FINANCIAL INDUSTRY REGULATORY AUTHORITY
LETTER OF ACCEPTANCE, WAIVER AND CONSENT
NO. 20080152998

TO: Department of Enforcement
Financial Industry Regulatory Authority (FINRA)

RE: D.A. Davidson & Co.
(CRD No. 199)

Pursuant to FINRA Rule 9216 of FINRA's Code of Procedure, D.A. Davidson & Co. ("D.A. Davidson" or the "Firm"), submits this Letter of Acceptance, Waiver and Consent ("AWC") for the purpose of proposing a settlement of the alleged rule violations described below. This AWC is submitted on the condition that, if accepted, FINRA will not bring any future actions against the Firm alleging violations based on the same factual findings described herein.

I.

ACCEPTANCE AND CONSENT

A. The Firm hereby accepts and consents, without admitting or denying the findings, and solely for the purposes of this proceeding and any other proceeding brought by or on behalf of FINRA, or to which FINRA is a party, prior to a hearing and without an adjudication of any issue of law or fact, to the entry of the following findings by FINRA:

BACKGROUND

D.A. Davidson has been a FINRA regulated broker-dealer since 1952 and is headquartered in Great Falls, Montana. The Firm has no relevant disciplinary history.

OVERVIEW

Prior to January 2008 (the "Relevant Period"), D.A. Davidson failed to protect certain confidential information of its customers when it utilized a database server (the "Database") containing customer account numbers, social security numbers, names, addresses, dates of birth and certain other confidential data (the "Confidential Customer Information"), but without adequate safeguards to protect the security and confidentiality of that information. D.A. Davidson's failure to adequately protect its Database permitted international criminals to improperly access, by a computer hack, the Confidential Customer Information of approximately 192,000 customers.

Based on the foregoing, D.A. Davidson failed to adopt and implement policies and procedures reasonably designed to safeguard customer records and information, and to establish and maintain a system, including written supervisory procedures, reasonably designed to achieve compliance with Rule 30 of Regulation S-P. As a result, D.A. Davidson violated Rule 30 of Regulation S-P and NASD Rule 2110 and NASD Rules 3010(a) and (b) and NASD Rule 2110.

FACTS AND VIOLATIVE CONDUCT BY RESPONDENT

Rule 30 of Regulation S-P provides that "[e]very broker, dealer . . . 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 unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."

The Firm employed a public facing computer web server that hosted certain Firm web pages behind an external perimeter firewall. The computer that housed the web server also housed the Database containing the Confidential Customer Information even though the web pages did not offer its customers on-line transaction capabilities and were purely informational. The Database was stored on a computer with a persistent Internet connection, thereby leaving the information in the Database exposed to the Internet. Nonetheless, the Firm failed to implement adequate safeguards to protect the information housed on the Database.

The Database was not encrypted and the Firm never activated a password, thereby leaving the default setting of a blank password in place. The lack of encryption on the Database also increased the vulnerability of the Confidential Customer Information in that data was transmitted and stored in readable text, thus encryption mechanisms did not have to be bypassed in order to access the information stored on the Database.

a. The Compromise of Confidential Customer Information:

On December 25 and 26, 2007, the Database was compromised when an unidentified third party downloaded the Confidential Customer Information through a sophisticated network intrusion. The Firm learned of the breach through an email that was sent to it by the hacker ("Hacker") on January 16, 2008. The perpetrator, who is believed to be part of an international crime group under investigation by the U.S. Secret Service, demanded that the Firm pay a sum of money in furtherance of a blackmail scheme.

The means employed by the Hacker to breach the Firm's system was through a mechanism called "SQL injection." A structured query language (SQL) injection is an attack whereby computer code is repeatedly inserted into a web page for the purpose of extracting information from a database. By doing so, Hacker was able to access and download the Confidential Customer Information of approximately 192,000 customers.[1] The attacks did not affect any of the Firm's computer systems for transactions, transfers of assets, accounting or any other operational functions. These attacks were visible on web server logs, however the Firm failed to review those logs. The Firm did regularly review perimeter security logs, however the attacks were not visible on those logs. The Firm did not have any written procedures in place for the review of system 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.

Between April 2006 and October 2007 the Firm voluntarily retained independent auditors and outside security consultants at various points in time to review and/or audit its network security. During the course of those consultations, recommendations for enhancements to the Firm's security systems were made and the Firm implemented the majority of those recommendations. However, notwithstanding a recommendation to the Firm, made in or about April 2006, that an intrusion detection system be implemented, the Firm had not implemented such a system at the time the hack occurred in December 2007. The Firm received an audit report stating that the auditor had been unable to breach the Firm's external security, in October 2007. While the Firm placed no limit on the scope of the reviews, there is no indication that the auditors or outside security consultants reviewed or examined the computer housing the Database.

