POLSINELLI

# Publications

February 26, 2025 • Updates

## Recent Developments Relating to the SEC's Cybersecurity Disclosure Requirements

The U.S. Securities and Exchange Commission (SEC) is becoming one of the federal agencies at the forefront of driving transparency, cybersecurity awareness and cyber incident reporting. As we reported in last year's publication, in 2023 the SEC implemented significant enhancements to cybersecurity-based disclosures for public companies (including new incident reporting requirements). The new incident reporting rule became effective for larger companies in December 2023 and has now been in force for an entire year. During this time, we observed the marked impact on public company decision-making while also noting the SEC's multifaceted enforcement of its more seasoned cybersecurity disclosure guidance that existed prior to 2023. This article summarizes our findings and experience over the past year guiding public companies affected by these changes.

### Overview of the 2023 Rules

The SEC's new cybersecurity disclosure rules create more prescriptive data security incident disclosure and governance disclosure requirements, as follows:

**1. Form 8-K Disclosure of Material Cybersecurity Incidents.** The SEC added a new Item 1.05 to Form 8-K that requires companies to disclose a cybersecurity incident within four business days of the date such cybersecurity incident is determined to be material. The materiality standard is the same as for other required disclosures — information is material "if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision" or if it would have "significantly altered the 'total mix' of information made available." The SEC has also encouraged voluntary disclosure of cybersecurity incidents that are not material (or for which a materiality decision has not yet been made) in other ways besides the new 8-K Item 1.05.[1]

**2. Regulation S-K Disclosure of Cybersecurity Risk Management, Strategy and Governance.** The SEC added Item 106 to Regulation S-K, which requires disclosure in a registrant's annual report on Form 10-K of: (1) the registrant's processes — if any — for assessing, identifying and managing material risks from cybersecurity threats, and whether any risks from cybersecurity threats, including risks from previous cybersecurity incidents, have materially affected (or are reasonably likely to materially affect) the

### Related People

- Eric S. Wu
- Pavel (Pasha) A. Sternberg
- Mary Ann H. Quinn

### Related Capabilities

- Privacy & Cybersecurity

registrant, and (2) the Board's oversight of such risks and management's role in assessing and managing such risks. Under this requirement, registrants should provide investors with enough information for them to understand the registrant's cybersecurity practices but need not include a level of detail that could increase the registrant's vulnerability to future cyberattacks.

Recent Disclosure Trends In the second half of 2024, a survey of approximately 80 SEC cybersecurity incident disclosures revealed some notable trends:

- Only ten of the surveyed filings reported a material cybersecurity incident under Item 1.05.
- Nearly 40 filings reported the incident was not material, showing that at least for now, public companies are following the SEC's recommendation to voluntarily disclose incidents even when they are not deemed material.[2]
- Significantly, approximately 30 filings reported a third-party/ vendor incident.

## Recent Enforcement Actions

**1. The SEC Brings an Internal Accounting Control Claim, June 18, 2024**

In June 2024, R.R. Donnelley & Sons, Co. (RRD) agreed to a $2.125 million civil penalty. The SEC charged RRD with security and disclosure failures related to a 2021 ransomware incident. The SEC found that RRD's business was so critically dependent on storing and transmitting large amounts of potentially sensitive customer data that the SEC broadly deemed the company's information technology (IT) systems and networks to constitute "assets" requiring "sufficient accounting controls" under Section 13(b)(2)(B) of the Securities Exchange Act of 1934 (Exchange Act). The SEC specifically criticized the company's handling of its internal alert process and indicated that the staff tasked with reviewing security alerts was insufficient, had ill-defined roles and responsibilities and lacked clear criteria for alert prioritization and workflows.

Two SEC commissioners published a public dissent of this settlement order, saying that including IT systems in "accounting controls" was an overreach that unfairly allowed the SEC to regulate public companies' cybersecurity practices.[3] These dissenters noted that the SEC had begun to treat the accounting controls provision of Section 13(b) (2)(B) like a "Swiss Army Statute to compel issuers to adopt policies and procedures the Commission believes prudent," but that doing so "distort[ed] a statutory provision" to "punish a company that was the victim of a cyberattack."[4] The dissent also maintained that RRD's "information technology systems and networks" do not fit the category of assets intended to be captured by Section 13(b)(2)(B).

**2. The SEC's Federal Case Against SolarWinds Corporation (SolarWinds) and Its CISO Is Largely Dismissed, July 18, 2024**

The SEC filed a complaint in the Southern District of New York (SDNY) on October 30, 2023, against SolarWinds and its chief information security officer (CISO), Timothy Brown, with claims arising from disclosures the company made about its cybersecurity practices and the massive cyberattack the company suffered in 2020. The filing of the case itself marked a new era in the SEC's enforcement of cybersecurity disclosure practices. The SEC alleged SolarWinds committed securities fraud, made materially misleading disclosures, had ineffective internal accounting controls and had ineffective disclosure controls. Notably, this was the first time the SEC brought to federal court its claim for ineffective accounting controls based on cybersecurity controls such as password and VPN protocols.

