

SEC Fines Investment Firm for Inadequate Cybersecurity

October 1, 2015

On September 22, 2015, the U.S. Securities and Exchange Commission (“SEC”) [fined](#) investment adviser R.T. Jones Capital Equities Management Inc. \$75,000 for its lack of cybersecurity protections which contributed to a 2013 system hack that compromised the personal data of approximately 100,000 people. In addition to the fine, the company agreed to strengthen its data security measures as part of its settlement with the SEC. This action follows just one week after the SEC announced its second round of examinations into the cybersecurity policies of broker-dealers and investment firms (like R.T. Jones), clearly demonstrating the SEC’s continued focus on the securities industry’s cybersecurity preparedness. R.T. Jones is a relatively small retirement investment firm with only about 8,400 clients (with around \$480 million in assets). The breach compromised the personal data of approximately 100,000 people, however, because the firm used a managed account called Artesys which provided it with access to more than 100,000 individual profiles. When R.T. Jones system was breached, the hackers, therefore, were able to access the personal data of substantially more individuals than just the firm’s clients. The breach was traced back to mainland China, although the two cybersecurity firms hired by the firm were unable to ascertain the full nature of the hack. After the 2013 hack, the SEC investigated the firm. Despite the considerable amount of sensitive information stored on R.T. Jones’ servers, the SEC found that from 2009 until the 2013 hack the company failed to adopt even elementary safety features, such as data encryption and the use of a firewall. The SEC also found that this lack of consumer data protection safeguards violated the SEC’s 2000 Safeguards Rule of the 1933 Securities Act. Though R.T. Jones did not comment upon the SEC’s findings, the company agreed to the \$75,000 fine, as well as to cease and desist from any further violations of the Safeguards Rule. R.T. Jones also has installed an information security manager to oversee data protection, implemented a written security policy, stopped storing the personal information of clients on a third-party server, and started using internal encryption and firewalls. Although the fine is relatively small, the SEC’s action against R.T. Jones clearly demonstrates the agency’s commitment to the securities industry’s ability to protect the integrity of the market system and customer data from cyberattack. It is likely that subsequent enforcement actions will involve larger fines should larger entities be involved. Additionally, the SEC’s action makes clear that individuals who raise concerns regarding cybersecurity violations at broker-dealers and investment firms are reporting violations of SEC rules and regulations and, as such, are protected by the anti-retaliation provisions of the [Dodd-Frank Act](#).