SULLIVAN & CROMWELL LLP

S&C memo

September 1, 2021

SEC Sanctions Firms in Three Actions for Deficient Cybersecurity Controls

Actions Illustrate SEC's Heightened Focus on Cybersecurity Controls and Disclosure Controls and Procedures in the Cybersecurity Context

SUMMARY

On August 30, 2021, the U.S. Securities and Exchange Commission (SEC) sanctioned a group of eight broker-dealers and registered investment advisors in three different actions for failing to maintain adequate cybersecurity procedures and disclosure controls, in violation of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) (the Safeguards Rule). According to the SEC's Orders, these failures allowed unauthorized third parties to compromise the email accounts of the firms' representatives and thus resulted in the exposure of their clients' personally identifiable information (PII). The SEC further found that, in notifying affected clients of the breach, two of the firms misleadingly suggested that the incident had been discovered more recently than it actually was, in violation of Section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder (17 C.F.R. § 275.206(4)-7) (collectively, Section 206(4)). The three Orders imposed civil money penalties in the amount of $300,000, $250,000, and $200,000, respectively. The actions follow two other SEC enforcement actions recently brought against public companies for failure to make sufficient disclosures and to maintain adequate disclosure controls and procedures in the cyber context, and reflect the SEC's recent, heightened interest in enhancing regulated entities' focus on these issues.

BACKGROUND

The eight firms sanctioned by the SEC—Cetera Advisor Networks LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC, Cetera Advisors LLC, and Cetera Investment Advisers LLC (collectively, Cetera); Cambridge Investment Research, Inc. and Cambridge Investment Research Advisors, Inc. (collectively, Cambridge); and KMS Financial Services, Inc. (KMS)—are all SEC-registered broker-dealers, investment advisory firms, or both.[1]

Cetera. Between 2017 and 2020, Cetera's employees, independent contractor representatives, and offshore contractors used cloud-based email services for communications that routinely contained customers' PII.[2] In early 2018, following two incidents that resulted in the breach of 32 email accounts of Cetera's independent contractor representatives, Cetera turned on multi-factor authentication (MFA) for its employees' email accounts and most, but not all, of its independent contractors' email accounts.[3] Also in 2018, Cetera updated its policies to require that MFA be turned on "wherever possible, but at a minimum for privileged or high-risk access."[4] However, between October 2018 and June 2020, the email accounts of more than 30 independent contractors—none of which had MFA turned on, despite the policy requiring its use "wherever possible"[5]—were taken over by unauthorized third parties.[6] Furthermore, Cetera did not implement MFA for offshore contractor email accounts until the end of 2019, even though the email accounts of four such contractors were hacked in 2018 and 2019.[7] Collectively, these breaches resulted in the exposure of more than 4,388 customers' PII.[8]

Following each incident in which Cetera identified potential exposure of customer data, Cetera issued breach notifications to impacted customers. In certain instances, the notifications from two Cetera entities—Cetera Advisors LLC and Cetera Investment Advisers LLC—included template language referring to the underlying breach as "recent" and stating that Cetera had "learned that an unauthorized individual gained access" to the recipient's PII two months prior to the issuance of the notification.[9] The dates referenced in those letters, however, did not reflect the date on which the firms learned of the breach—which was at least six months earlier—but rather the date on which they had completed their review of the compromised email accounts and determined that the particular customer's PII may have been accessed.[10] Based on this conduct, the SEC found that Cetera violated the Safeguards Rule because its policy requiring MFA for privileged and high-risk access was not reasonably designed as applied to email accounts of Cetera's contractor representatives and offshore contractors, whose systems and access to sensitive data were generally at risk of compromise equal to or higher than that of Cetera employees.[11] The SEC further found that, although Cetera Advisors LLC and Cetera Investment Advisers LLC had policies requiring the firms' personnel to review client communications regarding cybersecurity incidents prior to their issuance, those procedures were not reasonably designed under Section 206(4) because the firms' review of the breach notifications was conducted in a manner that failed to correct template language that was misleading in light of the circumstances.[12] Cetera was ordered to pay a $300,000 civil money penalty in connection with these violations.[13]

Cambridge. Cambridge has approximately 4,750 registered representatives and investment adviser representatives, the vast majority of which are registered with the Financial Industry Regulatory Authority (FINRA) as independent contractors.[14] While Cambridge provided its independent representatives with cybersecurity guidance and policies, each independent representative was responsible for implementing its own cybersecurity measures.[15] Among other things, Cambridge's policies recommended, but did not

require, independent contractors to implement enhanced security measures, such as MFA, on cloud-based email accounts.[16] Between January 2018 and July 2021, Cambridge discovered that the email accounts of 121 independent contractors were taken over by unauthorized third parties.[17] After gaining access to the email accounts, the intruders took various actions, including forwarding emails containing customers' PII to parties outside of Cambridge, and using the independent representatives' accounts to email customers and request that they provide PII or click on a malicious link.[18] Cambridge determined that the confidential data of at least 2,177 customers and clients had been exposed in these breaches.[19]

