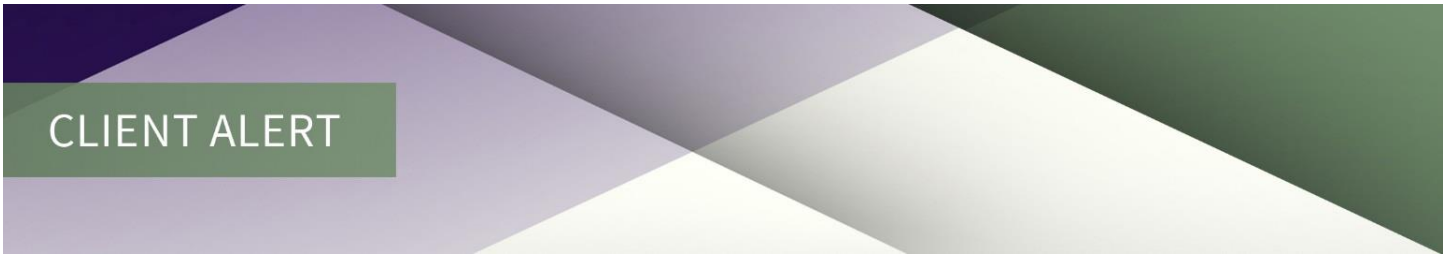
WILLKIE FARR & GALLAGHER LLP



SEC Prioritizes Cyber/Privacy Enforcement

September 16, 2021

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Elizabeth P. Gray | Elizabeth Bower
Amelia A. Cottrell | William J. Stellmach | Richard M. Borden

Over the past few months, the Securities and Exchange Commission (the "SEC") has taken a number of enforcement actions related to cybersecurity issues broadly, and to data security and privacy issues in particular, adding muscle to Chair Gensler's commitment to policing financial markets for cybersecurity vulnerabilities. Most recently, last month the SEC announced three settlements stemming from financial firms' failures to implement appropriate data security policies and procedures as required by Rule 30(a) of Regulation S-P (the "Safeguards Rule"), and earlier in the month announced a settlement with a publicly traded company for failure to disclose adequately the known effects of a data security breach involving personal information. For companies that fall within the SEC's broad ambit, the key takeaway is that the SEC is approaching cybersecurity, data security, and privacy issues in a manner that could have significant implications for the ways that financial institutions and public issuers disclose, identify, and mitigate cybersecurity and data security risk.

Background

Cybersecurity and Data Security Requirements

The protection of customer and non-public information has been an explicit and increasingly important priority for the SEC in recent years, including with respect to the implementation of appropriate technical security measures. For instance, the 2021 Examination Priorities identified a primary focus on measures to "safeguard customer accounts and prevent account intrusions, including verifying an investor's identity to prevent unauthorized account access."[1] Likewise, in 2020, the SEC

[1] SEC Office of Compliance Inspections and Examination, *2021 Examination Priorities*, at p. 24 (here).

emphasized the need to manage user access through systems and procedures that leverage security features like multi-factor authentication ("MFA").[2]

These recent enforcement actions highlight two of the primary tools that the SEC has available to it for regulating the cybersecurity and data security space. First, the SEC's Safeguards Rule requires every broker-dealer, investment company, and investment advisor registered with the SEC to adopt written policies and procedures "that address administrative, technical and physical safeguards for the protection of customer records and information."[3] Such policies must be reasonably designed to do the following:

(1) insure the security and confidentiality of customer records and information;

(2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and

(3) protect against unauthorized access to or use of such records that could result in substantial harm or inconvenience to customers.

Second, the SEC's ability to impose disclosure requirements for public issuers under Sections 17(a)(2)-(3) of the Securities Act of 1933, and Section 13(a) of the Exchange Act of 1934, and regulations promulgated thereunder, provides a powerful stick that the Commission can use against any publicly traded company. In 2018 guidance on this subject, the SEC said, "Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack."[4]

The Settlements

Security Rule Settlements: Cetera Entities, Cambridge Investment, KMS Financial Services

On August 31, 2021, the SEC announced three actions against the Cetera Entities, Cambridge Investment, and KMS Financial Services. Each is a registered broker-dealer, investment advisory firm, or both. All also experienced data security breaches stemming from unauthorized third parties taking over cloud-based email accounts, where the firm's failure to detect the breach and/or failure to subsequently implement appropriate remedial measures contributed to ongoing security vulnerabilities that placed customer information at risk for an extended period. As part of the

2 SEC Office of Compliance Inspections and Examinations, *Cybersecurity and Resiliency Observation*, at p. 3 (here).

3 17 CFR § 248.30(a).

4 https://www.sec.gov/rules/interp/2018/33-10459.pdf.

settlements, the SEC found that each firm willfully violated the Safeguards Rule, ordered the firms to cease and desist from such violations, censured each firm and imposed penalties ranging from $200,000 to $300,000.

One of the common themes throughout these actions is that the SEC specifically identified failures to properly implement MFA—inconsistent with the firm's written policies (Cetera Entities), as an appropriate security enhancement following detection of an initial account takeover (Cambridge Investment), or for delayed implementation (KMS Financial)—as contributing to violations of the Safeguards Rule. *The focus on MFA suggests that the practice is now considered by regulators as a baseline requirement of reasonable security measures, not a "nice to have" best practice.*

Pearson

Pearson is a publicly traded, London-based multinational educational publishing and services company that experienced a data security breach in 2018, resulting in the exposure of U.S. student data. In its action against Pearson, the SEC found that the company omitted material facts about the incident in its 2019 Form 6-K disclosure (wherein it identified data privacy incidents as a hypothetical risk but failed to disclose that the firm had actually experienced a breach), and thereafter misled affected individuals through its belated breach notification by misstating the amount and type of data involved.

The SEC also noted that the 2018 breach stemmed from a vulnerability in software used by Pearson, that Pearson had been notified by the software manufacturer about the criticality of the vulnerability and the existence of a patch beginning in September 2018, and that Pearson did not implement the patch until after it learned of the attack in March 2019. These particular facts are not directly relevant to the SEC's primary charge—that Pearson failed to make proper disclosures—but their inclusion strongly suggests that the SEC will consider a company's efforts to address cybersecurity and data security risk as part of its analysis.

Takeaways

Following the SEC's enforcement action earlier this summer focusing on public disclosures related to cybersecurity, these August enforcement actions related to specific practices and failure to make adequate disclosures serve as a reminder that the agency has some potentially significant tools at its disposal that it is increasingly willing to use to drive the policy discussion and to require companies to take steps they may not otherwise want to take.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Laura E. Jehl
202 303 1056
ljehl@willkie.com

Elizabeth P. Gray
202 303 1207
egray@willkie.com

Elizabeth Bower
202 303 1252
ebower@willkie.com

Amelia A. Cottrell
212 728 8281
acottrell@willkie.com

William J. Stellmach
202 303 1130
wstellmach@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com