WILMERHALE

Making the Connection – What Do Recent SEC Enforcement Actions Mean for Cyber Controls?

AUGUST 12, 2024

On July 18, 2024, the U.S. District Court for the Southern District of New York dismissed most of the claims brought by the Securities and Exchange Commission (the "Commission") against SolarWinds Corp. ("SolarWinds") and its Chief Information Security Officer ("CISO") in *SEC v. SolarWinds Corp. et al.* in connection with the SUNBURST attack.[1] Among other things, the decision provides important perspective to the debate regarding whether controls associated with cybersecurity matters are covered by the internal accounting controls provisions of Section 13(b)(2)(B) of the Securities Exchange Act of 1934, as amended (the "Exchange Act"). The court's dismissal in *SolarWinds* follows in sharp contrast to the Commission's June 18, 2024 settlement with R.R. Donnelley & Sons Company ("RRD") relating to cybersecurity incidents, including violations of Section 13(b)(2)(B) with regard to internal accounting controls, and Exchange Act Rule 13a-15(a) with regard to disclosure controls and procedures ("DCP").[2]

Not all of the SEC's claims against SolarWinds and its CISO were dismissed. Some limited claims were allowed to proceed, including the claims of securities fraud related to SolarWinds' Security Statement, which included statements related to the strength of SolarWinds' password protections and access controls. The court found that, in the context of the motion to dismiss where the assertions in the pleadings were taken as true, SolarWinds' statements in the Security Statement would be "materially misleading by a wide margin" as opposed to mere "puffery."

This alert explores these recent developments, beginning with a refresher on the elements of DCP, internal accounting controls, and internal control over financial reporting ("ICFR"), analyzes those

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

[2] Press Release, U.S. Sec. Exch. Comm'n, *SEC Charges R.R. Donnelley & Sons Co. with Cybersecurity-Related Controls Violations* (June 18, 2024), https://www.sec.gov/newsroom/press-releases/2024-75.

requirements in light of recent Commission enforcement and judicial actions, and concludes with some practical considerations for issuers.

Background

In 1977, Congress enacted the Foreign Corrupt Practices Act (the "FCPA") and added Section 13(b)(2)(B) to the Exchange Act, which requires issuers to maintain necessary precautions, known as internal accounting controls, to ensure the reliability and accuracy of financial records. Section 13(b)(2)(B) codified auditing standards then set forth in American Institute of Certified Public Accountants Statement on Auditing Standards No. 1. These provisions fundamentally sought to deter the inaccurate accounting of transactions intended to conceal corporate bribery.

Twenty-five years later, Congress enacted the Sarbanes-Oxley Act of 2002 ("SOX") following a number of corporate misdeeds, which sought to protect investors by improving the accuracy and reliability of corporate disclosures. SOX Section 302 tasked the Commission with promulgating requirements that public company principal executive officers and principal financial officers certify each annual and quarterly report, making several representations within those certifications, including as to responsibility for designing and evaluating the effectiveness of internal controls. Similarly, SOX Section 404 tasked the Commission with promulgating rules requiring an annual assessment of a company's internal control structure.

In response, the Commission promulgated Exchange Act Rule 13a-15 in late 2002, which requires certain officers to establish, maintain and evaluate the effectiveness of DCP.[3] At that time, DCP was a newly-defined term reflecting the concept of controls and procedures related to disclosure embodied in Section 302(a)(4) of SOX. In 2003, the Commission amended Rule 13a-15 to implement Section 404 of SOX, adding to the rule the requirement that issuers maintain and evaluate ICFR and that certain issuers obtain an annual attestation report on ICFR from an independent registered public accounting firm.[4] Similar to DCP, ICFR was a newly-defined term at the time. In the adopting release, the Commission noted the evolution of the meaning of "internal controls" beginning with the groundwork laid by the FCPA and subsequent confusion over its meaning. Some commenters urged the Commission "to adopt a considerably broader definition of internal control that would focus not only on internal control over financial reporting, but also on internal control objectives associated with enterprise risk management and corporate governance." The Commission rejected that proposal, articulating the following rationales in the adopting release:

---

[3] Certification of Disclosure in Companies' Quarterly and Annual Reports, Release No. 33-8124 (Aug. 29, 2002), https://www.sec.gov/rules-regulations/2002/08/certification-disclosure-companies-quarterly-annual-reports.