After discovering the email account takeovers, Cambridge suspended the affected contractors' accounts, reset their account passwords, and recommended that these contractors implement MFA on their accounts.[20] Until July 2021, however, Cambridge did not require the affected or other independent contractors to implement MFA or adopt other security measures in order to prevent similar breaches.[21] Based on this conduct, the SEC concluded that Cambridge violated the Safeguards Rule by failing to adopt policies and procedures reasonably designed to protect customer records and information, and imposed a civil money penalty in the amount of $250,000.[22]

KMS. Between September 2018 and August 2020, KMS provided customer services through more than 400 financial advisers who were independent contractors.[23] These financial advisers used a cloud-based email system for communications, which regularly contained confidential customer information.[24] Although the financial advisers generally used their own computer equipment and networks, they were required under KMS policies to (1) "[c]onduct [their] business practices in a way that safeguards the confidentiality of [their] client's identity"; (2) "[p]eriodically review [their] internal business policies to make sure they are adequately designed to protect sensitive client information"; and (3) undertake certain security measures, such as using anti-virus and malware protection, securing stored data, and encrypting hard drives, and inform KMS of any suspected cybersecurity incidents.[25] KMS's policies recommended, but did not require, the advisers' use of MFA when accessing sensitive data.[26]

During the relevant time period, intruders gained access to the email accounts of more than 15 KMS financial advisers or their assistants.[27] With that access, hackers forwarded emails containing customer PII to external email accounts and sent emails to customers asking them to wire funds to a bank account, provide PII to access a document, or click on a malicious link.[28] Ultimately, these email account takeovers resulted in the exposure of information, including PII, concerning approximately 4,900 KMS customers.[29]

After discovering the email account takeovers, KMS took certain remedial measures, including resetting the financial advisers' passwords, removing forwarding rules, and enabling MFA.[30] However, KMS did not adopt written policies requiring additional security measures for all KMS email users until May 2020, and did not fully implement those additional security measures on a firm-wide basis until August 2020—approximately 21 months after discovery of the first breach.[31] In addition, KMS did not have its own Incident

Response Policy and instead relied upon a policy tailored to another entity owned by the same parent company, which lacked guidelines regarding timeframes for various response activities, and failed to complete written summaries of the email account takeovers until several months after the incidents were discovered.[32] For all of these reasons, the SEC concluded that KMS willfully violated the Safeguards Rule, and imposed a civil money penalty of $200,000.[33]

IMPLICATIONS

These three actions confirm, as we previously discussed in our client memoranda addressing the SEC's actions in June against First American Financial Corporation and earlier this month against Pearson plc, that the SEC is decisively moving to enhance regulated entities' focus on cybersecurity controls and disclosure controls and procedures in the cybersecurity context. The SEC's announcement of a total of five cybersecurity-based enforcement actions in three months is unprecedented, and the actions show key themes and areas of focus for the SEC in this area.

Across these actions, the SEC has demonstrated a particular focus on companies' (i) failures to implement or carry out sufficient cybersecurity policies, programs, recommendations, and widely known best practices; (ii) failures to timely remediate these lapses once they were identified; and (iii) public statements about cybersecurity incidents that the SEC has deemed misleading because disclosure personnel were inadequately and untimely informed of the relevant facts, or because the statements downplayed the timing or significance of a breach or described cybersecurity risks as hypothetical when in fact they had occurred.

For example, as to its focus on failures with respect to cybersecurity policies, programs, recommendations, and widely known best practices, in the *First American* and *Pearson* actions, the SEC alleged that the companies failed to timely remediate known, critical software vulnerabilities that exposed millions of customer records.[34] Similarly, in the newly announced actions, the SEC criticized investment advisers' failure to require MFA, a widely adopted and well-understood security precaution, and criticized one firm for lacking an incident response plan, which companies typically have, and for failing to document its cybersecurity incident timely, as companies typically otherwise do.[35]

As to failures to timely remediate identified lapses, the SEC noted in *First American* that a cybersecurity vulnerability was inadvertently documented as less severe than intended, providing the company with 90 days rather than the required 45 days under its policies to remedy the vulnerability, and that the company missed even the extended deadline.[36] Similarly, in the newly announced action against KMS, the SEC noted that KMS had received an audit report from a third party that recommended "consideration of stronger access controls, such as two-factor authorization" in July 2018, and thus, "[b]y the time of the first email account takeover in September 2018, KMS had known for several months that remote access to its systems needed stronger security controls."[37] The SEC was particularly critical that the firms in the newly announced actions did not require MFA promptly even after the companies learned that the lack of MFA enabled

account takeovers to occur.[38] In light of the SEC's focus on perceived norms in the implementation of certain cybersecurity policies and controls, companies should review their policies and controls, including with the assistance of external advisers if needed, to be comfortable that they are meeting industry standards in these areas and timely addressing cybersecurity issues that have been identified.

