The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 33751

September 2, 2021

SEC Sanctions Brokers and Advisers for Deficient Email Security Procedures and Insufficient Breach Notices

[33751]

September 2, 2021

TO: ICI Members
Chief Compliance Officer Committee
Chief Information Security Officer Committee
Operations Committee
Technology Committee SUBJECTS: Compliance
Cybersecurity RE: SEC Sanctions Brokers and Advisers for Deficient Email Security Procedures and Insufficient Breach Notices

Earlier this week, the SEC sanctioned eight firms in three actions for failures in their data security practices relating to cloud-based email accounts. While the respondents in these actions neither admitted nor denied the alleged violations, below are the findings from the SEC's three Orders.

The Cetera Order[1]

According to the SEC order relating to the Cetera Respondents, between November 2017 and June 2020, the cloud-based email accounts of 60 staff persons working for five related Cetera firms, each of which is a broker-dealer and/or investment adviser, were taken over by unauthorized third parties. This takeover resulted in the exposure of personally identifying information (PII) of at least 4,388 customers and clients. None of the impacted email accounts were protected with multi-factor authentication (MFA) even though the firms' policies required MFA "whenever possible." According to the SEC, the Respondents' failure to protect the clients' account information constituted a violation of SEC Regulation S-P, which requires registrants to have policies and procedures reasonably designed to protect the confidentiality of customers' information. The Order additionally found that the Respondents sent 220 impacted clients breach notices that included misleading language suggesting that such notices were issued much sooner after the discovery of the breach than they really were.[2] According to the SEC, the Respondents' conduct violated Regulation S-P and Section 206(4) of the Investment Advisers Act of 1940 and Rule 206(4)-7 thereunder, which requires investment advisers to adopt and implement written compliance policies and procedures reasonably designed to prevent violations of the Act.

The Respondents were censured, ordered to cease and desist from further violations, and fined $300,000.

The Cambridge Order[3]

The Cambridge Order finds that, between January 2018 and July 2021, the cloud-based email accounts of over 121 Cambridge representatives were taken over by unauthorized third parties. These takeovers resulted in the PII exposure of at least 2,177 Cambridge customers and clients. Even though Cambridge discovered the first email takeover in January 2018, it failed to adopt and implement firm-wide enhanced security measures for its representatives' cloud-based email accounts until 2021. This delay resulted in the exposure and potential exposure of additional customer and client records and information. Like the Cetera account takeovers, the SEC noted that the Cambridge email account takeovers did not appear to have resulted in any unauthorized trades or fund transfers to unauthorized parties from any Cambridge customer accounts. Based on its conduct, the SEC found that Cambridge willfully violated Regulation S-P.

Cambridge was censured, ordered to cease and desist, and fined $250,000. In imposing these sanctions, the Order notes that the SEC took into account the firm's remedial acts, which included requiring all representatives' accounts to implement MFA.

The KMS Order[4]

The SEC's third order was against KMS Financial Services, Inc., a dually registered broker-dealer and investment adviser. The SEC found that, between, September 2018 and December 2019, the cloud-based email accounts of 15 KMS financial advisers or their assistants were taken over by unauthorized third parties. This resulted in the exposure of PII for approximately 4,900 KMS customers and clients. The Order noted that the firm's Computer Network and Security Policies included requirements for certain technical security issues, such as maintaining strong passwords, securing wireless networks, using anti-virus and malware protection, securing backup and stored data, and encrypting hard drives. They also recommended, but did not require, the use of MFS for accessing sensitive data. Financial advisers were also required to notify KMS of any suspected cybersecurity breaches.

As explained in the Order, "[d]uring the relevant time period, fifteen KMS financial advisers experienced email account takeovers in which unauthorized persons accessed the email accounts of the financial advisers or their assistants and had the ability to take action in the accounts. . . . In many of these instances, emails containing customer PII were forwarded to unauthorized email addresses outside of KMS. In some instances, customers received 'phishing' emails that requested them to: (a) wire funds to a bank account; (b) enter PII (such as a driver's license number or Social Security number) to access a document; or (c) click on a link to view an investment recommendation, which would grant access to the customer's computer." Once the account takeovers were discovered, the affected financial advisers' email passwords were reset, forwarding rules removed, and MFA enabled. However, "these security measures were not fully implemented firm-wide until August 2020, which was approximately 21 months after discovery of the first breach, in which approximately 2,700 emails of one KMS financial adviser were exposed for a period of 26 days during which unauthorized third parties forwarded the financial adviser's emails to an email address outside of the firm." The SEC also found that KMS lacked its own Incident Response Policy and, instead, used one tailored to one of the firm's subsidiaries.

According to the Order, the Respondent's conduct constituted a willful violation of Regulation S-P. The Respondent was censured, ordered to cease and desist, and fined $300,000. In imposing these sanctions the SEC acknowledged the Respondent's remedial acts.

Tamara K. Salmon
Associate General Counsel

endnotes

[1] See In the Matter of Cetera Advisor Networks, LLC, Cetera Investment Services, LLC, Cetera Financial Specialists, LLC, Cetera Advisors, LLC, and Cetera Investment Advisers LLC, SEC Administrative Proceeding File No. 3-20490 (August 30, 2021), which is *available at* https://www.sec.gov/litigation/admin/2021/34-92800.pdf. The Order notes that these email account takeovers do not appear to have resulted in any unauthorized trades or transfers in the customers' accounts.

[2] These notices stated that the breach resulted in unauthorized persons accessing the clients' information two months before the notice. According to the Order, "Each entity . . . had learned of the underlying breach at least six months earlier. The dates referenced in the letters were the dates the firms completed PII review of compromised email accounts and determined that particular recipient's PII may have been accessed. . . . Clients who were misinformed . . . would not have known to look for or guard against potential misuse of their PII that may have occurred more than two months before the received the misleading notices." Order at ¶ 18

[3] See In the Matter of Cambridge Investment Research, Inc. and Cambridge Investment Research Advisors, Inc., SEC Administrative Proceeding No. 3-20496 (August 30, 2021), which is *available at* https://www.sec.gov/litigation/admin/2021/34-92806.pdf.

[4] See In the Matter of KMS Financial Services, SEC Administrative Proceeding No. 3-20495 (August 30, 2021), which is *available at* https://www.sec.gov/litigation/admin/2021/34-92807.pdf. The Order notes that email account takeovers did not appear to have resulted in any unauthorized trades or fund transfers to unauthorized parties from the customers' accounts.