CARLTON FIELDS

Investment Adviser Settles SEC Charges After Data Breach

September 28, 2015

Last week, the Securities and Exchange Commission (SEC) settled charges against a registered investment adviser for failing to comply with Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) ("Safeguards Rule"). The Safeguards Rule requires that every registered investment adviser must adopt written policies and procedures reasonably designed to: (1) insure 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. According to the SEC order, St. Louis, Missouri adviser R.T. Jones Capital Management, Inc. had agreements with a retirement plan administrator and various retirement plan sponsors to provide a managed account service offering model portfolios to retirement plan participants. Individuals seeking to enroll in the program were instructed to fill out a questionnaire on the adviser's public website regarding their investment objectives and risk tolerance. To verify eligibility to enroll in the program, the adviser required prospective clients to log onto its website by entering their name, date of birth and social security number (PII). The login information was then compared against the PII of eligible plan participants, which was provided to the adviser by plan sponsors. The adviser stored this PII, without modification or encryption, on its third party-hosted web server. To facilitate the verification process, the plan sponsors provided the adviser with information about all of their plan participants even for those who did not select the managed

account option. Thus, even though the adviser had fewer than 8,000 plan participant clients, its web server contained the PII of over 100,000 individuals. In July 2013, the adviser discovered a potential breach of the third party-hosted web server and promptly retained multiple cybersecurity firms that traced the attack to mainland China. The breach potentially allowed the intruder free reign over the access and copy rights of the PII data. The adviser notified all affected individuals and offered free identity monitoring. To date, the breach has not caused any financial losses to the affected individuals. Despite the adviser's quick response and actions to mitigate the breach impact, the SEC concluded that the adviser's failure to adopt written policies and procedures reasonably designed to safeguard customer records and information resulted in the breach and a violation of the Safeguards Rule. The adviser entered into a cease and desist order and paid a $75,000 penalty. This matter is instructive on several points:

- Just because no one is financially harmed does not mean that you cannot be sanctioned.
- You must adopt and implement a written information security policy (WISP).
- You should have personnel responsible for overseeing data security and protection of PII.
- PII should be encrypted.
- Systems should be put in place to prevent and detect breaches.
- Ongoing systems monitoring and regular reporting to management on the effectiveness of security systems should be instituted.
- Know what your outside vendors and suppliers are doing to protect PII and other proprietary business information they have access to.
- Collect the minimum amount of PII needed for your business purposes.

This is not an exhaustive list of all the steps registered investment advisers should be taking but does serve as a reminder that the SEC is serious about making sure investment advisers are taking action to mitigate cyber risks.

Related Practices

Cybersecurity and Privacy
Securities Litigation and Enforcement
Technology
Securities Transactions and Compliance

Related Industries

Technology