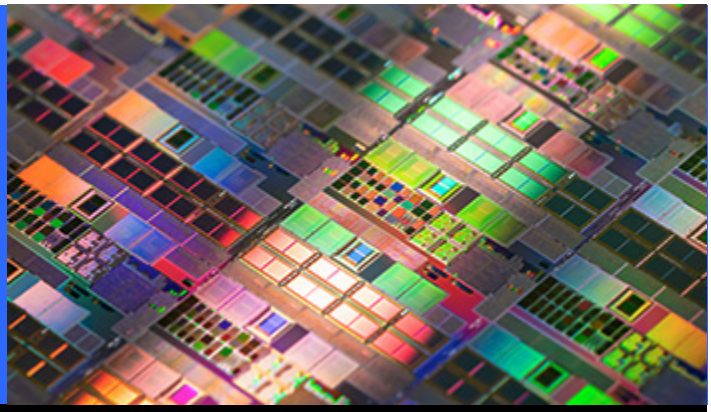
View on our website.

GIBSON DUNN



Privacy, Cybersecurity & Data Innovation Update June 20, 2024

SEC as Cybersecurity Regulator

SEC Expands Scope of Internal Accounting Controls to Encompass Companies' Cybersecurity Practices in Recent Enforcement Action.

In another extension of the internal accounting controls provisions of the securities laws, this week the Securities and Exchange Commission (the "Commission" or "SEC") announced a settled enforcement action with a public company victimized by a ransomware attack (the "Company") for violations of Section 13(b)(2)(B) of the Exchange Act and Exchange Rule 13a-15(a). According to the Commission's order, the Company's response to the late-2021 cyber incident showed that it had failed to (1) devise and maintain a sufficient "system of cybersecurity-related internal accounting controls" sufficient to provide reasonable assurances that access to its IT systems was only permitted with management's authorization, in violation of Section 13(b)(2)(B); and (2) design effective disclosure controls and procedures for cybersecurity risks and incidents, in violation of Rule 13a-15(a). As part of the settlement, the Company agreed to pay a $2.125 million civil penalty, an amount which, according to the SEC's announcement, took into account the Company's "meaningful cooperation that helped expedite the staff's investigation" and their voluntary adoption of "new cybersecurity technology and controls."

The settlement is notable in two key respects:

1. It departs from the traditional disclosure-related theories that have underpinned previous settlements related to cyber incidents; and
2. It extends the internal accounting controls provisions of Section 13(b)(2)(B) of the Exchange Act, which the SEC has already used to resolve other financial reporting and

disclosure cases, to a company's IT systems, as well as related policies and procedures relating to cybersecurity.

The order reflects an aggressive stance by the Commission as to the scope of its authority and is an articulation of its belief that it can use authorities relating to internal accounting controls—namely Section 13(b)(2)(B) of the Securities Exchange Act—to regulate public companies' cyber-related procedures (including vendor management and incident response) even in the absence of unauthorized access to a company's financial or accounting systems.

The order was accompanied by a strongly-worded dissent from Commissioners Hester Peirce and Mark Uyeda, challenging this expansive interpretation of the SEC's authority. Commissioners Peirce and Uyeda accused the Commission of "stretch[ing] the law" and "distort[ing]" the internal accounting controls provision to regulate public companies' cybersecurity practices—including deeming any departure from what the Commission deems appropriate policies to be an internal accounting controls violation.

Background

For a period of approximately four weeks in 2021, the Company was the victim of a ransomware incident during which a threat actor was able to exfiltrate data belonging to 29 of the Company's clients, including data containing personal identification and financial information. Notably, the investigation into the incident uncovered no evidence that financial systems or corporate financial and accounting data were accessed. The Company's internal intrusion detection system began issuing alerts on the day the attack commenced, and the third-party managed security services provider ("MSSP") tasked with reviewing these alerts escalated three of these alerts to the Company. The MSSP also reviewed, but did not escalate, at least 20 other alerts. In its escalation, the MSSP noted that there were indications that similar activity was taking place on multiple computers, that there were connections to a broad phishing campaign, and that the malware appeared capable of facilitating remote execution of arbitrary code. Personnel at the Company reviewed the escalated alerts but, in partial reliance on its MSSP, did not conduct its own investigation of the activity or remove infected instances off the network. The Company did not actively respond to the cyber-attack until it was alerted by another company with shared access to the Company's network several weeks later. The Company then promptly undertook an extensive response operation, notified government agencies and clients, and issued public disclosures.