As to allegedly misleading statements by registrants, the SEC alleged in the *Pearson* action that the company minimized the extent of the underlying breach in public statements and that the processes leading to the drafting of those statements "failed to inform relevant personnel of certain information about the circumstances surrounding the breach."[39] The SEC also found that Pearson's risk factors in its periodic filings inaccurately described its cybersecurity risk as merely hypothetical when the risk had in fact materialized.[40] In sanctioning Cetera, the SEC likewise found that Cetera misled affected customers about the timing of the relevant breach, and that Cetera's policies governing its review of the disclosures were inadequate because "that review was conducted in a manner that failed to correct template language that was misleading in light of the circumstances."[41] In light of the SEC's scrutiny of these companies' public statements concerning cybersecurity risks and incidents, and the processes for timely informing disclosure personnel of relevant information in this regard, companies should expect heightened focus from the SEC on whether their public statements concerning cybersecurity matters are sufficiently specific and tailored to the company's circumstances and experience. Companies should also ensure that risk factors and other disclosures and public statements are adequately and timely reviewed on a regular basis, including by considering updating risk factors in periodic filings during the year.

Finally, the SEC's focus on the risk posed by independent contractors or other third parties who may have email accounts associated with a company or access to a company's network is noteworthy. The focus is unsurprising given the frequency of email account takeovers and similar cyber intrusions, and in light of the federal government's heightened awareness of the risks of vendor and supply chain attacks following the compromise of SolarWinds software. In light of this focus, companies should review their access controls for third parties to ensure they are adequate and at least as stringent as those that apply to employees.

* * *

ENDNOTES

1 U.S. Securities & Exchange Commission, Press Release, *SEC Announces Three Actions Charging Deficient Cybersecurity Procedures* (Aug. 30, 2021), *available at* https://www.sec.gov/news/press-release/2021-169.

2 *In the Matter of Cetera Advisor Networks LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC, Cetera Advisors LLC, and Cetera Investment Advisers LLC*, Securities Exchange Act Release No. 92800, Investment Advisers Act Release No. 5834 (Aug. 30, 2021), at ¶ 11 [hereinafter Cetera Order].

3 *Id.* at ¶¶ 13-15.

4 *Id.* at ¶ 11.

5 *Id.* at ¶ 15.

6 *Id.*

7 *Id.*

8 *Id.* at ¶ 3.

9 *Id.* at ¶ 18.

10 *Id*.

11 *Id.* at ¶ 17.

12 *Id.* at ¶ 19.

13 *Id.* at 7.

14 *In the Matter of Cambridge Investment Research, Inc. and Cambridge Investment Research Advisors, Inc.,* Securities Exchange Act Release No. 92806, Investment Advisers Act Release No. 5839 (Aug. 30, 2021), at ¶ 6 [hereinafter Cambridge Order].

15 *Id.* ¶ 7.

16 *Id.* ¶ 8.

17 *Id.* ¶ 9.

18 *Id*.

19 *Id.* ¶ 10.

20 *Id.* ¶ 13.

21 *Id.*

22 *Id.* ¶¶ 15-16.

23 *In the Matter of KMS Financial Services, Inc.,* Securities Exchange Act Release No. 92807, Investment Advisers Act Release No. 5840 (Aug. 30, 2021), at ¶ 5 [hereinafter KMS Order].

24 *Id.* ¶ 7.

25 *Id.* ¶¶ 8-9.

26 *Id.* ¶ 9.

27 *Id.* ¶ 10.

28 *Id.*

29 *Id.*

30 *Id.* ¶ 11.

ENDNOTES (CONTINUED)

31 *Id.*

32 *Id.* ¶¶ 13-14.

33 *Id.* at 6.

34 U.S. Securities & Exchange Commission, Press Release, *SEC Charges Issuer With Cybersecurity Disclosure Controls Failures* (June 15, 2021), *available at* https://www.sec.gov/news/press-release/2021-102; U.S. Securities & Exchange Commission, Press Release, *SEC Charges Pearson plc for Misleading Investors About Cyber Breach* (Aug. 16, 2021), *available at* https://www.sec.gov/news/press-release/2021-154.

35 KMS Order, *supra* n.23, at ¶¶ 13-14.

36 *In the Matter of First American Financial Corporation*, Securities Exchange Act Release No. 92176 (June 14, 2021), at ¶¶ 14-15.

37 KMS Order, *supra* n.23, at ¶ 12 n.7.

38 Cetera Order, *supra* n.2, at ¶¶ 15-17; Cambridge Order, *supra* n.14, at ¶¶ 13-14; KMS Order, *supra* n.23, at ¶¶ 11-13.

39 *In the Matter of Pearson plc*, Securities Act Release No. 10963, Securities Exchange Act Release No. 92676 (Aug. 16, 2021), at ¶ 13.

40 *Id.* at 2.

41 Cetera Order, *supra* n.2, at ¶ 19.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.