

**FINRA FINES BROKER-DEALER FOR ITS FAILURE TO PROTECT
CONFIDENTIAL CUSTOMER INFORMATION FROM HACKERS****Overview**

The Financial Industry Regulatory Authority (FINRA) announced on April 12, 2010 that it had fined Montana based broker-dealer D.A. Davidson & Co. (“Davidson”) for its failure to protect confidential customer information from an international crime group that hacked into its computer systems.¹

Summary of Facts

In December 2007 hackers used a sophisticated network intrusion mechanism² to breach Davidson’s database and access and download confidential customer information of over 200,000 of Davidson’s clients.³ The confidential customer information included customer account numbers, social security numbers, names, addresses and dates of birth. The breach was discovered when the crime group attempted to blackmail Davidson in January 2008.

Findings of FINRA

FINRA cited security and procedural failures that led to Davidson’s breach of confidential customer information, including not activating a password, not encrypting the database, failing to install an intrusion detection system⁴ and not having finalized and implemented written procedures in place for its information security program. Aside from these technological deficiencies, FINRA indicated that Davidson still could have responded earlier to the breach had it had procedures in place to review web server logs that would have evidenced the attack.

FINRA found Davidson to be in violation of Rule 30 of Regulation S-P, which requires a broker-dealer’s systems and procedures to be reasonably designed to safeguard customer records and information, NASD Rules 3010(a) and (b) (failure to supervise and have written procedures to comply with securities laws) and NASD Rule 2110 (failure to observe high standards of commercial honor and just and equitable principles of trade).

¹ <http://www.finra.org/Newsroom/NewsReleases/2010/P121262>.

² The hackers attacked by using an “SQL injection” in which computer code is repeatedly inserted into a Web page to extract data.

³ A total of 230,000 of Davidson’s clients were affected, and because over 190,000 of those were individuals, Regulation S-P which covers only individual consumers or customers, was implicated.

⁴ While Davidson implemented many of the recommendations made by independent auditors and security consultants that Davidson had hired prior to the attack, it failed to implement the intrusion detection system before the breach occurred.

Mitigating Factors

FINRA took into account several mitigating factors in the settlement with Davidson resulting in a censure and a \$375,000 fine, with an agreement not to bring any future actions based upon the same facts. Davidson’s mitigating actions included:

- a) Notification to and prompt cooperation with law enforcement following discovery of the breach, which led to the identification and apprehension of several members of the international crime group;
- b) Taking down its website for a period of time and the removal of certain confidential information from its database;
- c) Its hiring of an outside consulting firm to advise on electronic security, which resulted in adding an additional firewall, deploying intrusion prevention software, employing web application testing software to test for security vulnerabilities, updating the database server to the latest encryption software, installing a repository for server and network logs to be stored centrally, and formalizing written procedures for the periodic review of web server logs;
- d) Issuing a press release to the public reporting the incident and providing written notice to its affected customers;
- e) Preparing a detailed communication plan for its employees, including establishing internal and external call centers to respond to customer inquiries; and
- f) Voluntarily offering its affected customers a subscription to a credit-monitoring service for a two-year coverage period at a cost to Davidson of \$1,300,000 and providing loss reimbursement for potential victims of the hacking of up to an aggregate of \$1,000,000. To date, Davidson is not aware of any incidents of identity theft or of actual damages incurred by an affected customer as a result of the breach.

Practical Implications

The findings of fact in this settlement indicate that broker-dealers should employ a number of IT security measures to protect confidential customer information, but should also have compliance procedures designed to prevent and respond to security breaches in the event they occur. However, should confidential client data be compromised, FINRA appears to consider favorably the fact that a broker-dealer responds with prompt notification and improvements to security and its compliance mechanisms and assistance to affected customers.

* * * * *

If you have any questions regarding this memorandum, please contact Martin R. Miller (212-728-8690, mmiller@willkie.com) or Marc J. Lederer (212-728-8624, mlederer@willkie.com), or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our website is located at www.willkie.com.

April 14, 2010

Copyright © 2010 by Willkie Farr & Gallagher LLP.

All Rights Reserved. This memorandum may not be reproduced or disseminated in any form without the express permission of Willkie Farr & Gallagher LLP. This memorandum is provided for news and information purposes only and does not constitute legal advice or an invitation to an attorney-client relationship. While every effort has been made to ensure the accuracy of the information contained herein, Willkie Farr & Gallagher LLP does not guarantee such accuracy and cannot be held liable for any errors in or any reliance upon this information. Under New York's Code of Professional Responsibility, this material may constitute attorney advertising. Prior results do not guarantee a similar outcome.