

Client Alert

October 2018

SEC Fines Broker-Dealer \$1 Million in First Enforcement Action Under Identity Theft Rule

On September 26, 2018, the SEC announced a settlement with Voya Financial Advisers, Inc. (Voya), a registered investment advisor and broker-dealer, for violating Regulation S-ID, also known as the “Identity Theft Red Flags Rule,” as well as Regulation S-P, the “Safeguards Rule.” Together, Regulations S-ID and S-P are designed to require covered entities to help protect customers from the risk of identity theft and to safeguard confidential customer information. The settlement represents the first SEC enforcement action brought under Regulation S-ID.

I. The Identity Theft Red Flags Rule

Regulation S-ID covers SEC-registered broker-dealers, investment companies and investment advisors and mandates a written identity theft program, including policies and procedures designed to:

- Identify relevant types of identity theft red flags;
- Detect the occurrence of those red flags;
- Respond appropriately to the detected red flags; and
- Periodically update the identity theft program.

Covered entities are also required to ensure the proper administration of their preventative programs.

II. The Safeguards Rule

Rule 30(a) of Regulation S-P requires financial institutions to adopt written policies and procedures that address administrative, technical and physical safeguards to protect customer records and information. It further requires that those policies and procedures be reasonably designed to (1) ensure the security and confidentiality of customer records and information; (2) protect against 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.

III. The Voya Violations

According to [the SEC's order](#), cyber intruders successfully impersonated Voya contractor-representatives, gaining access to a web portal that housed the personally identifiable information (PII) of approximately 5,600 Voya customers. Over a six-day period, intruders called Voya's service call center and requested that three representatives' passwords be reset; the intruders then used the temporary passwords to create new customer profiles and access customer information and documents. The order indicated that, in two of the three cases, the phone number used to call the Voya service center had previously been flagged as associated with fraudulent activity.

Three hours after the first fraudulent reset, the targeted representative allegedly notified technical support that they had not requested the reset. While Voya did take some steps in response, the order found that those steps did not include terminating the fraudulent login sessions or imposing safeguards sufficient to

prevent intruders from obtaining passwords for two additional representative accounts over the next several days.

The SEC determined that Voya violated the Identity Theft Red Flags Rule because, while it had adopted an Identity Theft Prevention Program in 2009, it did not review and update this program in response to changes in the technological environment. The SEC also found that Voya failed to provide adequate training to its employees. Finally, the SEC found that Voya's Identity Theft Program lacked reasonable policies and procedures to respond to red flags. In addition to these violations, the SEC determined that Voya violated the Safeguards Rule by failing to adopt written policies and procedures reasonably designed to safeguard customer records and information.

IV. Aftermath and Implications

While neither admitting nor denying the SEC's findings, Voya agreed to a \$1 million fine to settle the enforcement action and will engage an independent consultant to evaluate its policies and procedures for compliance with the Safeguards Rule, Identity Theft Red Flags Rule and related regulations. The SEC additionally ordered that Voya cease and desist from committing any violations of Regulations S-ID and S-P.

The Voya settlement demonstrates that the SEC is focused on protecting consumer information, and ensuring that broker-dealers, investment companies and investment advisors comply with Regulation S-ID. The Voya settlement also provides that having policies and procedures designed to protect customer information alone may not suffice; entities subject to Regulation S-ID should frequently evaluate the adequacy of their policies and procedures designed to identify and address "red flags," and they should ensure that all relevant employees receive comprehensive training on identify theft. Such entities must also ensure that their compliance program is frequently updated to address changes in technology and corresponding changes to the risk environment.

Authors

Brittany M. Bacon
bbacon@HuntonAK.com

Mark S. Mandel
markmandel@HuntonAK.com

Trevor T. Garmey
tgarmey@HuntonAK.com

Ann E. Hancock
hancocka@HuntonAK.com

© 2018 Hunton Andrews Kurth LLP. Attorney advertising materials. These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create an attorney-client or similar relationship. Please do not send us confidential information. Past successes cannot be an assurance of future success. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials.