The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 24239

April 15, 2010

FINRA Fines Broker-Dealer for Failure to Protect Customer Data From a Computer Hacker's SQL Attack

[24239]

April 15, 2010

TO: COMPLIANCE MEMBERS No. 9-10
INTERNAL AUDIT ADVISORY COMMITTEE No. 5-10
PRIVACY ISSUES WORKING GROUP No. 3-10
RISK MANAGEMENT ADVISORY COMMITTEE No. 5-10
RISK MANAGEMENT COMMITTEE No. 8-10
TECHNOLOGY COMMITTEE No. 3-10 RE: FINRA FINES BROKER-DEALER FOR FAILURE TO PROTECT CUSTOMER DATA FROM A COMPUTER HACKER'S SQL ATTACK

FINRA has announced its settlement of an enforcement proceeding involving a broker-dealer who was the victim of a computer hacker who utilized a sophisticated network intrusion attack known as a “structured query language” or “SQL” attack to infiltrate the broker-dealer’s database. [1] According to FINRA’s AWC, the facts of the case are as follows. Prior to January 2008, the broker-dealer failed to protect certain confidential information of its customers when it utilized a database server that contained confidential customer information without adequate safeguards to protect that information. In December 2007, this database was compromised when “an unidentified third party” downloaded this information through the SQL attack. The broker-dealer learned about the breach in January 2008, when this third party, who was “believed to be part of an international crime group under investigation by the U.S. Secret Service,” tried to blackmail the firm by requesting money in return for the customers’ information.

According to the AWC, the hacker was able to obtain confidential information on approximately 230,000 customers through its SQL attack. [2] While these attacks were

visible on the web server logs, the broker-dealer failed to review those logs. While the firm did regularly review its perimeter security logs, the SQL attack was not visible on those logs. The broker-dealer did not have any written procedures in place for the review of system web server logs, nor an intrusion detection system. Nor did the firm have written procedures setting forth an information security program that was designed to respond to intrusions. Interestingly, at various points between April 2006 and October 2007, the firm had voluntarily retained independent auditors and outside security consultants to review and/or audit its network security. These engagements resulted in recommendations for enhancements to the firm's security systems, which the firm implemented the majority of. However, at the time of the attack, they had not implemented a recommendation that an intrusion detection system be implemented. The AWC notes that, while the outside audits had not been able to breach the broker-dealers *external* security during their review, there was no indication that they had reviewed or examined the computer housing the broker-dealer's database, which is where the SQL attack occurred.

Subsequent to receiving the blackmail threat from the hacker, the firm took down its website and reported the incident to law enforcement. It also: hired an outside firm to advise on electronic security; removed certain customer sensitive information from its database; added an additional firewall between the internet and it internal systems; deployed intrusion prevention software; and employed web application testing software to test for security vulnerabilities. The broker-dealer also updated its database server to the latest encryption software, installed a repository for server and network logs to be stored centrally, and formalized written procedures for the periodic review of web server logs.

Based upon the compromise of its systems by the hacker, FINRA found that the broker-dealer violated Rule 30 of Regulation S-P, which requires SEC registrants to adopt and implement policies and procedures reasonably designed to safeguard customer records and information. It also found the broker-dealer violated NASD Rule 2110, which requires members to uphold high standards of commercial honor and just and equitable principles of trade, and Rule 3010(a) and (b), which require members to establish and maintain supervisory systems that are reasonably designed to achieve regulatory compliance.

The firm was fined $375,000 for its violation. In deciding upon the appropriate sanctions, FINRA considered the remedial steps the firm took after the hacker attacks, as well as the fact that, as a result of its cooperation, four suspects were indicted, three of whom were extradited to the United States. [3] In addition to the above discussed steps the firm took subsequent to the attack, these remedial steps included: issuing a press release to the public reporting the incident; preparing a detailed communication plan for employees; establishing internal and external call centers to respond to customer inquiries; providing written notice to affected customers; and voluntarily offering affected customers a subscription to a credit-monitoring service for a two-year period at a cost to the firm of $1.3 million. The AWC notes that the broker-dealer also resolved a class action suit with affected customers, which including providing loss reimbursement for potential victims of the hack of up to $1,000,000. [4]

Tamara K. Salmon
Senior Associate Counsel

Attachment

endnotes

[1] See In Re D.A. Davidson & Co., FINRA Letter of Acceptance, Waiver, and Consent (April 9, 2010) (the "AWC"), which is attached. The AWC describes an SQL as "an attack whereby computer code is repeatedly inserted into a web page for the purpose of extracting information from a database." See AWC at p. 3.

[2] While the AWC notes that the records of 230,000 customers were accessed, the broker-dealer only violated Regulation S-P with respect to the records of 193,000 of these customers. This is because they were individuals' accounts covered by Regulation S-P. The remaining customers were corporate or other entity accounts who are not covered by Regulation S-P's protections.

[3] According to information obtained from other sources, including the U.S. Department of Justice, there were four hackers involved in the attack, three of whom were Latvian nationals who were extradited from the Netherlands to face charges in Montana, where the broker-dealer was headquartered. The fourth attacker apparently remains at large. The three hackers who were extradited, Aleksandrs Hoholko (30), Jevgenijis Kuzmenko (26), and Vitalijs Drozdovs (33) pleaded guilty last month to Federal charges of making threatening communications and receiving extortion proceeds. They are scheduled to be sentenced in June. According to the indictment, the fourth suspect was responsible for conducting the breach and then using the three Latvians as couriers to receive the extortion payments. Apparently, in connection with the extortion agreement, the fourth suspect, who identified himself to the broker-dealer as an "independent IT security consultant," agreed to delete the stolen information and identify weaknesses in the broker-dealer's security in return for $80,000.

[4] The AWC notes that, to date, to the broker-dealer's knowledge, no customer has suffered any instances of identity theft or other actual damages as a result of the hacking.