Proskauer

SEC Charges Broker-Dealer and Investment Adviser with Violations of the Safeguards Rule and Identity Theft Red Flags Rule

Privacy Law Blog on **October 4, 2018**

In September 2018, the Securities and Exchange Commission ("SEC") announced that broker-dealer and investment adviser Voya Financial Advisors Inc. ("VFA") agreed to pay $1,000,000 to settle charges related to alleged failures in its cybersecurity policies and procedures relating to a data breach that compromised the personal information of 5,600 customers. The SEC charged VFA with violating Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) (the "Safeguards Rule") and Rule 201 of Regulation S-ID (17 C.F.R. § 248.201) (the "Identity Theft Red Flags Rule"). This charge against VFA is the first SEC enforcement action charging violations of the Identity Theft Red Flags Rule.

In 2016, cyber intruders impersonated VFA contractors by calling VFA's support line and requesting the contractors' passwords be reset. The intruders then used these passwords to gain access to the personal identifiable information ("PII") of at least 5,600 VFA customers and subsequently created new online customer profiles and obtained unauthorized access to account documents for three customers. According to the SEC's order, VFA's failure to terminate the intruders' access was a result of weaknesses in VFA's cybersecurity procedures, some of which VFA knew of from prior similar fraudulent activity. The order also notes that VFA failed to apply its procedures to the systems used by independent contractors.

The SEC found that VFA willfully violated the Safeguards Rule, which requires broker-dealers and investment advisers to adopt written policies and procedures that are reasonably designed to safeguard customer records and information. During the relevant period, while VFA employees generally used IT equipment and IT systems provided by its parent company Voya, VFA contractors generally used their own IT equipment and operated over their own networks. VFA contractors accessed customer information through a proprietary web portal ("VPro"). The contractors could log in with a username and password to gain access to certain web applications that contained sensitive information relating to VFA customers. VFA outsourced most of its cybersecurity functions and some of its information technology functions to Voya, which was responsible for responding to contractors' requests for assistance with respect to the web applications.

Over a dozen Voya policies and procedures relating to cybersecurity were supposed to govern the conduct of VFA, including:

- manual account lock-outs for a user suspected of being involved in a security incident from web applications containing critical data, including customer PII,
- a session timeout after fifteen minutes of user inactivity in web applications containing customer PII,
- a prohibition of concurrent web sessions by a single user in web applications containing customer PII,
- multi-factor authentication ("MFA") for access to applications containing customer PII,
- annual and ad-hoc review of cybersecurity policies, and
- cybersecurity awareness training and updates for VFA employees and contractors.

The SEC found that these policies were not reasonably designed to apply to the systems that independent contractors used. Specifically, the SEC found that the following VFA policies and procedures were not reasonably designed to safeguard customer records and information: (1) resetting contractors' passwords,[1](2) terminating web sessions in its proprietary gateway system for VFA contractors,[2] (3) identifying higher-risk representatives and customer accounts for additional security measures,[3] and (4) creation and alteration of customer profiles.[4]

The SEC also found that VFA willfully violated the Identity Theft Red Flags Rule, which requires registered broker-dealers and investment advisers that offer or maintain covered accounts to develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. Although VFA adopted a written Identity Theft Prevention Program in 2009, the SEC found that VFA violated the Identity Theft Red Flags Rule because it had not reviewed or updated the program in response to changes to risks to its customers and did not provide adequate training to its employees. Additionally, the program did not include reasonable policies and procedures to respond to identity theft red flags, including those detected by VFA during the 2016 breach.

As part of the settlement, VFA has agreed to retain, and cooperate fully with, a compliance consultant to review all of its policies and procedures for compliance with Regulation S-P and Regulation S-ID. The settlement also requires VFA to pay a civil penalty of $1,000,000 and cease and desist from violating Regulation S-P and Regulation S-ID.

[1] The password reset procedures for VPro allowed Voya staff to provide users who could not remember their passwords with a temporary password by phone as long as the user provided at least two pieces of PII. Temporary passwords were not required to be sent by secure email.

[2] VFA allowed contractors to maintain concurrent VPro sessions and did not apply 15-minute inactivity timeouts to VPro sessions. VFA also did not have a procedure for terminating an individual contractor’s remote session. Furthermore, resetting passwords did not terminate sessions, which meant that existing sessions continued after password resets.

[3] Voya kept a “monitoring list” of phone numbers associated with prior fraudulent activity at Voya, but there was no written policy or procedure requiring Voya to use this list when responding to requests for password resets or other calls from the phone numbers on this list. With respect to reviewing contractors’ computers for security deficiencies, some contractors delayed or did not complete such scans. Approximately 30% of scanned computers exhibited critical failures, such as lack of encryption and antivirus software.

[4] VFA did not notify customers when an initial profile was created and when contact information and document delivery preferences were changed for that customer. Thus, intruders could create and change customer profiles without being detected by customers, as was the case in the 2016 data breach.

View Original