Proskauer

SEC Announces Cybersecurity Enforcement Action

September 24, 2015

On September 22, 2015, the Securities and Exchange Commission (SEC) announced the settlement of an enforcement action against a St. Louis-based registered investment adviser (Adviser) brought under Rule 30(a) of Regulation S-P (Safeguards Rule). The SEC Order charged the Adviser with violating the Safeguards Rule by failing to adopt written cybersecurity policies and procedures reasonably designed to protect customer records and information.

The Safeguards Rule

The Safeguards Rule, adopted by the SEC in 2000 and subsequently amended in 2005, requires every SEC-registered investment adviser (among other SEC registrants) to adopt written policies and procedures addressing administrative, technical and physical safeguards that are reasonably designed to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

The SEC Order

According to the SEC Order, from at least September 2009 through July 2013, the Adviser, which did not have custody of client assets, stored sensitive personally identifiable information (PII) of its clients and other persons on its third party-hosted web server without adopting written policies and procedures regarding the security, confidentiality and protection of such PII from anticipated threats or unauthorized access. Among other things, the Adviser's policies and procedures failed to include 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.

In July 2013, an unauthorized and unknown intruder gained access to the data on the server, thereby rendering the PII of more than 100,000 individuals, including the PII of clients of the Adviser, vulnerable to theft. Following the Adviser's discovery of the potential breach, the Adviser retained several cybersecurity consulting firms to confirm the attack and assess the scope of the breach. In the end, the cybersecurity firms could neither determine the full nature and extent of the breach nor determine whether PII had been accessed or compromised. Following the breach, the Adviser notified all individuals whose PII may have been compromised and offered such persons free identity-monitoring through a third-party provider. As of the date of the SEC Order, the Adviser had not learned of any information indicating that a client had suffered any financial harm as a result of the cyber attack.

Nevertheless, based on the foregoing, the SEC concluded that the Adviser failed to adopt written policies and procedures reasonably designed to safeguard its clients' PII and, as a result, charged the Adviser with violating the Safeguards Rule.

To mitigate against any future risk of cyber threats, 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 Adviser no longer stores PII on its web server and any PII stored on its internal network is encrypted. It also installed a new firewall and logging system to prevent and detect malicious incursions and retained a cybersecurity firm to provide ongoing reports and advice on the Adviser's information technology security.

Without admitting or denying the findings set forth in the SEC Order, the Adviser agreed to be censured, to cease and desist from committing or causing any violations and any future violations of the Safeguards Rule and to pay a civil penalty of $75,000 to the SEC. In determining to accept the Adviser's offer, the SEC considered the remedial acts promptly undertaken by the Adviser and the cooperation it afforded the SEC Staff.

The SEC's investigation was conducted by representatives of the Chicago Regional Office and the Asset Management Unit.

Implications

This enforcement action highlights the SEC's continued focus on cybersecurity, one of the SEC's Office of Compliance and Inspections and Examination's examination priorities for 2015, as well as the SEC's willingness to bring an enforcement action against a registered investment adviser, despite there being no apparent financial harm to such adviser's clients. As noted by Marshall S. Sprung, Co-Chief of the SEC Enforcement Division's Asset Management Unit, "[firms] need to anticipate potential cybersecurity events and have clear procedures in place rather than waiting to react once a breach occurs."

Concurrent with the announcement of this enforcement action, the SEC's Office of Investor Education and Advocacy issued an Investor Alert setting forth important steps to take if an investor becomes a victim of identity theft or a data breach.

If you have any questions regarding the enforcement action or cybersecurity issues in general, please contact your usual contact at Proskauer or any of the Proskauer lawyers listed in this alert.

Related Professionals

- **Arnold P. May**
  Partner
- **Amanda H. Nussbaum**
  Partner
- **Scott S. Jones**
  Partner
- **Charles (Chip) Parsons**
  Partner
- **Bruno Bertrand-Delfau**
  Partner
- **Jamiel E. Poindexter**
  Partner
- **Marc A. Persily**
  Partner
- **Ira G. Bogner**

Managing Partner

- **Sarah K. Cherry**
  Partner
- **Bruce L. Lieb**
- **Nigel van Zyl**
  Partner
- **Michael R. Suppappola**
  Partner
- **Timothy W. Mungovan**
  Chairman of the Firm
- **Mary B. Kuusisto**
  Partner
- **Niamh A. Curry**
  Partner
- **Malcolm B. Nicholls III**
  Partner
- **David W. Tegeler**
- **Howard J. Beber**
  Partner
- **Robin A. Painter**
- **Stephen T. Mears**
  Partner