SEC Scrutinizes Response to Cyberattacks at Eight Firms

September 3, 2021 Kit Addleman, Tim Newman, Carrington Giammittorio

PRACTICES Investment Management, Investment Banking and Broker Dealer, Privacy and Cybersecurity

Eight broker-dealer and investment adviser firms were sanctioned by the U.S. Securities and Exchange Commission ("SEC") on August 30, 2021, for failures in their cybersecurity policies and procedures. According to the SEC, the failures allowed unauthorized third parties to take over cloud-based email accounts of firm representatives, exposing personally identifying information (PII) of thousands of firm customers and clients in violation of Rule 30(a) of Regulation S-P. Also known as the Safeguards Rule, Reg S-P is designed to protect confidential customer information. The SEC also alleged violations of the antifraud provisions of the Advisers Act in one of the settled orders. The firms neither admitted nor denied the SEC's charges.

According to the SEC order against five affiliated "Cetera entities," between November 2017 and June 2020, hackers accessed the email accounts of more than 60 Cetera employees, exposing the PII of more than 4,000 customers and clients. The SEC's order found that none of the hacked accounts had been protected in the manner required by the Cetera entities' internal policies. Further, the breach notifications sent to clients allegedly included misleading language regarding the timing of the notifications: namely, that the notifications were being issued much closer in time to the discovery of the breach than they really were. The settled order alleges violations of the Safeguards Rule in connection with the breach and also of Section 206(4) of the Advisers Act and Rule 206(4)-7 (which prohibit fraud and require investment advisers to adopt policies and procedures designed to prevent violations of the Advisers Act, respectively) in connection with Cetera's notifications to clients. The Cetera entities agreed to cease and desist from future violations, to a censure, and jointly to pay a civil monetary penalty of $300,000.

Regarding two affiliated "Cambridge entities," the SEC order found that, between January 2018 and July 2021, the email accounts of more than 120 Cambridge representatives were hacked, exposing the PII of more than 2,000 Cambridge customers and clients. Additionally, the order found that Cambridge had failed to implement enhanced cybersecurity measures despite discovering the initial breach in January 2018. This failure, according to the SEC, led to the potential (and in some instances *actual*) compromise of additional customer information. The order included a cease and desist and a censure and assessed a joint civil monetary penalty of $250,000.

Finally, the SEC's order against KMS Financial Services found that, between September 2018 and December 2019, the email accounts of 15 KMS employees were hacked, resulting in the exposure of nearly 5,000 customers' PII. The order also found that, although KMS had been aware of the breach, it did not implement any firmwide policies enhancing security measures until August 2020. KMS has agreed to cease and desist from future violations, a censure, and to pay $200,000 in civil monetary penalties.

The SEC is continuing to prioritize cybersecurity and focus on firms' obligations to protect confidential customer information under the Safeguards Rule. As evidenced by these actions, the SEC is willing to impose significant sanctions on firms that fail to meet that obligation. Although it is

important for firms to fashion appropriate cybersecurity policies and procedures on the front end, equally vital is the implementation of those policies and a prompt, transparent, and tailored response to any discovered breach. Companies who experience a cyberattack should promptly and accurately communicate with customers and clients who may have been affected in accordance with relevant laws and regulations. They should also timely review existing security policies and procedures, ensure compliance, and analyze what enhancements should be made.

These orders note that the actions arose from the Division of Examinations, thus highlighting the close coordination between the SEC's Examination Division and the Division of Enforcement on cybersecurity matters.

The cases are *In the Matter of Cetera Advisor Networks LLC*, Release No. 34-92800; *In the Matter of Cambridge Investment Research, Inc.*, Release No. 34-92806; and *In the Matter of KMS Financial Services, Inc.*, Release No. 34-92807, August 30, 2021.

If you have any questions about these orders, cybersecurity, or SEC enforcement activities, contact one of our attorneys listed below.