September 24, 2015

SEC Enforcement Action Alleges an Adviser Failed to Adopt Adequate Cybersecurity Policies and Procedures; SEC Issues an Investor Alert on Data Theft

On September 22, 2015, the Securities and Exchange Commission (SEC) filed a settled administrative proceeding[1] alleging that a registered investment adviser failed to adopt cybersecurity procedures in violation of an SEC rule. The adviser consented to a censure, a cease and desist order, and a $75,000 fine.

According to the SEC enforcement action, between 2009 and 2013, an adviser "stored sensitive personally identifiable information (PII) of clients and other persons on its third party-hosted web server without adopting written policies and procedures regarding the security and confidentiality of that information and the protection of that information from anticipated threats or unauthorized access. In July 2013, the firm's web server was attacked by an unauthorized, unknown intruder, who gained access rights and copy rights to the data on the server. As a result of the attack, the PII of more than 100,000 individuals, including thousands of [the adviser]'s clients, was rendered vulnerable to theft."

The SEC alleged that the adviser violated the relevant SEC rule – Rule 30(a) of Regulation S-P – because its "policies and procedures for protecting its clients' information did not include, for example: conducting periodic risk assessments, employing a firewall to protect the web server containing client PII, encrypting client PII stored on that server, or establishing procedures for responding to a cybersecurity incident."

Rule 30(a) of Regulation S-P expressly requires that every entity meeting the definition of a broker, dealer or investment company under applicable law (whether registered or not), and every investment adviser registered with the Commission, adopt written policies and procedures "reasonably designed" to ensure the security and confidentiality of customer records and information ("customer data"); protect against any anticipated hazards and threats to the security or integrity of customer data; and protect against unauthorized access to or use of customer data that could end up causing substantial harm or inconvenience to any customer.[2]

In accepting the adviser's settlement, the SEC gave credit to the adviser for its response to the cyber-attack, which included the following:

1. the adviser retained two cybersecurity firms to investigate the breach;

[1] Click here to access In re R.T. Jones Capital Equities Management, Inc., Admin Pro. 3-16827 (Sept. 22, 2015).

[2] Click here to access the full text of Rule 30(a) Regulation S-P.

For more information, please contact any of the following members of Katten's **Financial Services**, **Litigation and Dispute Resolution**, or **Privacy, Data and Cybersecurity** practices.

Richard D. Marshall
+1.212.940.8765
richard.marshall@kattenlaw.com

Wendy E. Cohen
+1.212.940.3846
wendy.cohen@kattenlaw.com

Alan J. Brudner
+1.212.940.6362
alan.brudner@kattenlaw.com

Gary DeWaal
+1.212.940.6558
gary.dewaal@kattenlaw.com

David Y. Dickstein
+1.212.940.8506
david.dickstein@kattenlaw.com

Doron S. Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

2. customers were promptly notified of the breach and offered free identity monitoring through a third-party firm. There has been no indication that any customer's personal information has been used improperly; and

3. the adviser "appointed an information security manager to oversee data security and protection of PII, and adopted and implemented a written information security policy. Among other things, the firm no longer stores PII on its webserver and any PII stored on its internal network is encrypted. The firm also has installed a new firewall and logging system to prevent and detect malicious incursions. Finally, [the firm] has retained a cybersecurity firm to provide ongoing reports and advice on the firm's information technology security."

According to the SEC, despite retaining the cybersecurity consulting firms to investigate the breach, the adviser was never able to determine whether any PII was compromised. In addition, the adviser has, to date, "not learned of any information indicating that a client has suffered any financial harm as a result of the cyber-attack."

Simultaneous with announcing this enforcement action, the SEC issued an investor alert recommending that investors take the following steps if they suspect they have been the victim of an identity theft:

1. contact their financial institution immediately if they suspect personal financial information has been stolen;

2. immediately change online passwords;

3. consider closing compromised accounts;

4. if available, activate a two-step verification process where an account cannot be accessed until a second password, sent to a secure location, is used;

5. monitor all accounts for suspicious activity;

6. place a fraud alert on credit files;

7. monitor credit reports; and

8. create an Identity Theft Report by reporting the incident to the Federal Trade Commission (FTC) by completing its online complaint form, then reporting the incident to the local police, who also should receive the FTC online complaint form.

For information on how financial services firms might help protect themselves against cyber-threats, click here to access the advisory entitled, "Cyber-Attacks: Threats, Regulatory Reaction and Practical Proactive Measures to Help Avoid Risks" by Katten Muchin Rosenman LLP dated June 24, 2015.