[4] Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, Release No. 33-8238 (June 5, 2003), https://www.sec.gov/rules-regulations/2003/03/managements-report-internal-control-over-financial-reporting-certification-disclosure-exchange-act.

- Section 404 of SOX focuses on the element of internal control that relates to financial reporting;
- even the more limited definition proposed by the Commission was expected to impose "substantial reporting and cost burdens on companies"; and
- independent accountants traditionally have not had responsibility to review and test, or attest to management's assessment of, internal controls that exist outside the boundaries of financial reporting.

Taking those considerations into account, including confusion over the terminology to be used, the Commission adopted the term "internal control over financial reporting," and noted that its final ICFR definition "is consistent with the description of internal accounting controls in Exchange Act Section 13(b)(2)(B)."[5]

Though the definitions of "internal accounting controls" from the FCPA and "ICFR" from SOX are intended to be "consistent," there are indeed definitional differences, with ICFR being more narrowly defined. With respect to applicable requirements, internal accounting controls speaks to "reasonable assurances" that "access to assets is permitted only in accordance with management's general or specific authorization." The corresponding provision in the ICFR definition includes a materiality qualifier and more directly focuses on the relationship to the financial statements, as it speaks to "reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer's assets that could have a material effect on the financial statements."

For purposes of comparative reference, the definitions of internal accounting controls, DCP and ICFR can be summarized, in relevant part, as follows (**emphasis added**):

[5] The adopting release also acknowledged that the term "does not encompass the elements of the [Committee of Sponsoring Organizations ("COSO") of the Treadway Commission] Report definition that relate to effectiveness and efficiency of a company's operations and a company's compliance with applicable laws and regulations, with the exception of compliance with the applicable laws and regulations directly related to the preparation of financial statements, such as the Commission's financial reporting requirements." The COSO framework was established in 1992, led by Executive Vice President and General Counsel James Treadway, Jr., and is a system used to establish internal controls to provide reasonable assurance that the organization is operating ethically, transparently and in accordance with industry standards. The COSO framework goes beyond financial reporting and defined internal control as "a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives" in three categories, effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations. Public companies commonly map their SOX controls against the COSO framework to evaluate their control environment.

Internal Accounting Controls Section 13(b)(2)(B)	Disclosure Controls and Procedures Rule 13a-15(e)	Internal Control Over Financial Reporting Rule 13a-15(f)
A system of internal accounting controls sufficient to provide reasonable assurances that: (i) transactions are executed in accordance with management's general or specific authorization; (ii) transactions are recorded as necessary (I) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and (II) to maintain accountability for assets; (iii) **access to assets is permitted only in accordance with management's general or specific authorization**; and (iv) the recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.	**Controls and other procedures designed to ensure that information** required to be disclosed in public reports **is recorded, processed, summarized and reported** within the time periods specified by the Commission's rules and forms, including the accumulation **and communication of such information to management as appropriate to allow timely decisions regarding required disclosure.**	A process to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that: (i) pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer; (ii) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the issuer are being made only in accordance with authorizations of management and directors of the issuer; and (iii) **provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer's assets that could have a material effect on the financial statements.**

Commission Perspectives on Section 13(b)(2)(B) Pre-SolarWinds

The Commission's recent actions leading up to the SolarWinds decision had made clear that it intended to enforce an expansive interpretation of the contours of the internal accounting controls requirements under Section 13(b)(2)(B), such that having ineffective cybersecurity controls could lead to violations of the requirement to maintain sufficient internal accounting controls. Whether the court's decision in SolarWinds changes that going forward remains to be seen.

In the RRD enforcement action, the Commission found that between November 29, 2021 and December 23, 2021, RRD experienced a ransomware network intrusion.[6] RRD's internal intrusion detection system issued at least 23 alerts during this period, which were visible to RRD staff and its third-party managed security services provider (the "MSSP"). The alerts were reviewed in the first instance by the MSSP, which escalated three alerts to RRD, along with its related analysis. RRD reviewed the escalated alerts but, in partial reliance on the MSSP's analysis, did not take the infected instances off the network and did not conduct its own investigation of the activity or otherwise take steps to prevent further compromise. RRD began actively responding to the attack on December 23, 2021, after a company with shared access to RRD's network alerted RRD about potential anomalous internet activity emanating from RRD's network. After this alert, RRD's security personnel conducted a rapid and extensive response operation, including shutting down servers and notifying clients and federal and state agencies. Beginning on December 27, 2021, RRD issued public statements, including in Commission filings, regarding the intrusion. RRD agreed to pay approximately $2.1 million to settle the charges.

In the Commission's announcement related to the RRD settlement, Jorge G. Tenreiro, Acting Chief of the Crypto Assets and Cyber Unit of the Commission, stated:

> The Commission instituted this enforcement action because **RRD's controls for elevating cybersecurity incidents to its management and protecting company assets from cyberattacks were insufficient.** (**emphasis added**)

This interpretation of Section 13(b)(2)(B)(iii) (i.e., that the system of internal accounting controls failed to safeguard access to company assets) supports the view held by some that cybersecurity controls generally are a subset of internal accounting controls and potentially within scope for the assessment of ICFR.

However, two of the five Commissioners, Hester M. Peirce and Mark Y. Uyeda, issued a strong dissent in opposition to the action against RRD,[7] arguing that **the Commission** is relying on internal accounting control provisions "to compel issuers to adopt policies and procedures the

---

[6] According to the Order, the threat actor was able to utilize deceptive hacking techniques to install encryption software on certain RRD computers (mostly virtual machines) and exfiltrated 70 Gigabytes of data, including data belonging to 29 of RRD's 22,000 clients, some of which contained personal identification and financial information. RRD's investigation uncovered no evidence that the threat actor accessed RRD's financial systems and corporate financial and accounting data.

[7] Statement of Commissioners Hester M. Pierce and Mark T. Uyeda, U.S. Sec. Exch. Comm'n, *Hey, look, there's a hoof cleaner! Statement on R.R. Donnelley & Sons, Co.*, Commissioners Hester M. Peirce and Mark T. Uyeda (June 18, 2024), https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-rr-donnelley-061824. Commissioner Peirce and former Commissioner Elad L. Roisman and Commissioners Peirce and Uyeda issued similar dissenting statements in enforcement actions related to buyback programs against Andeavor LLC in 2020 and Charter Communications, Inc. in 2023, respectively, arguing in each that the Commission inappropriately interpreted Section 13(b)(2)(B) to cover non-accounting related internal controls.

Commission believes prudent" and "breaks new ground with its **expansive interpretation** of what constitutes an asset under Section 13(b)(2)(B)(iii)." (**emphasis added**)

The dissenting statement focuses on the origins of Section 13(b)(2)(B) discussed above. Historically, the Commission has used the provision to enforce accounting controls violations that allowed unauthorized access to a company's financial or payment systems. Looking to the auditing standards that Section 13(b)(2)(B) was intended to codify, the dissenting statement points out that the auditing literature distinguishes between "administrative controls" and "accounting controls," with the latter being limited to the plan of organization and the procedures and records "that are concerned with the safeguarding of assets and the reliability of financial records."[8] Administrative controls, by contrast, are broader. As such, the dissenting statement argues that computer systems do not constitute an asset of the type covered by Section 13(b)(2)(B)'s internal accounting controls provisions, as computer systems are not the subject of corporate transactions and do not have any of the essential characteristics necessary to qualify as such – rather, the controls associated with cybersecurity matters are more appropriately categorized as administrative controls.

For additional context, the Commission has also relied on Section 13(b)(2)(B) in recent years to bring other enforcement actions in areas outside of cyber controls that have not traditionally been considered to fall within internal accounting controls.[9]

SolarWinds Decision

On July 18, 2024, Judge Engelmayer ruled on a motion to dismiss in the ongoing dispute between the Commission and SolarWinds and its current CISO, Timothy Brown (who was serving as SolarWinds' chief security officer at the time of the relevant cyber incidents). The Commission's action stemmed from a 2020 hack of SolarWinds by Russian threat actors. The Commission had alleged that between October 2018 and January 12, 2021, SolarWinds defrauded its investors and customers by concealing SolarWinds' poor cybersecurity practices and its increasing cybersecurity risks.

