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

SEC Issues $1 Million Identity Theft Rule Fine

Article By:

Liisa M. Thomas

Amber C. Thomson

The Securities and Exchange Commission recently settled with Voya Financial Advisors, Inc. for alleged violation of Regulation S-ID (otherwise known as the Identity Theft Red Flags Rule) and Regulation S-P (otherwise known as the Safeguards Rule). According to the SEC, Voya had failed to implement a written identity theft program as required of broker-dealers and investment advisors by the Identity Theft Red Flags Rule, and failed to have written policies and procedures to protect customer records and information as required by the Safeguards Rule. Specifically, in April 2016 intruders impersonated Voya independent contractors and contacted the company's technical support line. They asked for a reset of the contractors' passwords, which support staff did, giving them temporary passwords over the phone. The bad actors used these credentials to gain access to the company's proprietary web portal. The portal contained personally identifiable information of Voya customers, and according to the SEC the bad actors were able to access personal information for at least 5,600 of Voya's customers. This information included address, date of birth, last four digits of Social Security numbers, and email addresses. And, for at least 2,000, full Social Security number or other government-issued ID number. Voya was contacted by one of the targeted contractors, who said that he had gotten an email about a password change, but he had not requested the change. After receiving this alert of suspicious activity Voya took some steps, according to the SEC, but not sufficient ones, including not terminating the bad actors' access to the compromised accounts.

Of concern for the SEC in reaching its decision was the lack of personnel training and the failure by Voya to update its program in response to changing risks. In particular, the Safeguard Rule requirements were not met according to the SEC because the procedures relating to password resets, terminating web sessions, identifying high-risks and creation/alternation of user accounts were not designed reasonably. Also of concern to the SEC was its conclusion that the policies the company had in place were not designed to be applied to contractor representatives (i.e., the type of accounts impacted). The Identity Theft Rule was not met, the SEC charged, because although the company had created a written program in 2009, it had not reviewed and updated the program, provided sufficient training, nor did it include appropriate policies and procedures to respond to the identity theft red flags that were detected as part of this April 2016 intrusion. The SEC also noted that the company had outsourced most of its cyber functions.

After the incident Voya took several steps which the SEC took into consideration, including blocking

malicious IP addresses, revising its policies to prevent issuing temporary passwords by phone, and sending breach notices with one year of credit monitoring. As part of the settlement, Voya agreed to hire a compliance consultant under a two-year agreement, which consultant will issue a report to the company and to the SEC. Voya has agreed to follow the consultant's recommended changes. Voya also agreed to pay a $1 million fine, which is reported as the first fine the SEC has issued under the Identity Theft Red Flags Rule.

Putting it Into Practice: Companies should keep in mind that after a data incident, regulators may closely scrutinize the sufficiency of their data security measures. This holds true not just for entities in regulated industries like broker dealers and investment advisors, but those in other industries as well.

National Law Review, Volume VIII, Number 295