Davis Polk

SEC enforcement action highlights need for internal communications about cybersecurity problems

June 17, 2021 | Client Update | 4-minute read

The SEC filed an enforcement action involving a public company's cybersecurity disclosure. The action highlights the need for executives responsible for SEC reporting to be informed promptly about cybersecurity risks and incidents.

The Securities and Exchange Commission (SEC) announced a settled enforcement action on June 15 against a company for violating the requirement that public companies have controls and procedures to ensure that they make required disclosures in SEC filings. According to the SEC's order, a cybersecurity journalist informed the company of a vulnerability in a proprietary application that the company used to store and share document images. The vulnerability exposed more than 800 million documents that contained sensitive personal information, although the SEC's order did not say that anyone exploited the vulnerability to access the sensitive information. The company issued a statement for the journalist's report the same day, and filed a Form 8-K four days later.

The SEC alleged that senior executives responsible for filing the 8-K were not aware that company personnel had identified the vulnerability months before, or that the issue was not remediated as company policy required. Unaware of that history, despite attending meetings with informed personnel, the senior executives did not evaluate whether to disclose the prior detection or the failed remediation. As a result, the SEC concluded that the company violated the disclosure controls rules, which require controls and procedures "designed to ensure that information required to be disclosed by the issuer in the reports that it files or submits … is recorded, processed, summarized and reported, within the time periods specified" in SEC rules. Without admitting or denying the SEC's findings, the company agreed to pay a penalty of approximately $0.5 million. Demonstrating a recent increase in interagency cooperation on cybersecurity issues, the SEC acknowledged the assistance of the New York State Department of Financial Services, which previously filed a related enforcement action against the company.[1]

Takeaways

Although the SEC has filed few cases involving cybersecurity-related disclosures, this case shows the SEC's willingness to bring enforcement actions to back up its recent guidance on this topic. Public companies may want to revisit the SEC's 2018 guidance that the SEC expects disclosure controls to address cybersecurity risk and incidents:

When designing and evaluating disclosure controls and procedures, companies should consider whether such controls and procedures will appropriately record, process, summarize, and report the information related to cybersecurity risks and incidents that is required to be disclosed in filings. Controls and procedures should enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents.[2]

The case also is noteworthy for the SEC's decision to find a violation of the disclosure controls rules, which have been the subject of limited enforcement actions.[3] This may signal increased enforcement focus on internal controls

requirements, even in the absence of a disclosure violation or actual harm.

Cybersecurity is a material risk for many companies, but risk profiles vary by industry and company. Finding the right balance of cybersecurity updates without overwhelming senior management with too much information is an increasingly important governance challenge for public companies. With the growing frequency of cybersecurity vulnerabilities and incidents, companies can expect increased government scrutiny after disclosure of a cybersecurity issue. This includes the SEC, which we expect will continue to bring enforcement actions in this area.

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

Joseph A. Hall
+1 212 450 4565
joseph.hall@davispolk.com

Tatiana R. Martins
+1 212 450 4085
tatiana.martins@davispolk.com

Stefani Johnson Myrick
+1 202 962 7165
stefani.myrick@davispolk.com

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

[1] *See NYDFS Enforcement Action: Statement of Charges and Notice of Hearing to First American Title Insurance Company* (Jul. 21, 2020) (available at https://www.dfs.ny.gov/system/files/documents/2021/03/ea20200721_first_american_notice.pdf).

[2] *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, 83 Fed. Reg. 8166, 8171 (Feb. 26, 2018) (available at https://www.sec.gov/rules/interp/2018/33-10459.pdf).

[3] In 2019, the SEC charged four companies with violating a different aspect of the rule, Rule 13a-15, that requires companies to have internal controls over financial reporting. *See SEC Charges Four Public Companies with Longstanding ICFR Failures* (Jan. 29, 2019) (available at https://www.sec.gov/news/press-release/2019-60).