SEC Adds Cybersecurity Bite to its Bark

October 1, 2018

The charges against Voya Financial Advisors earlier this week, which resulted in the company paying a $1 million settlement, makes clear that the Securities and Exchange Commission is done warning firms about cybersecurity. It's ready to take action.
The SEC charged Voya for violating the "identity theft red flags" rule, which requires all SEC-regulated entities regardless of size to develop and implement a written program designed to detect, prevent and mitigate identity theft in connection with accounts.

Voya allegedly violated this rule by allowing attackers to gain access to its online portal by impersonating independent advisers. The adviser impersonators called Voya's help line, requested new passwords, and used them to access the system. Even though some of the numbers were already flagged as being associated with fraud, they still made it through Voya security.

The SEC rule has been on the books since 2013, but it has never been enforced until this week's charges.

"What we're seeing now is a potential increase in formal enforcement and consequences," said Bryan Baas, managing director of oversight and controls at TD Ameritrade Institutional.

"The SEC has warned the industry for many years, and now they are taking steps to make sure it's a top priority for all advisers," he said.

(More: Finra: Firms begin to heed cybersecurity, but have much to do)

It's time for advisers to go beyond awareness of cybersecurity and start taking action to protect themselves and their clients, Mr. Baas said.

TD Ameritrade has a new Risk Defense Assessment to help RIAs understand where they have security gaps across key areas to show how the firm stacks up against recommendations from the SEC's Office of Compliance Inspections and Examinations.
Even after the SEC announced in February that cybersecurity would be one of its 2018 exam priorities and hired four staff members devoted to expanding its efforts in this area, many firms still haven't taken action, according to Alan Brill, senior managing director of cyber risk practice at Kroll, a global risk consulting firm.

He calls the Voya charges a "very, very loud alarm ringing" to take this seriously, and recommends executives at all firms share the case with their security team.

"The SEC has talented cybersecurity professionals working for them who are busy as you and I speak," Mr. Brill said. "The SEC is moving from this being an esoteric problem to being a

part of their everyday thinking, their everyday analysis and their everyday actions." "Cybersecurity is the responsibility of everyone in the organization," he added.

The charges against Voya also highlight an ongoing vulnerability for many firms — independent contractors and other third-party partners. Even though they may not legally be employees, they are still the firm's responsibility from a security standpoint, Mr. Brill said. For example, the infamous Target data breach was traced back to a third-party company contracted to install air conditioning in stores.

(More: Retirement plans see rise in cyberattacks)

Firms have invested a great deal in protecting in-house systems, implementing official cybersecurity policies and training employees, but haven't extended the same diligence to third parties, said Sid Yenamandra, CEO of cybersecurity firm Entreda.

"Voya is just the tip of the iceberg," he said. "There are many firms that are probably in a similar boat. It just hasn't hit them yet."

Entreda offers a module to help firms conduct a comprehensive risk assessment of third-party vendors, and allows firms to institute a gateway that only allows authorized contractors using properly compliant devices to access the firm's portal. Mr. Yenamandra said this would have prevented a breach like the one Voya encountered.

He also recommends firms institute two-factor authentication, which requires a user to verify their identity on a second device, such as a cell phone, before gaining access to a system.

Wes Stillman, founder and CEO of RightSize Solutions, another cybersecurity firm, agreed that more SEC enforcement of cybersecurity is coming for the advice industry and a risk assessment is a "mandatory starting point" for firms. But firms can't view it as a problem that security alone will solve, as humans are often the weakest link. Training and a security-focused culture are necessary for a strong defense against data breaches and fraud, he said.

"It is time for RIAs to realize that it is no longer enough to have a policy, firms must use the policy to implement a systemic approach to security," Mr. Stillman told InvestmentNews. "They must also be able to show they are in a defensible position — including documentation of the firm's policy, supporting procedures, implemented enforcement, training and monitoring."

Related Topics: Securities and Exchange Commission