The court dismissed the majority of the Commission's claims, including claims against SolarWinds for failing to maintain appropriate internal accounting controls and proper DCP, explaining that, with regard to the latter, SolarWinds maintained a sufficient DCP system, as it was designed to ensure that material cybersecurity information was timely communicated to executives responsible for public disclosures and there was, at most, a showing that errors in the system occurred rather than

---

[8] For an expanded analysis of this distinction, see Commissioner Peirce's and former Commissioner Roisman's dissenting statement in the Andeavor LLC enforcement action in 2020, *available at* https://www.sec.gov/newsroom/speeches-statements/peirce-roisman-andeavor-2020-11-13.

[9] *See, e.g.*, In the Matter of Charter Communications, Inc., Release No. 34-98923 (Nov. 14, 2023), https://www.sec.gov/files/litigation/admin/2023/34-98923.pdf; In the Matter of Andeavor LLC, Release No. 34-90208 (Oct. 15, 2020), https://www.sec.gov/files/litigation/admin/2020/34-90208.pdf.

deficiencies in the construction of the system that would support a DCP violation. With respect to internal accounting controls claims under Section 13(b)(2)(B)(iii), the court's opinion states:

> The [Amended Complaint ("AC")] alleges that SolarWinds' cybersecurity deficiencies are actionable under Section 13(b)(2)(B)(iii) because (1) the company's source code, databases, and products were its most vital assets, but (2) as a result of its poor access controls, weak internal password policies, and VPN security gaps, the company failed to limit access to these 'only in accordance with management's general or specific authorization,' enabling access by external attackers. AC 320-24. Solar Winds counters that although the Section 13(b)(2)(B) term gives the SEC authority to regulate an issuer's "system of internal accounting controls," that term, as a matter of statutory construction, cannot reasonably be interpreted to cover a company's cybersecurity controls such as its password and VPN protocols. **SolarWinds is clearly correct**. (**emphasis added**)[10]

The court's opinion includes an extensive history of the internal accounting controls provision and analysis of precedent decisions interpreting Section 13(b)(2)(B). In countering the Commission's argument that it needs authority to regulate cybersecurity controls under Section 13(b)(2)(B), the court states:

> By its terms, Section 13(b)(2)(B) does not govern every internal system a public company uses to guard against unauthorized access to its assets, but only those qualifying as "internal accounting" controls. The SEC's rationale, under which the statute must be construed to broadly cover all systems public companies use to safeguard their valuable assets, would have sweeping ramifications. It could empower the agency to regulate background checks used in hiring nighttime security guards, the selection of padlocks for storage sheds, safety measures at water parks on whose reliability the asset of customer goodwill depended, and the lengths and configurations of passwords required to access company computers. That construction-and those outcomes-cannot be squared with the statutory text.

It is unclear whether the Commission will appeal the court's dismissal, and it is possible that other courts may rule differently if presented with similar Section 13(b)(2)(B)(iii) issues. For example, in its pleadings on the motion to dismiss, the Commission argued that SEC v. Cavco Industries Inc., No. 21 Civ. 01507 (PHX) (SRB), 2022 WL 1491279, at *4 (D. Ariz. Jan. 25, 2022) supports its interpretation of Section 13(b)(2)(B)(iii). That case found that the failure by Cavco Industries Inc. ("Cavco") to follow its insider trading policy constituted an internal accounting control failure where the policy required Cavco to invest its surplus assets in low-risk cash equivalents, which was not followed when Cavco's CEO created an "end-run around the process," resulting in investment of surplus cash in a publicly traded company without the requisite review or approval by the chief

[10] *Sec. Exch. Comm'n v. SolarWinds Corp.*, 23 Civ. 9518 (PAE), 2024 WL 3461952, at *48 (S.D.N.Y. July 18, 2024).

financial officer or board of directors. While Judge Engelmayer acknowledged the Commission's attempt to apply the same logic to SolarWinds, he differentiated Cavco because it directly related to ensuring the integrity of the company's financial transactions, stating "[t]he decision cannot responsibly be read as supporting the Commission's argument here that Section 13(b)(2)(B) reaches cybersecurity controls."

