SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach

FOR IMMEDIATE RELEASE
2015-202

Washington D.C., Sept. 22, 2015 — The Securities and Exchange Commission today announced that a St. Louis-based investment adviser has agreed to settle charges that it failed to establish the required cybersecurity policies and procedures in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals, including thousands of the firm's clients.

The federal securities laws require registered investment advisers to adopt written policies and procedures reasonably designed to protect customer records and information. An SEC investigation found that R.T. Jones Capital Equities Management violated this "safeguards rule" during a nearly four-year period when it failed to adopt any written policies and procedures to ensure the security and confidentiality of PII and protect it from anticipated threats or unauthorized access.

According to the SEC's order instituting a settled administrative proceeding:

- R.T. Jones stored sensitive PII of clients and others on its third party-hosted web server from September 2009 to July 2013.
- The firm's web server was attacked in July 2013 by an unknown hacker who gained access and copy rights to the data on the server, rendering the PII of more than 100,000 individuals, including thousands of R.T. Jones's clients, vulnerable to theft.
- The firm failed entirely to adopt written policies and procedures reasonably designed to safeguard customer information. For example, R.T. Jones failed to conduct periodic risk assessments, implement a firewall, encrypt PII stored on its server, or maintain a response plan for cybersecurity incidents.
- After R.T. Jones discovered the breach, the firm promptly retained more than one cybersecurity consulting firm to confirm the attack, which was traced to China, and determine the scope.
- Shortly after the incident, R.T. Jones provided notice of the breach to every individual whose PII may have been compromised and offered free identity theft monitoring through a third-party provider.
- To date, the firm has not received any indications of a client suffering financial harm as a result of the cyber attack.

"As we see an increasing barrage of cyber attacks on financial firms, it is important to enforce the safeguards rule even in cases like this when there is no apparent financial harm to clients," said Marshall S. Sprung, Co-Chief of the SEC Enforcement Division's Asset Management Unit. "Firms

must adopt written policies to protect their clients' private information and they need to anticipate potential cybersecurity events and have clear procedures in place rather than waiting to react once a breach occurs."

The SEC's order finds that R.T. Jones violated Rule 30(a) of Regulation S-P under the Securities Act of 1933. Without admitting or denying the findings, R.T. Jones agreed to cease and desist from committing or causing any future violations of Rule 30(a) of Regulation S-P. R.T. Jones also agreed to be censured and pay a $75,000 penalty.

Also today, the SEC's Office of Investor Education and Advocacy published a new Investor Alert, "*Identity Theft, Data Breaches, and Your Investment Accounts*." The alert, also available on Investor.gov, the SEC's website for individual investors, offers steps for investors to take regarding their investment accounts if they become victims of identity theft or a data breach.

The SEC's investigation was conducted by Thu Ta and supervised by Paul Montoya of the Chicago Regional Office and the Asset Management Unit. The examination that led to the investigation was conducted by Patrick Elgrably, Sarah Kuhn, Bradley Kartholl, Stacey Gohl, and Thomas Kirk of the Chicago office's investment adviser/investment company examination program.

###

Related Materials

- SEC order
- Investor Alert - Identity Theft, Data Breaches, and Your Investment Accounts