On July 18, 2024, the SDNY dismissed most of the SEC's claims against SolarWinds and its CISO.[5] The SDNY emphasized that "perspective and context are critical" and did not find any material misstatements in SolarWinds' SEC filings (but did permit a claim related to SolarWinds' website disclosure).[6] The SDNY also soundly dismissed the SEC's accounting controls claim, finding that Section 13(b)(2)(B) of the Exchange Act was clearly meant to cover only financial accounting controls, not cybersecurity.[7] As a result, the decision may shift the SEC's enforcement approach going forward, in and out of federal court.

**3. The SEC Settles With Four Additional Companies for SolarWinds Disclosures, October 22, 2024**

On October 22, 2024, the SEC settled with four current or former publicly traded companies for disseminating materially misleading disclosures regarding cybersecurity risks and incidents. Unlike the SolarWinds complaint, these four settlements did not involve any accounting controls claims. Each of these four cases arose from an investigation of companies impacted by the 2020 cyberattack on SolarWinds. The SEC alleged that each of the four companies violated Section 13(a) of the Exchange Act, as amended, as well as the respective rules promulgated thereunder that require public companies to file annual, quarterly and current reports in conformity with the SEC's rules and regulations. The SEC alleged that each of the four companies learned in either 2020 or 2021 that the perpetrator of the SolarWinds attack had also infiltrated their own systems, but in their respective 2021 and/or 2022 disclosures, each company negligently minimized the cybersecurity incident. The SEC found this particularly concerning because the SolarWinds incident compromised each of the four companies' core business functions — enterprise IT services. The companies agreed to settle the SEC's charges as follows:

- Company A agreed to a **$990,000 civil penalty**. In multiple Forms 8-K filed in 2021, Company A minimized the severity of the attack on it by, among other things, failing to disclose the quantity of encrypted credentials accessed by the threat actor.
- Company B agreed to a **$1 million civil penalty**. Company B disclosed in a Form 10-Q filed in February 2021 that the threat actor had accessed a limited number of email messages; in reality, Company B was already aware the threat actor accessed over 100 files in its cloud file-sharing environment.
- Company C agreed to a **$995,000 civil penalty**. Even though Company C was aware of the intrusion, it described cyber intrusions and related risks in a generic fashion in its Annual Reports on Form 20-F filed in both 2021 and 2022.
- Company D agreed to a **$4 million civil penalty**. Company D described its risks from hypothetical future cybersecurity events in its Annual Reports on Form 10-K filed in both 2021 and 2022, even though it was aware it had already experienced two intrusions related to SolarWinds. In addition, the SEC charged Company D with violations relating to disclosure controls and procedures, resulting in such materially misleading disclosures.

While the SEC's 2023 disclosure rules were not in effect at the time of these four companies' alleged violations, these settlements demonstrate that the SEC has been increasingly aware of and focused on enforcing sufficient and appropriate cybersecurity disclosures.

## Where Might the SEC Be Trending?

The SEC Staff has reiterated across multiple forums its position that, although public companies may be victims of cyberattacks, they may not in turn harm their shareholders or the investing public by issuing misleading disclosures about cybersecurity incidents,

controls, or overall risk. Moreover, it is clear that the SEC has increased its cybersecurity vigilance in recent years. In its 2018 Commission Statement and Guidance on Public Company Cybersecurity Disclosure (SEC Release Nos. 33-10459; 34-82746), the SEC's interpretive guidance specified that ". . . if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident may occur. . . . Instead, the company may need to discuss the occurrence of that cybersecurity incident and its consequences. . . ." The SEC's 2023 rulemaking and recent enforcement actions illustrate its continued focus on public companies disclosing cybersecurity incidents as well as accurately and specifically reporting cybersecurity risks. In particular, it is quite possible that the SEC's recent trend of scrutinizing cybersecurity disclosures may extend to the Form 8-K Item 1.05 requirement to disclose a material cybersecurity incident within four business days of a materiality determination. As such, public companies should review their disclosure controls and procedures to confirm their effectiveness in enabling compliance with the SEC's cybersecurity disclosure rules in connection with future cybersecurity incidents that may impact them directly or indirectly.

[1] "Disclosure of Cybersecurity Incidents Determined to Be Material and Other Cybersecurity Incidents" (May 21, 2024), https://www.sec.gov/newsroom/whats-new/gerding-cybersecurity-incidents-05212024

[2] We believe that some of these voluntary filings are being made out of an abundance of caution while practitioners become more experienced with the Item 1.05 materiality determination and, at least in part, to avoid allegations that a material incident was not timely reported.

[3] Commissioners Hester M. Peirce and Mark T. Uyeda, "Statement on R.R. Donnelley & Sons, Co." (June 18, 2024), https://www.sec.gov/newsroom/speeches-statements/peirceuyeda-statement-rr-donnelley-061824

[4] Id.

[5] Sec. & Exch. Comm'n v. SolarWinds Corp., No. 23 CIV. 9518 (PAE), 2024 WL 3461952 (S.D.N.Y. July 18, 2024).

[6] Id. at *44.

[7] Id. at *48-52.