Hedge Fund Law Report
An Acuris company

Cybersecurity

Lessons for Fund Managers From the SEC's First Identity Theft Red Flags Rule Settlement

Nov. 15, 2018

By Rebecca Hughes Parker, *Hedge Fund Law Report*

SEC-registered investment adviser Voya's $1-million settlement with the SEC for alleged violations of the so-called "Safeguards Rule" and the "Identity Theft Red Flags Rule" shows that the SEC is willing to act when it believes firms could have done more to prevent cyber attacks. "The SEC expects companies to not only have in place commercially reasonable standards, policies and procedures for cybersecurity, but to implement them along with compliance and audit procedures to ensure that they are working as intended," Jason Elmer, managing partner at Drawbridge Partners, told the Hedge Fund Law Report.

This article analyzes the circumstances underlying the order, which involved a network intrusion by people impersonating third-party contractors, and its lessons, including what mistakes Voya made, how fund managers can avoid them and what the settlement says about SEC cybersecurity enforcement. See our three-part series on how fund managers should structure their cybersecurity programs: "Background and Best Practices" (Mar. 22, 2018); "CISO Hiring, Governance Structures and the Role of the CCO" (Apr. 5, 2018); and "Stakeholder Communication, Outsourcing, Co-Sourcing and Managing Third Parties" (Apr. 12, 2018).

Failure to Follow Through

Voya Financial Advisors (VFA) – a Minnesota corporation that is headquartered in Iowa and dually registered as a broker-dealer and investment adviser with the Commission – is a subsidiary of Voya and has approximately 13 million customers and $11 billion under management. Ben Singer, partner at O'Melveny & Myers, pointed out that an action against a firm this size should serve as a warning that the SEC is not only going after large firms; small and midsize firms may not be able to fly under the radar.

A significant problem for VFA was that it had policies that it did not fully implement or update. Singer emphasized the importance of following through with written policies. He likened the situation to "trying to make a left turn and pulling halfway out – that is the worst outcome. It seems like this broker-dealer pulled halfway out." Deficiencies are particularly glaring, for example, when companies have a training program but then do not ensure employees actually are trained, he told the Hedge Fund Law Report.

If a comprehensive program seems like too much, Singer said he recommends enacting it in steps and making sure each step is completely executed before moving on to the next one. "From Voya's perspective, given its size, it may seem like a lot of resources are expected to be put into

compliance, but they would have been better served with a more narrowly tailored program that was more thoroughly implemented," he observed.

See "Practical Steps That Commodity-Focused Hedge Fund Managers Can Take to Combat Cybersecurity Threats" (Mar. 10, 2016).

Third-Party Troubles

Many of Voya's problems stemmed from actions of the contractors they hired – a significant point of breach risk that many firms still do not recognize.

See "Fund Managers Must Supervise Third-Party Service Providers or Risk Regulatory Action" (Nov. 16, 2017); and "How Managers Can Identify and Manage Cybersecurity Risks Posed by Third-Party Service Providers" (Jul. 27, 2017).

The Intrusion

The SEC's cease-and-desist order (Order), the allegations in which VFA does not admit nor deny, states that VFA gave a third-party contractor access to its customer information through a proprietary web portal called "Voya for Professionals" or "VPro" so that contractor could manage the customers' brokerage accounts. Voya maintained the portal, but the contractors used their own equipment and applications to access the portal. The Order also specifies that Voya's service call centers (called "Financial Application Support Team" or "FAST") serviced support calls from VFA's customers and VFA's contractor representatives.

VFA's controls proved easy to circumvent in a textbook case of telephone social engineering, sometimes called "vishing." The Order says that over six days in April 2016, at least one person "impersonating VFA contractor representatives called the technical support line and requested a reset of three representatives' passwords for the web portal used to access VFA customer information, in two instances using phone numbers Voya had previously identified as associated with prior fraudulent activity."

Not only did Voya staff reset the passwords, they also provided the representative's username in two of the three instances. The intruders were able to pull off this scheme two more times in the next few days.