The Firm also did not have finalized and implemented written procedures in place for its information security program that, among other things, should have been designed to protect confidential customer information. Based on the foregoing, the Firm's systems and procedures were not reasonably designed to safeguard customer records and information in accordance with Regulation S-P. These supervisory deficiencies contributed to Hacker's ability to obtain the Confidential Customer Information of approximately 192,000 Firm customers.

b. Firm Remedial Efforts after the Intrusion:

Upon receiving the blackmail threat from Hacker, the Firm took down its website and reported the incident to law enforcement. The Firm also took other remedial steps, including hiring an outside firm to advise on electronic security, removing certain customer sensitive information from the Database, and, while there was an existing firewall protecting the server, adding an additional firewall between the

[1] In fact, records relating to approximately 230,000 clients were downloaded from the Database, but only approximately 192,000 of those clients were individual customers covered by Regulation S-P; the remainder were corporate or other entity accounts.

internet and internal systems, deploying intrusion prevention software and employing web application testing software to test for security vulnerabilities. The Firm has also updated the 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.

c. Other Factors Considered:

The Firm provided significant cooperation to law enforcement agencies, which aided in the Secret Service's ability to identify four of the members of the international group suspected of participating in the hacking attack of the Firm. As a result of the Firm's cooperation, four suspects have been indicted, three of whom were extradited to the United States.

The Firm also took prompt remedial steps after the hacker attacks, including issuing a press release to the public reporting the incident; preparing a detailed communication plan for employees, including establishing internal and external call centers to respond to customer inquiries; providing written notice to its affected customers; and voluntarily offering affected customers a subscription to a credit-monitoring service for a two year coverage period at a cost to the Firm of $1.3 million. The Firm has also resolved a class action litigation with its affected customers, which includes providing loss reimbursement for potential victims of the hacking of up to an aggregate of $1,000,000. To date, to the Firm's knowledge, no customer has suffered any instances of identity theft or other actual damages as a result of the information security breach.

B. The Firm also consents to the imposition of the following sanction: a censure and fine in the amount of $375,000.

The Firm agrees to pay the monetary sanction upon notice that this AWC has been accepted and that such payment is due and payable. I have submitted an Election of Payment form showing the method by which I propose to pay the fine imposed.

The Firm specifically and voluntarily waives any right to claim that it is unable to pay, now or at any time hereafter, the monetary sanction imposed in this matter.

The sanctions imposed herein shall be effective on a date set by FINRA staff.

II.

WAIVER OF PROCEDURAL RIGHTS

I specifically and voluntarily waive the following rights granted under FINRA's Code of Procedure:

A. To have a Formal Complaint issued specifying the allegations against me;

B. To be notified of the Formal Complaint and have the opportunity to answer the allegations in writing;

C. To defend against the allegations in a disciplinary hearing before a hearing panel, to have a written record of the hearing made and to have a written decision issued; and,

D. To appeal any such decision to the NAC and then to the U.S. Securities and Exchange Commission and a U.S. Court of Appeals.

Further, I specifically and voluntarily waive any right to claim bias or prejudgment of the General Counsel, the NAC, or any member of the NAC, in connection with such person's or body's participation in discussions regarding the terms and conditions of this AWC, or other consideration of this AWC, including acceptance or rejection of this AWC.

I further specifically and voluntarily waive any right to claim that a person violated the ex parte prohibitions of FINRA Rule 9143 or the separation of functions prohibitions of FINRA Rule 9144, in connection with such person's or body's participation in discussions regarding the terms and conditions of this AWC, or other consideration of this AWC, including its acceptance or rejection.

III.

OTHER MATTERS

I understand that:

A. Submission of this AWC is voluntary and will not resolve this matter unless and until it has been reviewed and accepted by the NAC, a Review Subcommittee of the NAC, or the Office of Disciplinary Affairs ("ODA"), pursuant to FINRA Rule 9216;

B. If this AWC is not accepted, its submission will not be used as evidence to prove any of the allegations against me; and,

C. If accepted:

1. this AWC will become part of my permanent disciplinary record and may be considered in any future actions brought by FINRA or any other regulator against me;

2. this AWC will be made available through FINRA's public disclosure program in response to public inquiries about my disciplinary record;

3. FINRA may make a public announcement concerning this agreement and the subject matter thereof in accordance with FINRA Rule 8313; and,

4. I may not take any action or make or permit to be made any public statement, including in regulatory filings or otherwise, denying, directly or indirectly, any finding in this AWC or create the impression that the AWC is without factual basis. I may not take any position in any proceeding brought by or on behalf of FINRA, or to which FINRA is a party, that is inconsistent with any part of this AWC. Nothing in this provision affects my right to take legal or factual positions in litigation or other legal proceedings in which FINRA is not a party.

D. I may attach a Corrective Action Statement to this AWC that is a statement of demonstrable corrective steps taken to prevent future misconduct. I understand that I may not deny the charges or make any statement that is inconsistent with the AWC in this Statement. This Statement does not constitute factual or legal findings by FINRA, nor does it reflect the views of FINRA or its staff.

I certify that I have read and understand all of the provisions of this AWC and have been given a full opportunity to ask questions about it; that I have agreed to its provisions voluntarily; and that no offer, threat, inducement, or promise of any kind, other than the terms set forth herein and the prospect of avoiding the issuance of a Complaint, has been made to induce me to submit it.

April 9, 2010
Date

D.A. Davidson & Co.

By: Larry Martin
General Counsel

Reviewed by:

W. Hardy Callcott
Counsel for Respondent
Bingham McCutchen LLP
Three Embarcadero Center
San Francisco, CA 94111-4067

Accepted by FINRA:

4-9-10
Date

Signed on behalf of the
Director of ODA, by delegated authority

Suzanne R Elovic
Suzanne R. Elovic, Chief Counsel
Scott M. Andersen, Director
Chun Li, Counsel
FINRA Department of Enforcement
14 Wall Street
New York, New York 10005
(646) 315-7360