The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 23444

May 14, 2009

FINRA Sanctions Broker-Dealer For Failing To Protect Customer Information And Provide Adequate Notice Of Breach

[23444]

May 14, 2009

TO: TECHNOLOGY COMMITTEE No. 11-09
COMPLIANCE MEMBERS No. 22-09
INTERNAL AUDIT ADVISORY COMMITTEE No. 3-09
OPERATIONS MEMBERS No. 11-09
PRIVACY ISSUES WORKING GROUP No. 5-09 RE: FINRA SANCTIONS BROKER-DEALER FOR FAILING TO PROTECT CUSTOMER INFORMATION AND PROVIDE ADEQUATE NOTICE OF BREACH

The Financial Industry Regulatory Authority (FINRA) has settled a proceeding with one of its broker-dealer members that involved a breach of the member's fax system. [1] In addition to finding that the member violated Regulation S-P through its lax security, FINRA also found that the firm's inaccurate notifications to customers and registered representatives under state breach notification laws violated rules of the NASD. Based on these violations, the firm was censured, fined $175,000, and required to comply with certain undertakings. The facts of this case, the violations, and the sanctions agreed to are briefly discussed below.

Facts of the Case

This action involves a FINRA broker-dealer member with 600 registered representatives in 300 branch offices throughout the United States. In April 2006, the member used a third-party service provider to set up a Computer Fax Server to facilitate the ability of its registered representatives to send customer account documents to the Trading and

Operations Department at the member's home office. These documents, which included new account forms, account transfer forms, and letters of authorization, contained confidential information on the member's customers such as their social security numbers, account numbers, and name and address information. In setting up this new server, the member improperly configured its firewall, which enabled unauthorized individuals on the Internet to connect to it if such individuals had the correct username and password. Once connected, such unauthorized individuals could obtain full access to images of faxes that had been sent to the home office and stored on the server. The user name and password employed by the member for this new server were "Administrator" and "password," respectively.

On July 15, 2007, an unknown person uploaded a phishing program [2] on the server to host a phishing scam that replicated an eBay web page. After this program was uploaded, there were over 800 unauthorized logins onto the server, most of which were the result of individuals clicking on the link provided in a mass email that automatically logged them onto the server. After this phishing scam was enabled, it was posted to a phishing website that listed such scams in an effort to stop such activity. According to the AWC, certain individuals review the posted phishing sites to determine if there are ongoing scams and notify those persons whose systems may be compromised. On July 16, 2007, one day after the phishing program was uploaded, an individual identified in the AWC as "John Doe" notified the member via voicemail that the member's server was compromised and was being used to host a phishing site. John Doe also alerted the member to the fact that the server contained customer data the member may want to secure. He requested that the member contact him for more information. When the member contacted John Doe, he provided the contact the names of folders on the server that he was able to access. Notwithstanding this, the member "failed to promptly take sufficient steps to verify that its server had been accessed even though such unauthorized access was set forth on the server log."

On July 17th, John Doe again checked the member's server to see if it had been secured. When he saw that it had not, he downloaded over 1800 fax images, which included approximately 1400 customer fax images that contained some form of confidential customer information. He used this information to contact two of the customers to alert them to the fact that their information was not secured. These customers contacted the member through their registered representatives, who in turn contacted a compliance officer for the member. Once the compliance officer confirmed John Doe's identity and verify the information he had obtained, the member shut down the server and Internet access for the firm.

After the member shut down its server, it conducted a review with the assistance of an outside technology firm to determine the extent of the unauthorized access. However, the review was limited to activities in July 2007, even though the member had used a "weak username and password" to secure the system since the server was first installed in April 2006. Indeed, apparently unauthorized logins to the server began the month the server was installed. The review also failed to detect additional unauthorized logins and downloads from the server, which were apparent in the July 2007 logs.

In September 2007, pursuant to state law requirements, the member sent a letter to the approximately 1400 customers whose personal and confidential information had been downloaded by John Doe. According to the AWC, the "letter inaccurately stated that the unauthorized access was limited to one 'benevolent' person." It did not disclose that other unauthorized logins had occurred, nor did it note that the downloads were made possible

by the member's previously inadequately configured firewall and weak username and password. The member also sent a similar letter to the registered representatives who service these 1400 customer accounts.

Violations

Based upon these facts, FINRA found that the member violated Regulation S-P through: the member's use of a weak username and password; its insecure computer firewall; the inadequate investigation the member conducted following notice of unauthorized access of computerized data containing confidential customer information; and its inadequate supervisory procedures, which were not reasonably designed to comply with the federal securities laws. FINRA also found that the member violated NASD Rule 3010 [3] by violating Regulation S-P and NASD Rules 2210, 2211, and 2110 [4] by providing the members' customers and registered representatives "misleading" notifications in response to state breach notice laws.

In addition to being censured and fined $175,000, the member was required to:

- Disseminate corrected and accurate breach notifications, in a form not unacceptable to FINRA staff, to all customers and registered representatives who had received the misleading notifications;
- Offer notified customers "a reasonable and nationally-recognized credit monitoring service for a period of no less than one year at no charge to the customer;" and
- Certify to FINRA, within 90 days, that no unauthorized access has occurred that was not recorded in the member's server logs, that it has complied with the above undertakings, and that it has updated and improved its Regulation S-P procedures.

Tamara K. Salmon
Senior Associate Counsel

Attachment

endnotes

[1] See Re: Centaurus Financial, Inc., FINRA Letter of Acceptance, Waiver and Consent, which was announced on April 28, 2009 (the "AWC"). A copy of the AWC is attached.

[2] As described in the AWC, "Phishing is a computer-based artifice designed to fool computer users into divulging personal information such as usernames, passwords, and bank and credit card information. Typically, a realistic looking, but counterfeit website is created, then a mass e-mail is sent out to recipients with a link to the counterfeit website and a request to "update" their personal information by clicking on the link provided."

[3] NASD Rule 3010 requires members to establish and maintain supervisory systems that are reasonably designed to achieve compliance with applicable laws and regulations, including NASD rules.

[4] NASD Rule 2210 requires members to observe high standards of commercial honor and just and equitable principles of trade. NASD Rules 2210 and 2211 govern member

communications and sales material content.
