Cybersecurity Initiatives Intensify at the SEC: Enforcement Action against Investment Adviser and a Second Round of Cybersecurity Exams

September 30, 2015 Kit Addleman, Ronald Breaux, Tim Newman, Phong Tran

PRACTICES Privacy and Cybersecurity, Securities and Shareholder Litigation

As cyber threats and news of data breaches make headlines, the Securities Exchange Commission (the "**Commission**") has increased its expectations for investment advisers, broker-dealers, and funds to protect client information from hackers. On September 22, 2015, the Commission brought its first cybersecurity enforcement action against an investment adviser, sending a message to regulated entities. R.T. Jones Capital Equities Management, a St. Louis-based investment adviser, agreed to settle charges that it failed to establish cybersecurity policies and procedures in advance of a data breach affecting a web server containing personal information. With this enforcement action and a new round of examinations on cybersecurity preparedness, the Commission joins a crowded ensemble of government agencies enforcing cybersecurity in the industries they regulate.

The SEC brought the enforcement action under Rule 30(a) of Regulation S-P (the "**Safeguards Rule**"). Under the Safeguards Rule, "[e]very broker, dealer, and investment company, and every investment adviser registered with the Commission must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."

According to the Commission, R.T. Jones stored personally identifiable information ("**PII**")—without modification or encryption—of more than 100,000 clients and other individuals on a third-party hosted web server. The server contained information belonging to R.T. Jones's clients and clients of a retirement plan administrator through which R.T. Jones offers investment advice. A hacker—using IP addresses that traced back to mainland China—gained full access and copy rights to the server in July 2013.

At the time, R.T. Jones failed to have in place any written policies and procedures reasonably designed to safeguard customer information. For example, R.T. Jones did not conduct periodic risk assessments, did not have a firewall on its webserver, did not encrypt PII on that server, and had not established an incident response plan.

R.T. Jones responded promptly to the incident, retaining two cybersecurity firms to investigate the attack (although neither was able to determine whether PII had been accessed or compromised because the attacker destroyed the log files from the time period surrounding the attack). R.T. Jones also promptly notified all individuals affected by the breach and offered each free credit monitoring. To date, the firm has not learned that any of the affected individuals suffered any financial harm as a result of the attack.

The firm also engaged in extensive remedial efforts following the attack. The firm appointed an information security manager, adopted a written information security policy, moved PII to an internal server and began encrypting it, installed a new firewall and logging system, and retained the ongoing services of a cybersecurity firm.

R.T. Jones's prompt response was not enough for the Commission to excuse its violation of the Safeguards Rule, however. Although the Commission noted the firm's extensive remedial efforts and its cooperation in the settlement, R.T. Jones, without admitting or denying the findings, agreed to cease and desist from further violations of the Safeguards Rule, a censure, and a $75,000 civil penalty.

Cybersecurity Examination Initiative

The Commission's enforcement action comes on the heels of its September 15, 2015 risk alert announcing a new Cybersecurity Examination Initiative (the "Initiative") by the Office of Compliance Inspections and Examinations ("**OCIE**"). As part of the Initiative, OCIE will commence a second round of examinations of registered broker-dealers and investment advisers. OCIE's first round of examinations began in April 2014, and OCIE reported the results of those examinations in February 2015 (see our coverage here). OCIE has renewed the Initiative given recent high-profile data breaches and the continuing cybersecurity threat related to financial service firms.

In its exams, OCIE will evaluate a firm's cybersecurity preparedness by gathering information on cybersecurity-related controls and testing implementation of various controls. Specifically, OCIE will focus on the following areas:

- Governance and risk assessment
- Access rights and controls
- Data loss prevention
- Vendor management
- Training
- Incident response

In light of the Commission's continued focus on cybersecurity issues in the financial services industry, broker-dealers and investment advisers should evaluate their firms' cybersecurity policies and incident response preparedness. R.T. Jones responded promptly to the attack on its third-party web server, but the firm's response was not enough to excuse its failure to satisfy the Safeguards Rule. The settlement makes it clear that the Commission expects financial services firms to make cybersecurity—both before and after an incident—a priority.

A copy of the Commission's order can be found here. A copy of the risk alert release can be found here. For additional information, please contact one of the Haynes Boone lawyers listed below.

Kit Addleman
214.651.5783

Ronald W. Breaux
214.651.5688

Taylor H. Wilson
214.651.5615

Ricardo W. Davidovich
212.835.4837

David Siegal
212.659.4995

Emily Westridge Black
512.867.8422

Timothy Newman
214.651.5029
