wiley

ALERT

Dissenting Commissioners Criticize SEC's Latest Cybersecurity Disclosure Cases

November 4, 2024

Continuing its controversial and aggressive approaches to cybersecurity, the U.S. Securities and Exchange Commission (SEC) recently charged four current and former public companies for purportedly "materially misleading disclosures" about cybersecurity intrusions and risks. The four victim companies, without admitting or denying the facts of the SEC's allegations, agreed to pay civil penalties ranging from $4 million to $995 thousand for a combined total of nearly $7 million dollars to settle the charges. Two Commissioners sharply dissented from these charges, reproaching the SEC for "playing Monday morning quarterback" through a "hindsight review" second-guessing cybersecurity disclosures and citing "immaterial, undisclosed details to support its charges." They highlighted the SEC's "troubling" approach to materiality and inconsistency with the rulemaking that led to the controversial 2023 cybersecurity disclosure rule (2023 Cybersecurity Rule), longstanding Supreme Court precedent, and a federal district court's recent rejection of similar SEC theories. While the disclosures at issue pre-dated the 2023 Cybersecurity Rule, these proceedings are a cautionary tale for companies trying in good faith to comply with the Rule's disclosure requirements.

Background

The SEC's charges stemmed from its investigation of public companies potentially impacted by "one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and the private sector." The SEC alleged that in 2020 or 2021, each issuer learned that the threat actor likely behind the hack had accessed its systems without authorization. Two issuers supposedly omitted certain material information from their

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Privacy, Cyber & Data Governance

Securities Enforcement and Litigation

cyberattack disclosures while the others failed to update an existing risk factor in response. The SEC found each issuer "negligently minimized its cybersecurity incident in its public disclosures" further victimizing investors and shareholders. It charged them with violating the Securities Act of 1933, the Securities Exchange Act of 1934, and their related rules. Notably, the U.S. District Court for the Southern District of New York (SDNY) recently rejected the SEC's strained argument that internal controls accounting requirements for public companies in the Securities Exchange Act of 1934 extended to a company's cybersecurity policies and procedures.

Issuer 1

The SEC found Issuer 1's disclosures omitted material information, emphasizing "the likely attribution of the [cyberattack] to a nation-state threat actor." The dissent showed this was inconsistent with the SEC's own prior statements, investor opinions, and basic legal standards.

To start, the dissent criticized the SEC for regulating by enforcement, specifically, using a settled proceeding to articulate that the identity of a threat actor is material. Indeed, "it is highly unlikely that investors consider this information to be material." Neither the SEC nor investors raised this as material during the rulemaking process for the 2023 Cybersecurity Rule which involved over 150 comment letters. Even more, in adopting the Rule, the SEC stated cybersecurity incident disclosures should "focus … primarily on the impacts of … [the] … incident, rather than on … details regarding the incident itself." Threat actor identity, the dissent asserted, is "an obvious 'detail … regarding the incident,' [and] lacks a clear link to the 'impact' of the incident." Troublingly, the dissent found other undisclosed information the SEC highlighted to be the incident's "details" instead of "impact."

The dissent also clarified that government agencies (the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, the Office of the Director of National Intelligence, and the National Security Agency) jointly stated, and the media widely reported, that Russia was the likely threat actor before Issuer 1's disclosure. Quoting Supreme Court precedent from 1976, the dissent found it unlikely that identifying "Russia would have 'significantly altered the 'total mix' of information' about [Issuer 1] to a reasonable investor in light of the existing public information about the cyberattack."

Issuer 2

Like Issuer 1, the SEC found Issuer 2 omitted information from its disclosures. Notably, Issuer 2 filed not one, but three, Form 8-Ks regarding the cyberattack before the SEC had even imposed such a requirement with its 2023 Cybersecurity Rule. The SEC did not credit its efforts, particularly taking issue instead with "the large number of impacted customers and the percentage of code exfiltrated by the threat actor."

