Rocky Mountain Securities Conference: Cybersecurity Takes Center Stage

Given the security industry's increased use of information technology and the constant evolution of cyber threats, cybersecurity will continue to demand significant attention from regulators and industry participants in the coming year. Recent cases indicate the significant business, financial, and reputational consequences of a cyber breach, as well as the importance for securities firms and market participants to demonstrate compliance and preparation in this area.

In recent years, cyber threats have evolved from the theft of personal information to extortion attempts, where cyber criminals lock up or encrypt an entity's data using malware and literally hold it hostage for a ransom. Similarly, cyber crooks can bombard an entity's online services through a distributed denial of service or "DDoS" attack, rendering the services unavailable to customers, also in order to seek a ransom. Cyber criminals have also compromised the systems of securities industry participants to steal information used to commit other crimes, such as insider trading.[i]

On Friday, May 6, 2016, at the Securities and Exchange Commission (SEC) and the Colorado Bar Association's 48th annual Rocky Mountain Securities Conference in Denver, SEC Deputy Director Stephanie Avakian emphasized the agency's focus on cybersecurity within its enforcement program. She identified three areas of focus, including a registrant's failure to comply with SEC cyber rules and regulations concerning the protection of personal identifying information (PII), the theft of information to facilitate insider trading, and disclosure failures relating to cyber intrusions. She noted that the SEC has brought cases in the first two areas but has yet to bring a case relating to disclosure failures, although she did not rule out such a case in the future under the right set of facts.

In her remarks, Avakian identified *R.T. Jones*[ii] as an example of a case where a securities firm failed to comply with SEC rules and regulations relating to cybersecurity. Other regulators also highlighted this case during the conference. In *R.T. Jones*, the SEC filed a settled administrative proceeding against the St. Louis-based investment adviser for failing to adopt proper cybersecurity policies and procedures prior to a cyber breach that compromised the personal information of approximately 100,000 individuals. As described in the SEC Order, R.T. Jones had stored client PII, such as names, birth dates, and Social Security numbers, on a third-party host server without modification or encryption. In 2013, a cyberattack traced to mainland China compromised the third-party server. R.T. Jones was unable to determine the full nature and extent of the intrusion or whether its clients' PII had been accessed or compromised, since the intruder had covered its tracks.

In the settled order,[iii] the SEC enumerated R.T. Jones' specific failures to comply with SEC cyber rules and regulations including the failures to conduct periodic risk assessments, to employ a firewall to protect the web server containing client PII, to encrypt client PII on the server, and to establish procedures for responding to a cybersecurity incident. Based largely on R.T. Jones' cooperation, remedial efforts, and the relative scope of the cyber breach, the SEC censured the adviser and ordered it to cease and desist from committing or causing future SEC rule violations and to pay a $75,000 civil penalty.

While the sanctions against R.T. Jones were relatively modest, one can envision significant sanctions under the wrong set of facts, particularly where large-scale cyber intrusions result in significant investor

410 17th Street, Suite 2200
Denver, Colorado 80202

harm. Aside from monetary sanctions, the reputational harm that can result from a cybersecurity breach can be difficult to measure. For these reasons, securities firms and other market participants need to be vigilant in this area, particularly in light of the increase and continued evolution of cybersecurity threats.

Securities regulators will remain focused on cybersecurity given the risks that it poses to fair, orderly, and efficient capital markets. In the unfortunate event of a breach, securities firms and market participants must be prepared to provide answers to regulators regarding the policies and procedures they have established, and the resources they have devoted to cybersecurity. The ability to demonstrate diligence in this area will help put industry participants in the best possible position to deal with securities regulators should the need arise.

*Brownstein's **Securities Litigation & Enforcement Group** helps clients navigate challenges ranging from government enforcement actions to courtroom representation. Our litigators advise on SEC compliance and Financial Industry Regulatory Authority arbitrations, security fraud and cybersecurity issues. Brownstein's team provides guidance in an era of increasing scrutiny and enhanced regulation on how public and private companies, boards of directors and general counsel handle securities, discuss company performance and structure stock options and compensation packages, among other related issues.*

John V. McDermott
Shareholder
jmcdermott@bhfs.com
303.223.1118

Lawrence W. Treece
Shareholder
ltreece@bhfs.com
303.223.1257

Jeffrey S. Rugg
Shareholder
jrugg@bhfs.com
702.464.7011

Thomas J. Krysa
Shareholder
tkrysa@bhfs.com
303.223.1270

Emily R. Garnett
Associate
egarnett@bhfs.com
303.223.1171

Carrie E. Johnson
Associate
cjohnson@bhfs.com
303.223.1198

Joshua A. Weiss
Associate
jweiss@bhfs.com
303-223-1268

David B. Meschke
Associate
dmeschke@bhfs.com
303.223.1219

Elizabeth G. Tillotson
Associate
etillotson@bhfs.com
303.223.1173

Maximilien D. Fetaz
Associate
mfetaz@bhfs.com
702.464.7083

This document is intended to provide you with general information regarding cybersecurity for securities firms. The contents of this document are not intended to provide specific legal advice. If you have any questions about the contents of this document or if you need legal advice as to an issue, please contact the attorneys listed or your regular Brownstein Hyatt Farber Schreck, LLP attorney. This communication may be considered advertising in some jurisdictions.

---

[i] *SEC v. Dubovoy, et al.*, Civil Action No. 2:15-cv-06076-MCA-MAH (D. N.J., filed August 10, 2015).
[ii] *In the Matter of R.T. Jones Capital Management, Inc.*, A.P. File No. 3-16827, Investment Advisers Act Rel. No. 4204 (September 22, 2015).
[iii] *Id.*

410 17th Street, Suite 2200
Denver, Colorado 80202