Skadden

SEC Reporting & Compliance Alert

SEC Heightens Focus on Cybersecurity

On August 30, 2021, the Securities and Exchange Commission (SEC) announced that eight broker-dealers and/or investment advisers will pay civil monetary penalties to resolve enforcement actions arising from cybersecurity incidents that led to exposure of personally identifying information (PII) of thousands of customers and clients. Each of the incidents involved email account takeovers by unauthorized third parties. The related failures that led to the violations, however, differ in each action:

Firms	Time Period	# of Impacted			Alleged Company Failures According to SEC Order
		Entities	Company/ Affiliate Email Accounts	Customers/ Clients	
Cetera Advisor Networks LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC, Cetera Advisors LLC and Cetera Investment Advisers LLC	Nov. 2017–June 2020	5	60	4,388	– The companies did not protect the affected accounts in a manner consistent with the company's policies, leading to unauthorized access of the accounts (a violation of Regulation S-P, Rule 30(a)). – The companies failed to adopt and implement policies and procedures to review customer communications; as a result, breach notifications sent to clients included misleading language that suggested that the notifications were sent much sooner than they actually were after discovery of the incidents (a violation Section 206(4) of the Advisers Act; Rule 206(4)-7).
Cambridge Investment Research Inc. and Cambridge Investment Research Advisors Inc.	Jan. 2018–July 2021	2	121	2,177	The companies failed to adopt and implement firmwide enhanced security measures for cloud-based email accounts until 2021 — three years after discovering the first email account takeover (a violation of Regulation S-P, Rule 30(a)).
KMS Financial Services Inc.	Sept. 2018–Dec. 2019	1	15	4,900	The company failed to adopt written policies and procedures requiring additional firmwide security measures until May 2020 and did not implement those additional security measures firmwide until August 2020, despite discovering the first email incident in November 2018 (a violation of Regulation S-P, Rule 30(a)).

Consumer Privacy Regulations

The SEC found that each of the firms violated Rule 30(a) of Regulation S-P — also known as the Safeguard Rule — that requires registered broker-dealers, investment companies and investment advisers to adopt policies to safeguard customer records and information. The actions underscore that consumer privacy regulations continue to provide the SEC with a mechanism to bring enforcement actions following cyber events, particularly where companies fail to (i) adopt or implement written cybersecurity policies or (ii) enhance their cybersecurity policies and practices in a timely manner following a breach.

Third-Party Communications About Cyber Events

Misleading or inaccurate third-party communications about cyber events may form the basis of liability. According to the SEC order, Cetera's outside counsel sent impacted clients breach notifications informing them that Cetera had experienced a "recent" cyber incident and "learned that an unauthorized individual gained access to" the client's PII two months prior to the notification; in fact, Cetera learned of the breach at least six months earlier. As a result, the SEC found that Cetera violated Section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder.

Other Recent SEC Cyber Actions

The Cetera order follows SEC settlements with First American Financial Corporation (First American) and Pearson plc (Pearson) on June 15, 2021, and August 16, 2021, respectively. Both actions related to disclosure controls and misleading statements made to investors with respect to cyber incidents.

- **First American:** This action addressed disclosures made in connection with a cybersecurity vulnerability involving the company's document image sharing application, which exposed over 800 million title and escrow document images, including images containing sensitive personal data and financial information. A cybersecurity journalist first brought the vulnerability to the company's attention, and in response, the company issued a statement for inclusion in the journalist's report and disclosed the event on a Form 8-K. The SEC found that the company's disclosure controls and procedures failed to inform senior executives, who were responsible for the public disclosures, that the company's information security personnel were previously aware of the vulnerability or that the company failed to remediate the issue in accordance with company policies. As a result of failing to ensure that senior management had this relevant information prior to issuing disclosures about the vulnerability, the SEC found that First American violated Exchange Act Rule 13a-15(a).
- **Pearson:** The SEC charged the company with making material misstatements and omissions regarding a cyber intrusion involving the theft of millions of student records. According to the SEC, Pearson's disclosures implied that it faced the hypothetical risk that a "data privacy incident" "could result in a major data privacy or confidentiality breach," but did not disclose that the company had experienced such a breach. Pearson also issued a media statement, approximately two weeks after sending breach notifications to affected customers, that made misstatements about the nature of the breach and data involved. The SEC found that Pearson violated Sections 17(a)(2) and 17(a)(3) of the Securities Act and Section 13(a) of the Exchange Act and Rules 12b-20, 13a-15(a) and 13a-16 thereunder.

SolarWinds Sweep[1]

In addition to the five cybersecurity-related actions the SEC has brought over the summer of 2021, beginning in June 2021, the Enforcement Division sent numerous letters requesting information from issuers and other SEC-regulated companies that the SEC "believe[s] … may have been impacted by the SolarWinds Compromise." The letters requested information about the December 2020 SolarWinds cyber breach, as well as "Other Compromises," which the SEC defined broadly as "unauthorized access by external actors lasting longer than one day, without limitations based on materiality or access to material nonpublic information."

Takeaway

These recent cyber enforcement actions, coupled with the inclusion of "cybersecurity risk governance" on the SEC's near-term rulemaking agenda, signal that cybersecurity will continue to be a priority area for the SEC. Taken together, these enforcement actions underscore the importance of (i) completeness and accuracy when describing cyber incidents to third parties, whether customers, clients or investors and (ii) disclosures and procedures that provide timely and accurate information to investors about material cyber events. SEC staff also has warned that companies should not understate the nature and scope of cyber incidents or overstate the company's cyber protections. Issuers and other SEC-regulated entities should continuously monitor their cybersecurity protections and disclosure controls and provide complete, accurate and timely updates to disclosures, particularly in the wake of a cybersecurity incident.

[1] See our June 19, 2021, client alert "Recent SEC Enforcement Requests Related to SolarWinds Cyberattack."

SEC Reporting & Compliance Alert

Contacts

Brian V. Breheny
Partner / Washington, D.C.
202.371.7180
brian.breheny@skadden.com

Andrew M. Lawrence
Partner / Washington, D.C.
202.371.7097
andrew.lawrence@skadden.com

Colleen P. Mahoney
Partner / Washington, D.C.
202.371.7900
colleen.mahoney@skadden.com

Andrew Hanson
Associate / Washington, D.C.
202.371.7225
andrew.hanson@skadden.com

Raquel Fox
Partner / Washington, D.C.
202.371.7050
raquel.fox@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Lauren A. Eisenberg
Associate / Washington, D.C.
202.371.7564
lauren.eisenberg@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Avenue, N.W.
Washington, D.C. 20005
202.371.7000

skadden.com