The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 29365

September 25, 2015

SEC Sanctions Advisory Firm for Failing to Adopt Policies and Procedures to Safeguard Customers' Personally Identifiable Information

[29365]

September 25, 2015

TO: COMPLIANCE MEMBERS No. 28-15
INVESTMENT ADVISER MEMBERS No. 21-15
OPERATIONS MEMBERS No. 27-15
PRIVACY ISSUES WORKING GROUP No. 1-15
TECHNOLOGY COMMITTEE No. 17-15 RE: SEC SANCTIONS ADVISORY FIRM FOR FAILING TO ADOPT POLICIES AND PROCEDURES TO SAFEGUARD CUSTOMERS' PERSONALLY IDENTIFIABLE INFORMATION

The SEC has announced the settlement of a case against an investment adviser involving a violation of the portion of Regulation S-P that requires registrants to safeguard customers' records and information. [1] Based on its violation, the adviser was censured, ordered to cease and desist from further violations, and fined $75,000. The facts of this case are summarized below.

Background

According to the Order, the Respondent was a registered adviser with approximately 8,400 client accounts. However, as a result of its work with retirement plans, it had non-public personal information ("NPPI") – including name, date of birth, and social security number – on over 100,000 individuals who were plan participants. Access to this information was limited to two individuals who had administrative rights to the adviser's servers. In July 2013, the Respondent discovered a potential cybersecurity breach at a third party-hosted web server. It promptly retained more than one cybersecurity firm to confirm the attack and assess the scope of the breach. These reviews determined that the attack had been launched by multiple IP addresses, each of which was traced back to China, and that the intruder had gained full access rights to the data stored on the server. Due to the intruder destroying log files surrounding the attack, the cybersecurity firms were unable to determine the full nature or extent of the breach. Another cybersecurity firm retained by the Respondent was unable to determine whether any personally-identifiable information

had been accessed or compromised during the breach. Shortly after the intrusion, the Respondent notified all individuals whose information may have been accessed of the breach and offered them free identity monitoring through a third-party provider. The Order notes that, "to date, the firm had not learned of any information indicating that a client has suffered any financial harm as a result of the cyber attack." [2]

SEC Findings

Based on the above, the Order found that, during the period that the Respondent maintained client data on a third-party web server, it "failed to adopt any written policies and procedures reasonably designed" to safeguard such data as required by Regulation S-P's safeguard rule (Regulation 248.30). In particular, among other things, the Respondent's policies and procedures did not provide for:

- Conducting periodic risk assessments;
- Employing a firewall to protect the web server containing customers' information;
- Encrypting client information stored on the server; or
- Establishing procedures for responding to a cybersecurity incident.

Based on these omissions, the Order concludes that, taken as a whole, the Respondent's "policies and procedures for protecting customer records and information were not reasonable to safeguard customer information." [3] As a result, the Order imposes the sanctions discussed above.

Remedial Efforts

The Order notes that, in order to mitigate against any future risk of cyber threats, the Respondent has:

- Appointed an information security manager to oversee data security and protection of its non-public personally identifiable information;
- Adopted and implemented a written information security policy;
- Ceased storing personally identifiable information on its webserver;
- Ensured that any of the personally identifiable information it stores on its internal network is encrypted;
- Installed a new firewall and logging system to prevent and detect malicious incursions; and
- Retained a cybersecurity firm to provide ongoing reports and advice on the firm's information technology systems.

In settling this matter, the SEC considered the Respondent's remedial actions.

Tamara K. Salmon
Associate General Counsel

endnotes

[1] See In the Matter of R.T. Jones Capital Equities Management, Inc., SEC Release No. IA-4201 (September 22, 2015) (the "Order"), which is available at: http://www.sec.gov/litigation/admin/2015/ia-4204.pdf. While the SEC's press release announcing the settlement stated that the firm was charged "with failing to adopt proper cybersecurity policies and procedures prior to breach," the violation involved Regulation S-P and not "cybersecurity policies and procedures." See "SEC Charges Investment Adviser

with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach", SEC Press Release No. 2015-202 (Sept. 22, 2015), which is available at: http://www.sec.gov/news/pressrelease/2015-202.html.

[2] Order at p. 3.

[3] Ibid. See, also, Cybersecurity Guidance No. 2015-02, which was published by the SEC's Division of Investment Management in April 2015 and discusses the Division's views regarding measures that registrants may wish to consider in addressing cyber security risks. This guidance, which is not mentioned in the Order, is available at: http://www.sec.gov/investment/im-guidance-2015-02.pdf.
