Client Alert | Data, Privacy & Cybersecurity

SEC Extends Cybersecurity Enforcement in $1 Million Settlement With Investment Advisor

October 2018

Authors: **Steven R. Chabinsky**, **F. Paul Pittman**

The Securities & Exchange Commission ("SEC") agreed to a $1 million settlement with Voya Financial Advisors ("VFA") based on a two-year-old customer data breach with no showing of harm. Under the terms of the settlement, VFA did not admit to the allegations against it, but agreed to retain an independent consultant to review its policies and procedures for compliance with the Safeguards Rule and the Identity Theft Red Flags Rule, and to certify implementation of the consultant's recommendations absent agreement by the SEC that they are unduly burdensome, impractical or inappropriate.

Background

VFA provides brokerage and investment advisory services to its customers primarily through contractor representatives. According to the SEC's settlement order[1] (the "Order"), for a period spanning six days in April 2016, VFA suffered a data breach when its technical and customer support personnel were duped into resetting the account credentials of three contractor representatives. According to the SEC, VFA support personnel provided temporary passwords over the phone for all three accounts, and also provided the representatives' usernames for two of them. Armed with these credentials, the hackers accessed a system containing the personally identifiable information (PII) of approximately 5,600 customers, often with full social security numbers. Perhaps not realizing they had the power to do so, the hackers did not take advantage of the ability their account access provided to execute trades and request distributions.

When VFA became aware of the breach, it took a number of incident response steps and the intrusion ended in slightly more than two days. According to the SEC, VFA took prompt steps after the intrusion to block the malicious IP addresses, revise its user authentication policy, implement multi-factor authentication, issue breach notifications, and offer a year of free credit monitoring to affected customers. The company also named a new Chief Information Security Officer.

Still, the SEC found VFA's response to the data breach was inadequate. As described in more detail below, although VFA had more than a dozen cybersecurity policies and procedures in place, the SEC determined that they were not reasonably designed to protect customer records and information, nor were they adequately developed, reviewed, updated and implemented to account for changes in risk and to respond to identity theft red flags.

---

1 The SEC's Order is available here.

SEC Claims

The SEC's settlement represents its first-ever enforcement action under the Identity Theft Red Flags Rule, which requires certain financial institutions and creditors to develop and implement a written Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft relating to a covered account. The SEC found that although VFA had previously registered with the SEC pursuant to the Identify Theft Red Flags Rule in 2009, the company did not subsequently update its program to account for changing cybersecurity risks to its customers, did not include procedures in its program to identify the red flags that led to the intrusion, did not provide Identity Theft Prevention Program training to its employees, and did not have involvement by the board of directors or VFA's management team to administer and oversee the Identity Theft Prevention Program.

The SEC also charged VFA under the Safeguards Rule, which requires all registered broker-dealers and investment advisers to adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information. In short, policies and procedures under the Safeguards Rule must be reasonably designed to keep customer records and information secure and confidential, and protect customer records and information against any anticipated security threats, hazards or unauthorized access or use. The SEC alleged that VFA violated the Safeguards Rule by failing to reasonably design password protection policies, contractor access controls, and security and customer account profile management procedures.

Determination of Reasonableness

The Order sheds light on the cybersecurity measures, policies and practices the SEC considers "reasonably designed" to insure the confidentiality and integrity of PII, and to protect against any threats and unauthorized access to customer PII under the Safeguards Rule. Simply having a related policy or procedure in place will not be sufficient absent adequate implementation and updating over time to reflect evolving risks. For example, here the SEC brought an enforcement action despite VFA's established, existing written policies, procedures and practices addressing data privacy and cybersecurity, including: (1) an incident response plan; (2) annual and ad-hoc review of cybersecurity policies; (3) authentication procedures for network access and password recovery; (4) security incident account lockouts and session timeouts; (5) maintaining a list of suspicious phone numbers and IP addresses; (6) cybersecurity awareness training; and (7) a written Identity Theft Prevention Program.

While the SEC acknowledged VFA's policies, procedures and programs, ultimately, the SEC found the following specific inadequacies:

- Existing cybersecurity policies and practices targeting employees were not "reasonably designed" to cover contractors accessing VFA's network
- Password reset procedures allowed distribution of temporary passwords over the phone using customer PII, and did not require that passwords be sent via secure email, despite prior fraudulent activity involving the impersonation of contractor representatives in calls to VFA's support personnel
- There was no written policy requiring customer support to consult an internal "monitoring list" of phone numbers suspected of being used in fraudulent activity and the unwritten policy was not consistently followed
- An ineffective program for scanning contractor personal computers for use of security measures such as antivirus software, encryption and software updates
- Policies and procedures in place to protect VFA user profiles did not protect against unauthorized changes and the creation of customer profiles and did not provide alerts to customer of changes to their contact information or document delivery preferences
- Existing breach response procedures did not limit or deny unauthorized access to VFA customer PII and information technology security personnel were not adequately trained in applying security changes to customer database
- The improper configuration of a system "flagging" contractor and customer accounts for further security measures

Outlook

The SEC's enforcement action reflects its attention to ensuring that a company's cybersecurity policies and governance procedures are not merely formalized in writing, but that they work in practice. Earlier this year, the SEC fined Yahoo $35 million for its untimely disclosure of cybersecurity risks and prior security incidents in its public filings, as well as in its stock purchase agreement pursuant to Verizon's bid to acquire Yahoo's core Internet operating business. The SEC determined, among other things, that Yahoo had inadequate controls and procedures in place to ensure proper disclosure. Taken together, these SEC enforcement actions emphasize the need for companies to address cybersecurity risk at the executive and Board level, and demonstrate the importance of periodic compliance reviews to ensure that a company's policies and programs are properly aligned to their risks and are adequately implemented, reviewed and revised over time.

White & Case LLP
701 Thirteenth Street, NW
Washington, DC 20005-3807
United States

T 1 202 626 3600