A novel and expansive interpretation of internal accounting controls in the cybersecurity context

The Commission's order for the first time applies an already expansive view of internal accounting controls to the cybersecurity context. Specifically, Section 13(b)(2)(B)(iii) requires issuers to "devise and maintain **a system of internal accounting controls sufficient to provide reasonable assurances** that . . .**access to assets** is permitted only in accordance with management's general or specific authorization." In the order, the Commission found that the Company failed to devise and maintain "a system of cybersecurity-related internal accounting controls" sufficient to provide reasonable assurances that **access to its "information technology systems and networks"** was only permitted with management's

authorization. Asserting that information technology systems and networks are "assets" is a novel and an expansive interpretation of Section 13(b)(2)(B)(iii).

As noted in the dissent, this interpretation of what constitutes an "asset" "breaks new ground," and there are arguments that this expansion runs contrary to the statutory language and policy. Commissioners Peirce and Uyeda noted that computer systems do not "fit the category of assets captured by Section 13(b)(2)(B)" because they "are not the subject of corporate transactions," and that expanding the definition of "assets" in this way "ignores the distinction between internal accounting controls and broader administrative controls." Notably, the Commission concluded that the computer systems at issue were "assets" despite the fact that the Company's investigation into the incident "uncovered no evidence that the threat actor accessed the Company's financial systems and corporate financial and accounting data."

While the Commission has taken an increasing interest in cybersecurity incidents, almost all of its recent cybersecurity enforcement efforts have focused on companies' disclosures (or lack thereof) of cybersecurity incidents. For example, in 2023, the SEC announced a $3M settlement with a South Carolina-based software company impacted in a 2020 ransomware attack. The SEC alleged that the company violated its "obligation to provide [] investors with accurate and timely material information" by making inaccurate disclosures about the types of information affected by the ransomware attack, even after company personnel learned "that its earlier public statements about the attack were erroneous."

Similarly, in 2021, the SEC brought a settled enforcement action against a London-based public company finding that it misled investors about a cyber intrusion involving the theft of millions of student records. That action came on the heels of two similar enforcement actions in 2018 and 2019. Notably, the SEC did not bring any of these enforcement actions under Section 13(b)(2)(B) of the Exchange Act. Rather, all three of these actions alleged violations in line with more established SEC legal enforcement theories, namely that the companies in question had violated provisions of the Sections 17(a)(2) and 17(a)(3) of the Securities Act of 1933, which prohibits material misrepresentations in the offer or sale of securities, and Section 13(a) of the Exchange Act, which requires companies to file complete and accurate annual and quarterly reports with the Commission.

This latest action departs from the traditional disclosure-related theories that have underpinned these and other previous settlements related to cyber incidents, and instead extends the internal controls provisions of the Exchange Act to a company's IT systems, as well as related cybersecurity policies and procedures. This expansive view of "accounting controls" in Section 13(b)(2)(B) represents yet a further extension of the Commission's use of this provision to resolve financial reporting and disclosure cases (over the objection of Commissioners Peirce and Uyeda):

- In a 2023 case, the Commission alleged that a company's use of Rule 10b5-1 plans that included "accordion" provisions—which gave the company flexibility on when it could buy back stock—reflected that the company had "insufficient accounting controls." In their dissent, Commissioners Peirce and Uyeda noted that "[w]e do not have the authority to tell companies how to run themselves, but we now routinely use Section 13(b)(2)(B) to do just that" and further noted that the company's alleged failures had nothing to do with accounting controls as required by the statute.

- In 2020, the Commission brought a similar case alleging violations of Section 13(b)(2)(B) in connection with a stock buyback (the allegation was that the company's process to assess whether it was in possession of material non-public information at the time of the buyback was inadequate). In that case, Commissioner Peirce also issued a strongly worded dissent, noting that "the Order does not articulate any securities law violations." Commissioner Peirce highlighted "the ease with which a violation of [Section 13(b)(2)(B)] can be alleged," including "the lack of specific standards" "by which to evaluate the sufficiency of controls," which mean that "even good faith corporate behavior may be scrutinized with 20/20 hindsight."

What constitutes "sufficient" controls?

Despite finding fault with several aspects of the Company's controls, the Commission did not provide guidance to companies seeking to ensure that their cybersecurity controls are sufficient to the Commission. In the settlement, the Commission alleged the following shortcomings:

- Failure to escalate alerts to management. The Commission found that the Company's procedures and controls were not designed to ensure that all relevant information relating to cybersecurity alerts and incidents would be provided to the Company's disclosure decision-makers in a timely manner, which resulted in it failing to adequately assess the information from a disclosure perspective.
- Deficiencies in vendor management. The Commission found several deficiencies in the Company's management of its MSSP, including that the Company did not:
    - reasonably manage their MSSP's allocation of resources to reviewing intrusion detection alerts;
    - "reasonably set out a sufficient prioritization scheme and workflow for review and escalation of the alerts" in its contract with its MSSP; and
    - have sufficient oversight over its MSSP to ensure that its review and escalation of the cybersecurity alerts was consistent with the Company's instructions.
- Deficiencies in cyber incident policies and procedures. The Commission found that the Company's internal incident response policies did not sufficiently identify lines of responsibility, criteria for incident prioritization, or procedures for incident response and reporting, nor did they ensure that relevant information was communicated to decision-makers in a timely manner to allow for potentially required disclosures. Notably, the Commission did not specify what policies *would* be sufficient in its view. The Commission also found that for alerts that were escalated to the Company, its staff members tasked with review of such alerts did not have sufficient time to dedicate to the escalated alerts because they had significant other responsibilities.

Disclosure controls and procedures

The Commission's order also found that "[d]espite the importance of data integrity and confidentiality" to the Company, the Company failed to design effective disclosure-related controls and procedures around cybersecurity incidents to "ensure that relevant information was communicated to management to allow timely decisions regarding potentially required disclosure." According to the order, the Company's processes did not provide for how cyber-related incidents should be communicated to the Company's "disclosure decision-makers" in a

timely manner. As a result, the cyber incident was not adequately assessed from a disclosure perspective.

Practical implications

The Commission's use of Section 13(b)(2)(B) of the Exchange Act to regulate public companies' cyber-related procedures (including vendor management and incident response), even in the absence of unauthorized access to a company's financial or accounting systems, suggests that public companies who are victims of cyber incidents may face further scrutiny from the Commission in the future.

As a practical matter, the lack of guidance from the SEC as to what they would find to be "reasonable" or "appropriate" presents significant challenges for companies looking to learn from this settlement and respond to the SEC's expectations. This is perhaps a natural consequence of the SEC's extension of Section 13(b)(2)(B) to a wholly unrelated area, as the letter of the law does not provide any guidance. Nonetheless, looking at the SEC's area of focus in this settlement, companies can:

- Ensure that policies governing cybersecurity and incident response:
    - sufficiently identify lines of responsibility and authority;
    - set out clear criteria for alert and incident prioritization; and
    - establish clear workflows for cybersecurity alert review, incident response, and internal escalation and reporting, including to disclosure decision-makers.
- Ensure that relevant contracts with third-party managed securities services providers set out a prioritization scheme and workflow for review and escalation of cybersecurity alerts.
- Establish and maintain robust procedures to audit and oversee third-party managed securities services providers.

The following Gibson Dunn lawyers prepared this update: Sophie Rohnke, Sarah Pongrace, Sarah Scharf, Vivek Mohan, Mark Schonfeld, Stephenie Gosnell Handler, Michael Scanlon, Julia Lapitskaya, David Woodcock, and Tina Samanta.

Gibson Dunn lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any leader or member of the firm's Privacy, Cybersecurity & Data Innovation, Securities Enforcement, or Securities Regulation & Corporate Governance practice groups:

Privacy, Cybersecurity and Data Innovation:
Ahmed Baladi – Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com)
S. Ashlie Beringer – Palo Alto (+1 650.849.5327, aberinger@gibsondunn.com)
Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com)
Joel Harrison – London (+44 20 7071 4289, jharrison@gibsondunn.com)
Jane C. Horvath – Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com)
Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com)
Rosemarie T. Ring – San Francisco (+1 415.393.8247, rring@gibsondunn.com)
Sophie C. Rohnke – Dallas (+1 214.698.3344, srohnke@gibsondunn.com)

Securities Enforcement:
Tina Samanta – New York (+1 212.351.2469, tsamanta@gibsondunn.com)
Mark K. Schonfeld – New York (+1 212.351.2433, mschonfeld@gibsondunn.com)
David Woodcock – Dallas/Washington, D.C. (+1 214.698.3211, dwoodcock@gibsondunn.com)

Securities Regulation and Corporate Governance:
Elizabeth Ising – Washington, D.C. (+1 202.955.8287, eising@gibsondunn.com)
Thomas J. Kim – Washington, D.C. (+1 202.887.3550, tkim@gibsondunn.com)
Julia Lapitskaya – New York (+1 212.351.2354, jlapitskaya@gibsondunn.com)
James J. Moloney – Orange County (+1 1149.451.4343, jmoloney@gibsondunn.com)
Ronald O. Mueller – Washington, D.C. (+1 202.955.8671, rmueller@gibsondunn.com)
Michael Scanlon – Washington, D.C.(+1 202.887.3668, mscanlon@gibsondunn.com)
Lori Zyskowski – New York (+1 212.351.2309, lzyskowski@gibsondunn.com)