The Latest Round of SEC Cybersecurity Enforcement Actions Targets MFA Deficiencies, Inadequate Policies, and Misleading Breach Notifications

September 1, 2021

On August 30, 2021, the SEC filed settled enforcement actions against three groups of broker-dealers and investment advisers for failing to protect confidential customer information in violation of Rule 30(a) of Regulation S-P (the "Safeguards Rule" or "Rule"). One group of the entities was also found to have violated Section 206(4) of the Advisers Act and Rule 206(4)-7, by allegedly providing misleading information in its breach notification to customers. These actions, which were announced just two weeks after the SEC imposed a $1 million civil penalty for an issuer's allegedly misleading data breach disclosures in connection with a public company's filings, demonstrate the agency's increased efforts to enforce its cyber priorities, as we noted in July 2021 with the First American settlement.

In total, eight firms agreed to settle the charges without admitting or denying fault: Cetera Advisor Networks LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC, Cetera Advisors LLC, and Cetera Investment Advisers LLC ("Cetera"); Cambridge Investment Research Inc. and Cambridge Investment Research Advisors Inc. ("Cambridge"); and KMS Financial Services Inc. ("KMS"). Collectively, the firms will pay $750,000 in penalties to the SEC.

The Safeguards Rule. These cases mark an expansion of the SEC's use of the Safeguards Rule for cybersecurity enforcement. The Rule requires registered broker-dealers and investment advisers to adopt written policies and procedures that are reasonably designed to protect against unauthorized access to customer information that could result in harm. In 2018, the SEC used the Safeguards Rule to find that Voya, a broker-dealer and investment adviser, did not have reasonable procedures to protect customer information, and failed to apply its procedures to the systems used by its independent contractors, who made up the largest part of Voya's workforce.

The Cetera Entities. In November and December 2017, the email accounts of several Cetera contractor representatives were taken over by attackers, resulting in the exposure of personal information of Cetera customers, whose data was contained in the compromised accounts. None of these accounts had multifactor authentication ("MFA") turned on.

In January 2018, Cetera implemented mandatory MFA for employee accounts, but not contractor accounts. In February 2018, Cetera's policies were updated to require MFA for email accounts "wherever possible." In March 2018, Cetera implemented MFA for over 6,000 contractor email accounts, but in September 2018, it identified approximately 1,500 accounts email accounts that still did not yet have MFA. In October 2018, the firm's policy was amended again to require MFA, at a minimum, for all privileged or high-risk access accounts. From October 2018 to June 2020, email accounts of seven contractors were compromised, resulting in the exposure of personal information of more than 2,500 customers. None of those compromised email accounts had MFA tuned on.

Based on these facts, the SEC found that Cetera's policy requiring MFA for privileged and high-risk access "was not reasonably designed to be applied to email accounts of Cetera Entities' contractor representatives and offshore contractors, whose systems and access to sensitive data was generally at the same or higher risk of compromise than the systems and access used by Cetera employees."

Essentially, the SEC appears to have found that Cetera violated the Safeguards Rule because (1) it did not follow its policies when it failed to implement MFA for contractor accounts that had access to the same sensitive customer information as employee email accounts (which did have mandatory MFA), or (2) if it was following its MFA policies, they were inadequate to protect customer information.

Additionally, the SEC found that some of the breach notifications that were sent to impacted Cetera customers were misleading because they referred to the incidents as "recent" and having occurred two months before the notification, when in fact, the underlying breaches were discovered at least six months before the notifications were sent out.

The Cambridge and KMS Entities. According to the SEC, both Cambridge and KMS provide services to customers through independent contractors who had access to sensitive customer information in their email accounts. From 2018 to 2020, email accounts of independent contractors at both firms were taken over, resulting in the exposure of personal information of thousands of customers. Enhanced security measures, such as mandatory MFA, for the email accounts of independent contractor representatives were not required firm-wide until 2020 (at KMS) and 2021 (at Cambridge). For both firms, the email account takeovers did not appear to have resulted in any unauthorized trades or fund transfers, but the SEC nonetheless found that the conduct violated the Safeguards Rule.

Takeaways

- The SEC as Enforcer for Cybersecurity: For registered broker-dealers and investment advisers, the SEC's cyber enforcement is not limited to disclosures, as it is now clearly using the Safeguards Rule to test firms' cybersecurity policies and procedures, and bring enforcement actions where it believes those policies or practices are inadequate at protecting sensitive customer information.

- Follow MFA Policies: These cases demonstrate the need for firms to ensure that they are following their MFA policies. The Cetera Order suggests that if a firm (a) has a policy that requires MFA for a certain category of email accounts, (b) some of those email accounts are then compromised by an unauthorized third party, (c) the compromised accounts include customer personal information, and (d) those compromised accounts were not protected by MFA as required by the policy, that may be a violation of the Safeguards Rule.

- Consistency in MFA Policies: These cases also demonstrate the risks of not providing the same security measures for email accounts that contain similar information. Many firms have policies requiring MFA for a certain category of email accounts (*e.g.*, employee accounts), but those policies do not apply to other categories of email accounts (*e.g.*, contractor accounts). If, however, the employee accounts and contractor accounts have access to the same kinds of sensitive information, and some of the contractor accounts without MFA are compromised and expose customer information, there is a risk that the SEC will view that as a violation of the Safeguards Rule on the basis that the policies were not reasonably designed to protect customer information.

- Effective Remediation of Vulnerabilities: Another takeaway from these cases is that, regardless of policies, firms need to have effective responses to email account compromises that impact customer information. For example, suppose some category of company email accounts is compromised by an attacker, and those accounts, which were not protected by MFA, include customer personal information. It appears that, in those circumstances, the SEC expects firms to implement some additional security protections, such as MFA, to reduce the risks of future successful attacks against similar accounts. If no additional measures are implemented, and a successful attack occurs that compromises sensitive customer information, the SEC may view that as a violation of the Safeguards Rule.

- Accurate Breach Notifications: The final takeaway is that notices to customers and regulators about a cyber incident must be accurate. This is especially important when drafting from templates that may include generic language that may not be applicable to the particular incident, such as "we recently learned that . . . ."

To subscribe to the Data Blog, please click here.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

James Pastore
jjpastore@debevoise.com

Mengyi Xu
mxu@debevoise.com

The authors would like to thank Debevoise law clerk Eric Carlson for his contribution to this article.