Davis Polk

SEC sanctions three entities for cybersecurity policies and procedures failures

September 1, 2021 | Client Update | 3-minute read

The SEC filed three enforcement actions against investment advisers and broker-dealers for cybersecurity deficiencies after the firms experienced incidents that exposed customer and client personal information. The SEC brought the cases under the Safeguards Rule, which is designed to protect customer information.

On August 30, the Securities and Exchange Commission (SEC) announced settlements with three entities, all of which are broker-dealers, investment advisory firms, or both, for failures in their cybersecurity policies and procedures. In each case, accounts of representatives working for the firms were compromised, exposing personal information of customers and clients. The SEC brought the enforcement actions even though it appears that no unauthorized trades or transfers occurred. The firms paid penalties ranging from $200,000 to $300,000.

Cetera

Between November 2017 and June 2020, unauthorized third parties accessed cloud-based email accounts used by investment adviser representatives who were independent contractors at Cetera Advisor Networks LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC, Cetera Advisors LLC, and Cetera Investment Advisers LLC (collectively, Cetera), resulting in the exposure of personally identifying information of over 4,000 customers and clients. The SEC found that the accounts were not protected in a manner consistent with Cetera's policies. For example, these accounts did not have multi-factor authentication (MFA) turned on even though Cetera's policies required them "whenever possible." In addition, the SEC found that Cetera had sent breach notifications to clients that included misleading language, suggesting to clients that the notifications were issued sooner than they actually were after discovery of the incidents.

Cambridge

Between January 2018 and July 2021, unauthorized third parties accessed cloud-based email accounts used by independent contractor representatives working for Cambridge Investment Research Inc. and Cambridge Investment Research Advisors Inc. (collectively, Cambridge). The unauthorized access arose from a variety of techniques, including phishing (tricking users into clicking on links in emails that download malware) and credential stuffing (automatically entering many different user name and password combinations), resulting in the exposure of personally identifying information of over 2,000 Cambridge customers and clients. The firm suspended the accounts, reset passwords, and recommended that the representatives implement MFA. The firm did not, however, require MFA or any other enhanced security measures until mid-2021.

KMS

Between September 2018 and December 2019, threat actors accessed cloud-based email accounts used by financial advisers at KMS Financial Services Inc. (KMS), resulting in the exposure of personally identifying information of approximately 4,900 KMS customers and clients. The firm implemented new security measures for the affected accounts, such as MFA, but did not fully implement them firm-wide until nearly two years later.

Takeaways

The cases have several important takeaways:

1. While these are the first Safeguards Rule cases in nearly three years (since the last action in 2018), the cases follow the SEC's recent actions concerning cybersecurity disclosures by public companies (discussed in our recent client update) and show the SEC's continuing focus on cybersecurity issues.
2. Each case mentioned MFA as a cybersecurity safeguard. Although the SEC did not say MFA is an absolute requirement, it is evidence that the SEC will focus on the absence of MFA in its exams and enforcement investigations.
3. The SEC focused on the firms' responses to the incidents. It is an important reminder to review incidents for possible lessons learned and implement any appropriate improvements within a reasonable timeframe.
4. Finally, in addition to investigating the adequacy of the firms' cybersecurity programs, the SEC also reviewed the firms' compliance with their own policies. The cases serve as a reminder that the SEC will hold firms accountable for not enforcing their own policies and procedures.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Matthew J. Bacal
+1 212 450 4790
matthew.bacal@davispolk.com

Martine M. Beamon
+1 212 450 4262
martine.beamon@davispolk.com

Angela T. Burgess
+1 212 450 4885
angela.burgess@davispolk.com

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

Paul J. Nathanson
+1 202 962 7055
+1 212 450 3133
paul.nathanson@davispolk.com

Gabriel D. Rosenberg
+1 212 450 4537
gabriel.rosenberg@davispolk.com

Margaret E. Tahyar
+1 212 450 4379
margaret.tahyar@davispolk.com