Armed with usernames and passwords, the intruders logged into the portal and were able to access the personally identifiable information (PII) of at least 5,600 of VFA's customers. "For at least 2,000 of these customers, the intruders viewed a full Social Security number and/or another government-issued identification number." The Order specifies that the "intruders also used customer information to create new Voya.com customer profiles, which gave them access to PII and account information of two additional customers."

See "SEC Review of Cybersecurity Finds Gains Since 2014, but Cites Gaps in Training and Compliance" (Aug. 24, 2017).

Treat Third Parties Like Employees

"Too often we see that third-party oversight is an area that firms don't spend enough time on," Elmer said. "Firms need to understand where their data is, and who has access to it, in order to conduct proper due diligence exercises on third parties. From a compliance perspective,

contractors with access to sensitive firm data need to follow the same policies and procedures that are in place for full-time employees."

Singer agreed, adding, "Some companies may not realize that they that they need to oversee their contractors, but clearly the SEC is sending this message with this case."

In the case of Voya specifically, the "policies may have been appropriate for the company but not appropriate for the contactor," Singer observed. "Some polices only related to company employees who had access to certain information, without recognizing that third parties also had access. According to the Order, the broker-dealer didn't match its compliance framework to how the business actually operated through those contractors."

See "Critical Components of a Hedge Fund Manager Cybersecurity Program: Resources, Preparation, Coordination, Response and Mitigation" (Jan. 15, 2015).

Policies Only on Paper

The Order specifies that Voya had more than a dozen policies and procedures before the intrusion, such as session timeouts, multi-factor authentication (MFA) and cybersecurity awareness training. These policies did apply to independent contractors but they "were not reasonably designed to apply to the systems the [contractors] used."

Elmer pointed out that "situations similar to this case are becoming increasingly more common, and this is just one instance of the SEC letting firms know that policies can't be 'off the shelf' but rather must be specific to the firm and its operations." He added, "It takes time and effort to create a properly sized and appropriate set of policies for a firm to follow."

According to the Order, Voya's deficiencies included, among other things:

- VFA allowed its contractor representatives to maintain concurrent VPro sessions and did not apply 15-minute inactivity timeouts to VPro sessions;
- VFA did not have a procedure for terminating an individual VFA contractor representative's remote session; and
- VFA contractor representatives' web access to VPro was subject to MFA that required the user to answer previously set security questions when a new device was connecting to the relevant VPro account. This form of MFA was rendered ineffective, however, when users called the FAST team to request a reset of VPro passwords and FAST staff reset the security questions, which was what happened during the intrusion.

See our two-part series "The Challenges and Benefits of Multi-Factor Authentication in the Financial Sector": Part One (Nov. 2, 2017); and Part Two (Nov. 9, 2017).

Password Reset Procedures

The password reset procedures that got Voya into trouble involved allowing FAST staff to provide users who called in requesting passwords temporary passwords on the phone, after the user provided at least two pieces of PII. These temporary passwords were not sent via secure email. Usernames (which were provided to the intruders) were not directly addressed in the policy.

On Notice

"These procedures remained in place at the time of the intrusion even though VFA was aware of prior fraudulent activity at Voya that involved attempts to impersonate its contractor representatives using their PII in calls to technical and customer support lines," the Order says.

VFA had a "monitoring list" of phone numbers suspected to have been used in connection with these prior incidents, but no policy required FAST to use this list. Further, VFA did not provide notice to a customer when account details were changed.

"This was not the first problem for this company," Singer said. "It had experienced problems in the past and it still had a compliance program that wasn't set up properly; thus, it was on notice." He added that this type of situation frequently leads to enforcement: "If it is a first-time issue, you can reasonably argue that you are going to fix it, but if you don't fix it and it happens again, that is when the SEC may act."

No Harm Needed

In this case, the SEC made no determination, or even allegation, of harm. "There have been no known unauthorized transfers of funds or securities from VFA customer accounts as a result of the attack," the Order says.

Harm is not an element of either the Safeguards Rule or the Identity Theft Red Flags Rule, and this case is a reminder that the SEC will act regardless of any damage an incident may have caused. "The SEC has now put all firms on notice that failing to implement, and abide by, the policies and procedures a firm puts in place, both logical and technical, is not acceptable behavior," Elmer said.

