Published on *The National Law Review* https://natlawreview.com

SEC Enforcement Action Portends Rewards for Cybersecurity Whistleblowers

Article By:

Dallas Hammer

The Securities and Exchange Commission announced on Tuesday that it had settled charges that investment adviser R.T. Jones Capital Equities Management failed to establish the required cybersecurity policies and procedures. This is the latest reason to conclude that cybersecurity issues have become a key enforcement priority for the SEC. And with the ever-increasing prevalence of cyber-attacks, this will likely remain a hot-button issue for the foreseeable future. In turn, whistleblower tips that touch on cybersecurity may receive additional scrutiny. It is also an important reminder of the broad scope of anti-retaliation protections under Section 806 of the Sarbanes-Oxley Act ("SOX") and Section 922 of the Dodd-Frank Act ("Dodd Frank").

R.T. Jones stored sensitive information about its clients and others on its third party-hosted web server from September 2009 to July 2013, according to the SEC's order instituting a settled administrative proceeding. The firm's web server was hacked in July 2013, exposing to theft the sensitive information of more than 100,000 people, including thousands of R.T. Jones' clients. At the time, the firm had no written policies and

procedures reasonably designed to safeguard customer information, according to the order. Despite the breach, there was no evidence that any clients suffered financial harm because of the attack to date, and R.T. Jones took prompt remedial actions.

The SEC's regulations contain a "safeguards rule," which requires every registered broker, dealer, investment company, and investment adviser to adopt written policies and procedures reasonably designed to protect customer records and information. The SEC's order found that R.T. Jones violated the safeguards rule, and R.T. Jones settled the charges by agreeing to be censured, pay a $75,000 penalty, and commit no further violations. R.T. Jones did not admit or deny the SEC's findings.

This particular case is instructive in several ways. The SEC took enforcement action though there was no actual economic harm and the firm took prompt remedial actions to inform and protect its clients, investigate the breach, and ensure future breaches did not recur. Further, investment advisers are among the smallest businesses the SEC regulates, and with seven employees, R.T. Jones is no exception.

And though the R.T. Jones matter may be novel, it is almost certainly only the first of many such cases. In April 2014, Commissioner Luis Aguilar addressed his personal view of the threat cyber-attacks pose. He said, "It is here to stay and cannot be ignored." In that same speech, Mr. Aguilar then stated that "cybersecurity would be an exam priority. You should expect that SEC examiners will be reviewing whether asset managers have policies and procedures in place to prevent and detect cyber-attacks and whether they are properly safeguarding their systems against security risks."

Less than two weeks later, the SEC announced its Cybersecurity Examination Initiative ("CEI"). Under the initiative, the SEC examined 57 registered broker-dealers and 49 registered investment advisers to better understand how broker-dealers and advisers address the legal, regulatory, and compliance issues associated with cybersecurity.

In January 2015, the SEC announced that cybersecurity would be a 2015 examination priority, and the next month it released the 2014 CEI examination report. The report found that almost all the examined firms had policies in place and most of the firms had experienced a cybersecurity incident. However, the report declined to draw any conclusions about the findings.

Ultimately, the SEC reiterated its view that the cybersecurity of registered investment companies and investment advisers is an important issue. And the SEC cited several factors, including the February 2015 report, in stressing the need for firms to review their cybersecurity measures. In April 2015, the SEC released cybersecurity guidance outlining recommendations for effective policies and procedures.

Then, just this past week, the Commission's Office of Compliance Inspections and Examinations announced a renewed 2015 Cybersecurity Examination Initiative.

And finally, on Wednesday – the day after the Commission announced the R.T. Jones settlement – Mr. Aguilar spoke to the Advisory Committee on Small and Emerging companies. He stressed the need to protect investors while considering the appropriate level of reporting for small businesses. Mr. Aguilar singled out cybersecurity despite the fact that it was not on the meeting's agenda. He acknowledged that although cybersecurity had historically not been a regulatory focus, it is an increasing concern for investors. Small firms are particularly attractive targets for hackers, and Mr. Aguilar opined that despite these threats, the small business sector was not taking cybersecurity as

seriously as it should. He cited a survey that found 27 percent of sampled small firms had no cybersecurity protocols and admonished that the “apathy is ill-advised.”

In short, cybersecurity has become an enforcement priority during the past year. The Commission’s examination prioritization, emphasis on the subject in public statements, and the lessons from the R.T. Jones case indicate that the SEC will aggressively pursue firms under its oversight that are not preparing for cyber-attacks, regardless of the firm’s size, good intentions, or remedial actions. It is likely to remain a priority for as long as cybersecurity remains a prominent public issue, i.e., for the foreseeable future.

This also means that whistleblower tips pertaining to cybersecurity issues may receive a discerning review from the SEC’s Office of the Whistleblower. Though the key to any successful whistleblower tip is credible, specific information about a violation, tips identifying claims that are enforcement priorities can reasonably be expected to generate interest. Employees should be particularly aware of deficient protocols, procedures and practices regarding:

- Governance and Risk Assessment;
- Access Rights and Controls;
- Data Loss Prevention;
- Vendor Management;
- Training; and
- Incident Response

The R.T. Jones case and the SEC’s focus on cybersecurity issues, also serve as an important reminder of the broad scope of whistleblower protections under SOX and Dodd-Frank. Most people familiar with these anti-retaliation provisions likely know them in the context of employees blowing the whistle on securities or accounting fraud. However, SOX covers disclosures of an employee’s reasonable belief that there has been (or likely will be) a violation of “*any* rule or regulation of the Securities and Exchange Commission” (emphasis added). Similarly, Dodd-Frank’s whistleblower protection provision extends to disclosures of any “law, rule, or regulation subject to the jurisdiction of” the SEC. And though the SEC has traditionally focused on protecting investors by investigating and prosecuting shareholder fraud and similar violations, the SEC’s regulations are actually quite broad and cover numerous aspects of the businesses under the SEC’s regulatory oversight. For example, disclosing that a publicly-traded company has failed to meet its obligations under the “safeguards rule” could very well constitute protected activity under SOX and Dodd-Frank.

National Law Review, Volumess V, Number 269