SEC Says No More Mr. Nice Guy on Investment

Digital Media and Data Privacy Law Blog

on 09.24.2015
Posted in Cyberattack, Privacy

Over the last couple years, the SEC's cybersecurity bark has been worse than its bite. Its Office of Compliance, Inspections, and Examinations issued examination priorities in 2014. Commissioner Aguilar warned public company boards that they had better get smart about the topic a few months later. The results of OCIE's cybersecurity exam sweep were released in March of this year. And the Investment Management Division said words, not many words, about investment advisers' responsibilities in this area in July.

Alleged Facts

What it hasn't done recently is sue somebody for violating Reg. S-P. But yesterday it did. According to the SEC's settled administrative order:

- St. Louis-based R.T. Jones Capital Equities Management stored sensitive personally identifiable information (PII) of clients and others on its third party-hosted web server from September 2009 to July 2013.
- Throughout this period, 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.
- An unknown hacker gained access to the firm's web server in July 2013, rendering the PII of more than 100,000 individuals, including thousands of R.T. Jones's clients, vulnerable to theft.

The Safeguards Rule

Whoops. But while all of that sounds bad, it's not actually what the firm is being sued over. At issue is Reg. S-P's Rule 30(a), the Safeguards Rule, which says, "Every broker, dealer, and investment company, and every investment adviser registered with the Commission must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." And unfortunately, R.T. Jones allegedly failed entirely to adopt written policies and procedures reasonably designed to safeguard customer information. Put another way, if R.T. Jones did have written policies and procedures designed to avoid the failures bulleted above, the cyber attack might have been avoided and we wouldn't be here. It's paying a $75,000 civil penalty to put this matter behind it.

Fortunately, to date, R.T. Jones has not received any indications of a client suffering financial harm as a result of the attack. And the firm appears to have acted quickly and responsibly once it did discover the breach.

Three Thoughts

I have three quick thoughts. First, this is a relatively easy case for the SEC to bring. RT. Jones didn't just have inadequate policies and procedures. According to the SEC's order, it didn't have *any* written policies and procedures reasonably designed to safeguard its clients' PII. Second, over 90% of the individuals whose information was compromised were not even R.T. Jones clients, but participants in an investment plan in which R.T. Jones had joined. The information appears to have been useful to R.T. Jones in the aggregate, but perhaps not so as to individuals. If not, the firm might have purged that information from its systems and avoided the liability from losing their data. Finally, periodic risk assessments, firewalls, encryption, and a cybersecurity response plan seem like good ideas right now. But you knew that already.