Pepper Hamilton LLP
Attorneys at Law

CLIENT ALERT

September 23, 2015

SEC Releases First Cybersecurity Enforcement Action for Failure to Protect Client Data

John M. Ford | fordjm@pepperlaw.com
John P. Falco | falcoj@pepperlaw.com

THE SEC'S FOCUS IN THE ACTION WAS NOT ON THE MANNER OF THE FIRM'S RESPONSES TO THE BREACH OR WHETHER THERE WAS ANY ACTUAL HARM, BUT PREDOMINANTLY ON THE ADEQUACY OF THE FIRM'S WRITTEN POLICIES FOR SAFEGUARDING CUSTOMER INFORMATION AND ITS CYBERSECURITY VULNERABILITIES.

On September 22, the Securities and Exchange Commission (SEC) announced (available at http://www.sec.gov/news/pressrelease/2015-202.html) that it had settled charges brought against an investment adviser under the Safeguards Rule of Regulation S-P for failures to protect client data after the firm's web server had been cyber-attacked. The announcement of the *In the Matter of R. T. Jones Capital Equities Management, Inc.* (*R. T. Jones*) settlement comes squarely on the heels of the Office of Compliance Inspections and Examinations' (OCIE's) "2015 Cybersecurity Examination Initiative" announced on September 15, and underscores the SEC's focus on cybersecurity and cybersecurity enforcement.

The OCIE described its 2015 Cybersecurity Examination Initiative as being intended to "assess cybersecurity preparedness in the securities industry, including firms' ability to protect broker-dealer customer and investment adviser client information." In particular, the OCIE announcement highlighted examination findings on cybersecurity breaches related to weaknesses in basic controls and stated that examiners would focus on cybersecurity-related controls and the implementation of certain firm controls and compliance practices.

The Safeguards Rule requires registered investment advisers to adopt written policies and procedures reasonably designed to (1) ensure 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. In *R. T. Jones*, the SEC alleged that the firm's policies and procedures "taken as a whole" were not reasonably designed to safeguard customer information.

The cybersecurity incident that was the basis for the order in *R. T. Jones* (the Order) occurred in 2013 and involved a suspected Chinese hacker breaching a third-party-hosted web server that held data on clients of R. T. Jones. According to the SEC, the breach may have caused approximately 100,000 individuals, including "thousands" of R. T. Jones's clients, to be "vulnerable to theft." The SEC noted in its Order that the firm had no information indicating that any client suffered financial harm as a result of the cyber-attack and that R. T. Jones had promptly notified affected customers and engaged in a number of other remedial efforts. Nonetheless, R. T. Jones was fined $75,000 as part of an overall settlement for failure to adopt written policies and procedures reasonably designed to protect customer records and information, in violation of Rule 30(a) of Regulation S-P.

Pepper Points

- The SEC's focus in *R. T. Jones* was not on the manner of the firm's responses to the breach or whether there was any actual harm, but predominantly on the adequacy of the firm's written policies for safeguarding customer information and its cybersecurity vulnerabilities.

- The SEC Office of Investor Education and Advocacy recently issued an Investor Alert to provide investors with important steps to take regarding their investment accounts if they become victims of identity theft or a data breach. The Investor Alert is a reminder that regulated entities should remain equally attentive as the SEC's cybersecurity initiatives continue.

- The Order appears to identify a list of minimum standards that the SEC staff would expect an investment adviser to maintain as part of a reasonably designed cybersecurity program, including conducting periodic risk assessments, employing a firewall to protect the web server containing client personally identifiable information (PII), encrypting client PII stored on that server, and establishing procedures for responding to a cybersecurity incident.

- The OCIE staff is expected to continue its focus on cybersecurity by conducting examinations that will focus on key topics, including governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response. When viewed against the backdrop of a lack of actual harm to clients and the relatively low fine assessed against R. T. Jones, the Order demonstrates that, consistent with its so-called "broken windows" approach to enforcement, the SEC will not overlook small violations to avoid breeding an environment of indifference to its rules.