from third party accessible resources, to name a few. Monitor your computer network for unauthorized users, connections, devices and software.

Facts: A computer that housed a Web server with a persistent Internet connection also housed a database containing confidential customer information such as account names, account numbers, dates of birth and Social Security numbers. The database was not secured by password and not encrypted. Through hacking by use of a structured query language (SQL) injection,[6] the confidential information of 192,000 customers in the database was exfiltrated. The SQL injection attacks were visible on Web server logs, but logs were not monitored. The firm learned of the breach when the perpetrator demanded a sum of money in furtherance of the extortion scheme.

- Inadequate Policies and Procedures. The firm lacked (1) written procedures for review of system Web server logs[7] and (2) a policy for responding to intrusions.

- Failure to Adopt a Recommendation by an Independent Auditor and Outside Security Consultant That the Firm Implement an Intrusion Detection System. While the firm employed an outside security consultant to audit network security and make recommendations, the recommendation to employ an intrusion detection system had not been implemented by the time the computer hack occurred.

- Poor Computer Security Protocols. D.A. Davidson failed to encrypt a database containing nonpublic customer information, even though it was exposed to the Internet. D.A. Davidson also failed to require a password to access a firm database containing nonpublic customer information.

- Sanctions. Censure and fine of $375,000.

Centaurus Financial Inc., FINRA Letter of Acceptance, Waiver and Consent No. 2007009780901, (April 28, 2009).

Basic Lesson No. 7: Strong password protocols are essential. Have a procedure in place so that your employees know what actions to take in the event of a computer security breach. Even anonymous tips regarding computer security breaches should be given serious consideration.

Facts: Centaurus set up a computer fax server using a third-party service provider so that its brokers could send computer-related account documents that included Social Security numbers, addresses and account numbers to the trading and operations department of the home office. Upon being warned by an anonymous third party that the security of its computer fax server was compromised, and that it hosted a phishing site[8] and exposed confidential information to the public, Centaurus did not act on the warning until two customers, who were also notified by the anonymous third party, contacted Centaurus about the breach. Subsequently, Centaurus mailed inaccurate data breach notification letters to its customers and registered representatives.

- Inadequate Supervisory System and Procedures. Centaurus improperly configured its firewall and used poor password protocols, including a user name of "Administrator" and password of "password," which allowed unauthorized individuals on the Internet to connect to the computer fax server and access all the images stored on the computer fax server.

- Inadequate Response to Security Breach. While Centaurus was warned by an anonymous third party that the computer fax server had been compromised and was hosting a phishing site, Centaurus did not take any action until two customers, who were also warned by the anonymous third party that their confidential information was accessible, had their registered representatives complain to Centaurus about the breach.

continued on next page

- Inadequate Investigation. Centaurus limited its review of the computer fax server logs to the month of the breach rather than reviewing for unauthorized access going back to when the computer fax server was installed.

- Sanctions. Censure and fine in amount of $175,000.

Additional Lessons to Be Learned

- **Periodically review and reassess your company's data privacy and computer security policies and procedures, as well as how they are communicated to your employees and implemented.**

  ❑ Are policies and procedures sufficiently detailed so that employees understand their obligations and responsibilities under the policies and procedures?

  ❑ Does your company verify that employees are following policies and procedures after they are adopted?

  ❑ Are your employees' actual practices consistent with the policies and procedures?

  ❑ Are consequences for employee non-compliance with policies and procedures severe enough to deter non-compliant behavior?

  ❑ Are policies and procedures staying up to date with technological advances?

  ❑ Does your company require employees to practice computer security best practices (e.g., use passwords with a mix of uppercase and lowercase letters, numbers and symbols)?

  ❑ Is information that needs protection secure? Has your company considered the mobility of that information and its security?

  ❑ Are computer systems and related access points tested and monitored?

  ❑ Are employees aware of the proper way to dispose of information that is no longer required to be held?

- **Periodically review and reassess your company's employee education/training programs.**

  ❑ Do your employees understand what your company's compliance policies and procedures require them to do?

  ❑ Does your company solely rely on written materials to inform employees of their compliance obligations or are training programs offered to review and explain those obligations?

  ❑ Are employees aware of the various computer threats so they can be recognized when they occur?

- **Periodically review and reassess your company's preparedness to handle a computer security breach.**

  ❑ Is your company prepared to move quickly to remediate in the event of a computer security breach?

  ❑ Is your company's IT staff sufficiently trained to recognize a security breach when it occurs and to act quickly to remediate?

  ❑ Does your company have a team already established that can begin to deal with a security breach as soon as it is discovered?

  ❑ Is the leader of the security breach team granted sufficient authority so that decisions made by the team may be quickly executed?

  ❑ Does your company conduct periodic "fire drills" or other exercises to test the preparedness of your company's staff in the event of a security breach?

- **Review and reassess the data privacy and computer security policies and procedures as they relate to third parties.**

  ❑ Do your company's employees understand under what circumstances proprietary or confidential personally identifiable information can be provided to third parties?

  ❑ Does someone in your company keep track of third parties who receive confidential or proprietary information?

  ❑ Are third-party data privacy and computer security policies and procedures assessed before information is provided to such third parties?

continued on next page

[1] FINRA regulatory actions also include citations involving Rule 3010 (failure to supervise) and Rule 2010 (failure to conduct high standards of commercial honor and just and equitable principles of trade). In contrast, the Federal Trade Commission, another regulator in the privacy and data security field, uses its authority to police unfair and deceptive trade practices as a means to enforce companies' privacy policies and address cybersecurity issues.

[2] Gramm-Leach-Bliley Act of 1999, Public L. No. 106–102, 113 Stat. 1338, Nov. 12, 1999.

[3] Generally, in SEC orders instituting administrative cease and desist proceedings and FINRA letters of acceptance, waiver and consent, the party involved neither admitted nor denied the findings contained in the regulatory action.

[4] In related enforcement actions, the president of GunnAllen Financial Inc., Frederick O. Kraus, and National Sales Manager David C. Levine were each censured and fined $20,000 for improperly transferring customer records to another firm (i.e., personal nonpublic information was supplied to another firm without proper client notice and without providing the client with a reasonable opportunity to opt out of the transfer) in connection with the winding down of GunnAllen's business operations. In the Matter of Frederick O. Kraus, Release Nos. 34-64221 (April 7, 2011) and In the Matter of David C. Levine, Release No. 34-6422 (April 7, 2011).

[5] *See also* In the Matter of NEXT Financial Group Inc., Release No. ID-349 (June 18, 2008). SEC administrative law judge fined NEXT Financial $125,000 for permitting registered representatives who were leaving the firm to take confidential personally identifiable information and encouraged registered representatives from other firms who were recruited to join NEXT Financial to bring confidential personally identifiable information to NEXT Financial.

[6] An SQL injection is an attack whereby computer code is repeatedly inserted into a Web page for the purpose of extracting information from a database.

[7] D.A. Davidson did monitor perimeter security logs, but the attacks were not visible on such logs.

[8] The fax servers were being used to host a counterfeit eBay Web page in connection with a mass email sent that had a link to the counterfeit website, which requested an update of personal information.