First, Issuer 2's disclosures did not identify a number or percentage but instead divulged that (1) the cyberattack accessed encrypted customer credentials; (2) it reset affected credentials; and (3) it did not find any "evidence that the threat actor accessed email or archive content held by [it] on behalf of [its] customers." The dissent found this sufficient under SDNY's recent logic that "perspective and context are critical" to evaluate if a Form 8-K is materially misleading and if "[the] disclosure, read as a whole, captured the big

picture," the filing is not material. "[R]ead as a whole," Issuer 2's disclosure "conveys the complete story about the unauthorized access of credentials and the lack of misappropriated information." But the SEC disregarded SDNY's reasoning and instead focused on "the detail of the threat actor accessing a database containing customer credentials." As the dissent explained, accessing credentials, on its own, does not necessarily equate to material information if the threat actor fails to use the credentials to misappropriate customer information.

Second, Issuer 2's incident report attached to its third Form 8-K disclosed the threat actor downloaded a "limited number" of its source code repositories, but the download was "incomplete and would be insufficient to build and run any aspect of the [Issuer 2's] service." Per the dissent, the material disclosure was the cyberattack "not result[ing] in modifications of the company's source code or hav[ing] effects on its products." Yet, the SEC wanted Issuer 2 to disclose precise percentages and identify the specific types of source code. As the dissent emphasized, the SEC "ignores the *reasonable* investor standard embedded within the materiality concept and the types of information that such investor would consider important in making an investment decision." (emphasis in the original).

Issuer 3

Unlike the first two issuers, the SEC alleged that Issuer 3 did not update its existing risk factor in response to the cyberattack. Curiously, the SEC found Issuer 3's risk disclosure was generic and required revision because the cybersecurity risk profile had materially changed. This is inconsistent with SDNY's rationale in rejecting the SEC's argument of an "unacceptably boilerplate and generic" risk disclosure. As the dissent's detailed chart shows, SDNY found similar language was not generic because it (1) "[d]isclosed specific risks the company faced given its business model"; (2) "[w]arned about the increasing frequency of attacks"; (3) "[w]arned that the company might prove unable to anticipate, prevent, or detect attacks"; and (4) "[a]lerted investors to the potential for a security breach to have very damaging consequences to the company." Yet again, the SEC ignored SDNY's recent teachings.

Issuer 4

Finally, the SEC faulted Issuer 4 for not updating its risk factor from hypothetical after the cyberattack occurred. The dissent acknowledged that "to the extent that an event *has* occurred and *has* materially affected the company, it is generally required to be disclosed in another part of a filing ...." (emphasis in original). However, the SEC's materiality analysis still fell short. As the dissent explained, "not every [cybersecurity] incident is material," and the SEC peculiarly failed to explain materiality findings, including the impact of a hindsight investigation. In doing so, the SEC disregarded SDNY's recent reasoning which repeatedly chastised that it cannot rely on hindsight and speculation to argue whether disclosures are materially misleading or otherwise require correction.

Takeaways

The SEC's aggressive approach here further muddies the waters for companies trying in good faith to determine whether, when, and what to disclose in compliance with the hotly contested 2023 Cybersecurity Rule. That Rule requires disclosure of cybersecurity incidents within four business days of a company's materiality determination. Specifically, companies must now disclose "the material aspects of the nature, scope, and timing" of material cybersecurity incidents in Item 1.05 of Form 8-K. In adopting the Rule, the SEC acknowledged that immaterial disclosures about cybersecurity incidents can "divert investor attention" causing "mispricing of securities." The SEC's sweeping enforcement, however, may produce those very results and belie its goal of preventing immaterial disclosures in a lengthy risk factor section. Given the current landscape, companies will likely reasonably fear SEC scrutiny and out of an abundance of caution include immaterial details about an incident or disclose immaterial incidents (exacerbating an existing issue) in their Item 1.05 disclosures.

As the dissent cautioned, if the SEC "does not exercise restraint, it could find a violation in every company's risk disclosure because risk factors cover a wide range of topics and are inherently a disclosure of hypothetical events." The SEC's inconsistent positions, disregard of recent federal court reasoning, and thin analyses further exacerbate this risk for companies. But one thing is clear: absent companies defending their decisions through litigation, the SEC will continue pushing the envelope on its ability to regulate a public company's cybersecurity practices. Companies and their Chief Information Security Officers should stay tuned for developments in the SEC's mercurial enforcement of its 2023 Cybersecurity Rule.