Bloomberg Law®

bloombergbna.com



*Data Security*

# INSIGHT: SEC's Voya Order Underscores Importance of Cybersecurity Practices



By Ian G. DiBernardo, Jeffrey M. Mann, and André B. Nance, Stroock & Stroock & Lavan LLP

The Securities and Exchange Commission (SEC) recently issued an order imposing a $1 million penalty and remedial sanctions against Voya Financial Advisors, Inc. (VFA), an entity registered as both a broker-dealer and an investment adviser, for violations of the cybersecurity requirements of the Safeguards Rule and the Identity Theft Red Flags Rule. This is the first SEC enforcement action charging violations of the Identity Theft Red Flags Rule since the agency began enforcing the rule in 2011.

According to the SEC, over six days in April 2016, intruders called VFA's technical support line, impersonating actual contractors, and were able to receive contractors' user names and reset their passwords for access to VFA's computer systems and applications via its web portal. The intruders were able to gain access to the personally identifiable information (PII) of at least 5,600 customers and to create new customer profiles. Although no known unauthorized transfers of funds or securities occurred, VFA agreed to pay the SEC penalty without admitting or denying the charges.

In this first-of-its-kind action, the bases the SEC detailed for finding violations provide valuable insight into appropriate cybersecurity policies and practices, particularly with respect to the use of third-party contractors. According to Robert A. Cohen, chief of the SEC Enforcement Division's Cyber Unit, this case ''is a reminder to brokers and investment advisers that cybersecurity procedures must be reasonably designed to fit their specific business models [and that they] also must review and update the procedures regularly to respond to changes in the risks they face.''

**The Regulations** As summarized by the order, the Safeguards Rule, Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)), requires every registered broker-dealer and investment adviser to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.

The policies and procedures must be reasonably designed to (1) ensure the security and confidentiality of customer records and information, (2) protect against any anticipated threats to the security or integrity of such records and information, and (3) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

The Identity Theft Red Flags Rule, Rule 201 of Regulation S-ID (17 C.F.R. § 248.201), requires registered broker-dealers and investment advisers, as well as other financial institutions, to develop and implement a written identity theft prevention program. The identity theft prevention program must be designed to detect,

prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

More specifically, the program must include reasonable policies and procedures to (1) identify relevant red flags for covered accounts, (2) detect such red flags, and (3) respond appropriately to any red flags that are detected. Additionally, the identity theft prevention program must be updated periodically to reflect changes in risks to customers from identity theft.

A covered account is an account that a broker-dealer or investment adviser offers or maintains, primarily for personal, family, or household purposes or that is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer. See 17 C.F.R. § 248. 201(b)(3).

**Factual Background** By way of background, the SEC described VFA as dually registered as a broker-dealer and investment adviser, with approximately 13 million customers and approximately $11 billion in assets under its management. It has over 1,000 employees, as well as 3,800 other associated persons, including contractor representatives, across 1,200 locations.

The contractor representatives provide brokerage and investment advisory services to VFA's customers. In providing the services, the contractor representatives access customer account information, including PII, via a web portal. More specifically, the contractor representative could access VFA's customer and prospect relationship management system, which contains account information and PII, and a customer account management system, which enables the representative to execute trades and initiate cash distributions. The portal was serviced and maintained by VFA's parent company, Voya Financial, Inc. (Voya).

As summarized in the order, VFA violated the Safeguards Rule because, among other things, its policies and procedures were not reasonably designed with respect to resetting contractor representative passwords, terminating contractor representative web sessions, identifying higher-risk representatives and customer accounts for additional security measures, and creating and altering customer profiles. In addition, the cybersecurity policies and procedures were not reasonably designed to be applied to contractor representatives.

With respect to the Identity Theft Red Flags Rule, VFA failed to review and update its identity theft prevention program in response to changing risks and provide adequate training to employees.

In resolving the action, VFA agreed to be censured and to pay the $1 million penalty. VFA also agreed to retain an independent compliance consultant to conduct a review of its policies and procedures for compliance with the rules, and to implement the recommendations of the consultant.

