The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 29973

June 9, 2016

SEC Sanctions Broker-Dealer for Reg. S-P Violation that Resulted from an Employee's Theft of Customer Information

[29973]

June 9, 2016

TO: BANK, TRUST AND RETIREMENT ADVISORY COMMITTEE No. 17-16
BROKER/DEALER ADVISORY COMMITTEE No. 18-16
CHIEF INFORMATION SECURITY OFFICER ADVISORY COMMITTEE
COMPLIANCE MEMBERS No. 16-16
OPERATIONS MEMBERS No. 16-16
SMALL FUNDS MEMBERS No. 23-16
TECHNOLOGY COMMITTEE No. 8-16
TRANSFER AGENT ADVISORY COMMITTEE No. 23-16 RE: SEC SANCTIONS BROKER-DEALER FOR REG. S-P VIOLATION THAT RESULTED FROM AN EMPLOYEE'S THEFT OF CUSTOMER INFORMATION

The SEC has announced that it has sanctioned a firm that is dually registered as a broker-dealer and investment adviser (the "Respondent") for violating Section 248.30(a) of Regulation S-P, which requires SEC registrants to adopt written policies and procedures that are reasonably designed to safeguard customer records and non-public personal information. [1] The violation resulted from an employee exfiltrating data regarding approximately 730,000 customer accounts associated with approximately 330,000 different households to his personal server between 2011 and 2014. [2] Some of this data was subsequently offered for sale on the Internet. Based on the violation, the Respondent was censured, ordered to cease and desist from future violations of Section 248.30(a), and fined $1 million. The facts of the case are briefly summarized below.

The Respondent's employee was able to access customer records beyond those necessary for him to provide services to his customers in his capacity as a financial advisor of the Respondent. He was able to do so because two of the portals the Respondent had designed for its representatives to use "were ineffective in limiting access with respect to one report available through [one of the portals] and absent with respect to one of the reports available through [the other portal]." [3] The reports that were accessible through

these portals contained non-public personal information on the Respondent's customers, beyond the employee's customers. According to the Release, when the employee discovered these vulnerabilities in the Respondent's system, he began to conduct unauthorized searches of the Respondent's account records, download data from these records, and transfer the data "to a personal server located at his home." [4] While the Respondent had installed and maintained controls on its computer system that, among other things, restricted employees from copying data onto removal storage devices and accessing certain categories of websites, the employee was able to bypass these controls. He did so by accessing his personal website (which was a .com site), "which had a feature that enabled [the employee] to transfer data from [his computer in the Respondent's offices] to his personal server." [5] According to the Release, the Respondent's Internet filtering software did not prevent employees from accessing such "uncategorized" websites from the Respondent's computers.

The Release notes that, between approximately December 15, 2014 and February 3, 2015, portions of the downloaded data were posted to at least three Internet sites "purportedly for sale to a third party." [6] The Respondent discovered the data breach on December 17, 2014 through one of its routine Internet sweeps. At that time, it removed the data from the Internet and notified law enforcement and other authorities. While the Respondent was able to determine that the employee had exfiltrated the data, "[s]ubsequent forensic analysis of the employee's personal server revealed that a third party likely hacked into the server and copied confidential customer data that [the employee] had downloaded." [7] In January 2015, the Respondent began notifying customers who had been impacted by the breach.

In settling this matter, the Commission considered "the remedial efforts promptly taken by the Respondent" and the cooperation it afforded to the Commission.

Tamara K. Salmon
Associate General Counsel

endnotes

[1] See In the Matter of Morgan Stanley Smith Barney, LLC, SEC Release No. 34-78021 (June 8, 2011) ("Release"), which is available at: https://www.sec.gov/litigation/admin/2016/34-78021.pdf.

[2] The employee pled guilty to a criminal information in United States v. Galen Marsh, No. 15 Cr. 641 (KTD)(S.D.N.Y.) that charged him with one count of exceeding his authorized access to a computer and thereby obtaining information contained in a financial record of a financial institution in violation of 18 U.S.C.§1030(a)(2)(A). He was sentenced to 36 months' probation and ordered to pay restitution of $600,000. Based on his criminal plea and conduct, in a separate proceeding the Commission barred him from association with any broker, dealer, investment adviser, municipal securities dealers, municipal advisor, transfer agent, or NRSRO and from participating in any capacity with any offering of a penny stock. See In the Matter of Galen J. Marsh, SEC Release No. 34-78020 (June 8, 2016), which is available at: https://www.sec.gov/litigation/admin/2016/34-78020.pdf.

[3] Release at pp. 3-4.

[4] Release at p. 5.

[5] Id.

[6] Id.

[7] Id.