Singer did point out that the SEC will often go after the more egregious intrusions that are more likely to cause harm, but, "it is, of course, not a good compliance policy to focus on whether there is damage because a company has no way of knowing whether there will be damage before the incident."

See "SEC Enforcement Action Illustrates Focus on Investment Adviser Obligation to Secure Client Information" (Jun. 23, 2016).

Breach Response and Identity-Theft Mitigation Problems

The Order details Voya's troubling response to the intrusion. On April 13, 2016, one contractor representative notified FAST that he received an email indicating a password change he had not made, and the next morning, the incident was escalated. By that time, however, the intruders had obtained a second contractor's username. "Moreover," the SEC said, "the FAST manager's directive that no passwords be provided by phone and that the phone number monitoring list should be reviewed was not heeded on April 18, 2016, when a FAST team member provided a password to an intruder impersonating a third representative."

Other errors followed, including a failure to block IP addresses or freeze the sessions of the third-party application the intruders were using while malicious sessions were in progress. FAST staff had mistakenly thought that resetting the compromised VPro passwords would terminate these sessions, and their error prolonged the intruders' access to the information. The SEC noted that training on this point was lacking, adding that "VFA's incident response procedures also failed to ensure that the FAST and customer-facing call center staff were notified about an ongoing intrusion."

In January 2016, VFA did adopt a procedure to place flags on compromised representative and customer accounts. However those flags were, according to the SEC, "erased from the system periodically in connection with unrelated automated system activities," an example perhaps of failing to follow through with extant policies.

The Settlement

The Order charges VFA with willfully violating the Safeguards Rule (Rule 30-a of Regulation S-P) which requires every broker-dealer and every investment adviser registered with the SEC to adopt written policies and procedures that are reasonably designed to safeguard customer records and information.

It also, for the first time, cites a willful violation of Rule 201 of Regulation S-ID, which requires registered broker-dealers and investment advisers that offer or maintain covered accounts to develop and implement written identity theft prevention programs that are designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

The Order states that – despite changes in cybersecurity risks, both in the external environment and specific to VFA – VFA did not update its identity theft prevention program after 2009, and it failed to conduct training specific to an identity theft prevention program.

In extending the settlement offer, the SEC said it took into account VFA's remedial acts, including:

- blocking the malicious IP addresses;
- revising its user authentication policy to prohibit provision of a temporary password by phone;
- issuing breach notices to the affected customers, describing the intrusion and offering one year of free credit monitoring;
- implementing effective MFA for VPro; and
- naming a new chief information security officer, who is responsible for creating and maintaining cybersecurity policies and procedures and an incident response plan tailored to VFA's business.

In addition to paying the $1-million fine, VFA is required hire a compliance consultant who must issue a report to the Commission. VFA must certify its compliance with the undertakings the report sets forth.

See "In Deutsche Bank Case, SEC Emphasizes Protecting Information From More Than Just Cyber Threats" (Nov. 10, 2016).

What's Next?

Singer expects more Identity Theft Red Flag cases to follow. He said that larger companies are attuned to this rule, especially given the cases of identity theft in the headlines, but "for mid-sized and smaller companies, this is the type of enforcement action that will grab their attention."

Actions against broker-dealers may also be a continued focus for the SEC because it thinks of them as crucial in cybersecurity. "For the SEC, the broker-dealer is the number-one gatekeeper

of the confidential information in those accounts," Singer said. "As a gatekeeper of people's brokerage information, if broker-dealers don't have good compliance, that calls into question the effectiveness of all the other rules and regulations that are in place."

See "What Fund Managers Can Learn About Cyber-Breach Disclosure From Yahoo's $35-Million SEC Settlement" (May 10, 2018). See also "SEC Chair Outlines Approach to Dodd-Frank Rulemaking and Expectations for Fund 'Gatekeepers'" (Feb. 15, 2018); and "SEC Order Warns Fund 'Gatekeepers' That They Remain a Focus of Fund Scrutiny" (Feb. 8, 2018).