Client Alert: Securities and Exchange Commission Imposes $1 Million Penalty on Voya Financial Advisors after Cybersecurity Intrusion

Related Professionals

John L. Landolfi

Christopher L. Ingram

Related Services

Data Strategy, Privacy and Security

Litigation and Appeals

CLIENT ALERT | 11.5.2018

Recently, the Securities and Exchange Commission (SEC) imposed a $1 million penalty against Voya Financial Advisors, Inc. (VFA). The SEC alleged that VFA violated the Safeguards Rule and the Identity Theft Red Flags Rule through deficient cybersecurity procedures that led to the breach of customers' sensitive information. This was the first SEC enforcement action charging violations of the Identity Theft Red Flags Rule.

According to the SEC's order, fraudsters called VFA's technical support line over a six-day period impersonating VFA's contractor representatives. The fraudsters were successful in obtaining valid user names and temporary passwords to access VFA's web portal, which contained its customers' information. The credentials were then used to access personal information from at least 5,600 VFA customer accounts. Despite receiving notice from one of VFA's contractors that his password was reset without his knowledge, the SEC alleged that VFA failed to take adequate measures to secure its web portal from unauthorized access. There were no known unauthorized transfers of funds or securities from any VFA accounts.

Nevertheless, the SEC alleged that VFA violated the Safeguards Rule because the company's cybersecurity policies and procedures were not reasonably designed to protect customer information or to prevent or respond to cybersecurity incidents. The Safeguards Rule requires every broker-dealer and investment adviser registered with the SEC to adopt written policies and procedures reasonably designed to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. The SEC criticized VFA's policies and procedures over the resetting of passwords, termination of web sessions in VFA's online portal, classification of risk for users and customers' accounts, and the creation or alteration of customers' online profiles.

The SEC also alleged that VFA violated the Identity Theft Red Flags Rule because VFA failed to show that it reviewed and updated its existing Identity Theft Prevention Program or provide adequate training to its employees. The Identity Theft Red Flags Rule requires certain financial institutions and creditors, including broker-dealer and investment advisers registered or required to register with the SEC, to develop and implement a written Identity Theft Prevention Program. The 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. It must include reasonable policies and procedures to: identify relevant red flags for the covered accounts and incorporate them into the Program; detect the red flags that have been incorporated into the Program; respond appropriately to any red flags detected; and ensure that the Program is updated periodically to reflect changes in risks to customers. In this case, the SEC alleged that the fraudsters called into the technical support line from telephone numbers that VFA had previously identified as being associated with fraudulent activity in which callers attempted to impersonate VFA contractor representatives. According to the SEC, VFA should have had reasonable policies and procedures in place to respond to these red flags which may have prevented the cyber intrusions.

This case illustrates how the SEC and other regulators will continue to investigate cyber intrusions, expose flaws in companies' cybersecurity posture, and impose significant penalties for noncompliance with privacy laws. Companies should review their cybersecurity policies and procedures for any compliance gaps and ensure that employees are adequately trained. For assistance with compliance questions, policy reviews, or employee training, please contact John Landolfi, Christopher Ingram, Sarah Boudouris, or your Vorys attorney.