**Lessons Learned** Although the SEC cites many specific facts in support of finding violations, several are reminders of broader, important concepts for complying with the rules.

Policies and practices cannot be stagnant. Highlighting the need to react to changing risks and update policies and procedures, the SEC noted that VFA had not substantively updated its Identify Theft Protection Program since 2009, despite ''significant changes in external cybersecurity risks and in VFA's own risk profile.'' Putting aside how long it had been since the policy was updated, the SEC's statements serve as a reminder of the need to revisit policies and practices in connection with material events, which may include changes in technology infrastructure and the outsourcing of business functions or other use of third-party contractors.

Policies and practices should provide not only for technical measures to mitigate risks but also for administrative ones that guide employee action. In this respect, the SEC noted VFA's failure to respond to signs of the targeted attack and to train its employees adequately. Despite an actual contractor representative notifying VFA that they had received an e-mail confirming a password change while not requesting one—the first fraudulent request to reset a representative password—subsequent fraudulent requests over the next several days were successful. More specifically, the SEC noted that in two instances, the intruders used phone numbers that had previously been identified with prior fraudulent activity. Despite keeping a list of phone numbers suspected of being used in connection with fraudulent activity, there was no written policy or procedure that required support employees to reference the list when responding to requests for password resets. To the extent VFA had a policy of reviewing calls from such numbers on the following business day, the policy was not consistently applied.

The order also highlights the need to have adequate training—another administrative control—in the relevant systems. Although VFA's incident response procedures required potentially compromised user accounts to be disabled or the relevant applications to be shut down, security personnel erroneously believed that resetting a password for a user would terminate that user's existing session. Compounding the issue, the incident response procedures failed to ensure that relevant staff were notified of ongoing intrusions.

Appropriate administrative measures also require proper follow-up to identify potential issues. VFA hired a third-party service provider to scan contractor representatives' remote computers. However, according to the SEC, VFA failed to follow up with representatives that failed to scan their computers or whose scans identified security deficiencies.

While both the Safeguards Rule and the Identity Theft Red Flags Rule require written policies, the SEC made clear in its order that it will look beyond the surface, into the sufficiency of the policies and procedures and their actual implementation across the organization, including third-party contractors.

Although VFA had in place cybersecurity policies and procedures applicable to contractors, they were not applied to contractors in practice. For example, despite a policy of prohibiting employees from having concurrent web sessions accessing systems containing PII, VFA allowed contractor representatives to maintain concurrent sessions. And despite a policy of web application sessions automatically being timed out after 15 minutes of inactivity, the inactivity timeout for a key application was reset to 60 minutes without any formal documentation. Moreover, although multi-factor authentication was used, a less secure form was used for contractor representatives, as opposed to employees.

The SEC's discussion also highlights the need for a thorough intrusion response plan. Voya security staff, who were in charge of responding to the breach, identified certain IP addresses as likely involved in the intrusion; however, they failed to block them. Also, in an ef-

fort to assess the scope and mitigate the effects of the intrusion, VFA followed up with contractor representatives whose passwords were reset during the intrusion to identify other fraudulent resets. However, the testing covered passwords reset during only a portion of the actual duration of the intrusion. Furthermore, more than 40 percent of the representatives having reset passwords could not be reached, and no follow-up inquiry was made.

**Conclusion** In its first order enforcing the Identity Theft Red Flags Rule, the SEC has made clear that broker-dealers and investment advisers must remain vigilant in implementing and maintaining cybersecurity policies and practices. In choosing VFA—where no known unauthorized transfers of funds or securities occurred—the SEC has also made clear that it is not waiting until fraudulent transfers take place before asserting its authority. In light of this order, it would behoove all broker-dealers and investment advisers to review the adequacy and effectiveness of their current cybersecurity policies and practices and update them as needed.

———

*Ian G. DiBernardo is the co-head of the FinTech and Intellectual Property & Technology Practice Groups at Stroock & Stroock & Lavan LLP in New York. Jeffrey Mann, a Special Counsel in those groups, is a Certified Information Privacy Professional (CIPP/US). André B. Nance is a partner in the firm's Private Funds Practice Group.*