>>>FAIRVIEW FLASH REPORT <<<
Investment Adviser Settles with the SEC for Failing to Adopt Cybersecurity Policies and Procedures

WHAT HAPPENED?	Yesterday, the SEC announced its settlement with R.T. Jones for failing to adopt proper cybersecurity procedures prior to a breach that exposed personally identifiable information ("PII") of nearly 100,000 individuals, including clients. The charges were brought under Rule 30(a) of Regulations S-P of the Securities Act of 1933, which requires registered advisers to adopt cybersecurity policies and procedures designed to protect client information. In this case, unlike many cybersecurity-related enforcement actions, there was no apparent financial harm to R.T. Jones clients. Nevertheless, the SEC stressed the importance of enforcing the rule as cybersecurity breaches continue to increase.
WHAT ARE THE DETAILS?	According to the SEC's investigation, when the adviser's web server was hacked in 2013, the firm had yet to: • Adopt written policies and procedures to protect client information; • Adopt an incident response plan for cybersecurity incidents; • Conduct periodic risk assessments; • Implement a firewall; or • Encrypt PII stored on the firm server. After the breach R.T. Jones retained cybersecurity consulting firms to confirm the breach and determine the scope. The adviser also provided prompt notice and free identity theft monitoring to the affected individuals. To date, no clients are believed to have suffered financial harm as a result of the breach. Regardless of the steps taken after the breach and the lack of financial harm, the adviser's failure to adopt proper written policies and procedures provided sufficient grounds for the SEC to bring the suit. As part of the settlement, the adviser agreed to pay a $75,000 fine.
WHAT IS NEXT?	With cybersecurity breaches on the rise, it is of utmost importance for investment advisers to adopt customized, written policies and procedures to protect client information. Advisers should consider including requirements such as periodic risk assessments, encryption of PII, and firewall implementation. An incident response plan or disaster recovery plan should also be adopted to govern cybersecurity breaches. Please contact Fairview with any questions or concerns you have regarding your current cybersecurity policies and procedures.

Source: SEC Press Release Dated 9.22.2015