SEC Fines Investment Firm $75,000 for Failing to Adopt Written Cybersecurity Policies and Procedures

Insights
10.08.15

Investment firm R.T. Jones Capital Equities Management (R.T. Jones) has agreed to settle with the Securities and Exchange Commission (SEC) and pay a $75,000 penalty over charges that it failed to adopt written policies and procedures to protect customer information before a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals.

According to the SEC's order, R.T. Jones stored PII of clients and prospective clients on its third party-hosted web server *without adopting written policies* and procedures regarding the security and protection of that information from anticipated threats or unauthorized access. R.T. Jones allegedly did not conduct periodic risk assessments, employ firewalls, encrypt PII, or establish procedures for responding to a cybersecurity incident.

In July 2013, R.T. Jones discovered a potential cybersecurity breach at its third party-hosted web server. R.T. Jones retained a cybersecurity firm that reportedly traced the attack back to mainland China. The cybersecurity firm was unable to confirm whether PII stored on the server had actually been accessed or compromised during the breach and to date R.T. Jones has not learned of any information indicating that a client has suffered any financial harm as a result of the cyberattack.

Notwithstanding the absence of financial harm, the SEC found that R.T. Jones willfully violated Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30 (a)) – the "Safeguards Rule" -which requires registered investment advisers to adopt written policies and procedures that are reasonably designed to safeguard customer records and information.

"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," Marshall S. Sprung, co-chief of the SEC Enforcement Division's Asset Management Unit, said in the SEC release. "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."

What is the Safeguards Rule?
The Federal Trade Commission (FTC) issued the Safeguards Rule as part of the Gramm-Leach-Bliley Act (GLB), which requires financial institutions to develop a written security plan to protect customer information. The definition of "financial institutions" is broad and applies to all businesses

customer information. The definition of "financial institutions" is broad and applies to all businesses "significantly engaged" in providing financial services or products. As part of the security plan, each covered company must:

- Designate one or more employees to coordinate its information security program;
- Identify and assess the risks of customer information in each relevant area of the company's operation, and evaluate the effectiveness of current safeguards for controlling these risks;
- Design and implement a safeguards program, and regularly monitor and test it;
- Select service providers that can maintain appropriate safeguards and contractually require service providers to implement and maintain such safeguards; and,
- Evaluate and adjust the program in light of the results of the testing and monitoring, or changes in operations or business arrangements.

In its guidance on "Complying with the Safeguards Rule", the FTC recommends:

- Checking references or doing background checks before hiring employees who will have access to customer information.
- Asking new employees to sign agreements to follow the company's confidentiality and security standards for handling customer information.
- Limiting access to customer information to employees who have a business reason to see it.
- Controlling access to sensitive information by requiring employees to use strong passwords that must be changed on a regular basis.
- Using password-activated screen savers to lock employee computers after a period of inactivity.
- Training employees to take basic steps to maintain security, confidentiality, and integrity of customer information.
- Regularly reminding employees of the company's policy and the legal requirement to keep customer information secure and confidential.
- Developing policies for employees who telecommute.
- Imposing disciplinary measures for security violations.
- Preventing terminated employees from accessing customer information by immediately deactivating passwords and user names.

As the FTC notes, the success of any information security plan depends on the employees who implement it.

Related People

Melissa A. Dials
Partner
440.740.2108
Email