While beyond the scope of discussion about internal accounting controls and DCP, it is worth noting that with respect to cybersecurity-related disclosures, although the court dismissed the majority of the Commission's securities fraud claims, it allowed claims regarding the SolarWinds' Security Statement—which appeared on SolarWinds' website and described its cybersecurity practices in detail—to move forward against both SolarWinds and Brown. However, the court dismissed all claims based on the SolarWinds' risk disclosures because, among other things, the disclosures were not misleading and were adequately specific, and because the company had no duty to update its risk disclosures after certain incidents occurred, as well as the claims of securities fraud with respect to statements made via press releases, blog posts, and podcasts, reasoning that these statements generally were "non-actionable corporate puffery" on which a reasonable investor would not reasonably rely.

Specifically, the Commission had argued that the Security Statement contained misstatements about SolarWinds' access controls, password protections, compliance with the National Institute of Standards and Technology Cybersecurity Framework, network monitoring, and compliance with the security development lifecycle. In response, SolarWinds argued that (i) the Security Statement was directed at customers, not investors, and (ii) each of the representations in the Security Statement should be evaluated in isolation. The court found that the Commission's amended complaint adequately pled that the Security Statement contained misrepresentations with regard to at least access controls and password protections. Citing a variety of cases, the court states that "[i]t is well established that false statements on public websites can sustain securities fraud liability," noting that because "the Statement was on SolarWinds' public website and accessible to all, including investors," it was therefore "unavoidably" part of the "'total mix of information' that SolarWinds furnished the investing public." The court also rejected defendants' arguments that the representations should be viewed in isolation and that if any representation, individually, is not found materially misleading, it should be put aside in the court's motion to dismiss analysis.

Impact on Issuers

While the RRD settlement put public companies on notice that the Commission, including its Division of Enforcement, may regard a successful cybersecurity intrusion as indicative of an internal accounting controls and/or DCP failure, the holding in *SolarWinds* may temper the Commission's approach to cybersecurity enforcement and impact the way the Commission frames actions related to cybersecurity incidents.

That said, we expect that the Commission will continue to scrutinize significant cybersecurity incidents and related responses, including, among other things, incident and response policies and adherence thereto, internal communications among cybersecurity personnel, responsibilities of cybersecurity team members, involvement and oversight of third parties and public disclosure of all forms. It is perhaps notable that neither the Commission's Form 8-K Item 1.05 cybersecurity disclosure requirement nor the recent cybersecurity rule amendments to Regulation S-P that apply to brokers, dealers, investment companies and others were in effect at the time of the events that underlie the *SolarWinds* case.

Furthermore, we expect that the Commission will continue to focus on public statements made by companies in their filings and on their websites, especially where such statements pertain to security controls, compliance with security frameworks such as National Institute of Standards and Technology Cybersecurity Framework or Cybersecurity Maturity Model Certification, password complexity and more.

Relatedly, even if cyber controls are not squarely within the purview of internal accounting controls or ICFR, it is possible that auditors could nevertheless ask to review cyber controls and incident response plans as part of internal control assessments more broadly and could expect internal control teams to be involved in assessing the effectiveness of DCP around Form 8-K, Item 1.05 and Form 10-K, Item 1C disclosures.

Irrespective of the potential clarification around internal accounting controls, we also expect increased pressure on public companies from stakeholders to bolster internal controls and procedures more generally with respect to incident and response policies, security operations centers, security incident information and event management and technical and executive tabletops. There could also be an expectation that companies incorporate additional layers of oversight, including audits to (i) independently assess the design and operating effectiveness of controls, (ii) assess appropriate involvement of cybersecurity specialists to test newly designed and implemented controls and (iii) evaluate management's ability to promptly react to cybersecurity events, escalate responses and provide appropriate disclosures.

As a housekeeping matter, issuers may also be well advised to take a fresh look at their public statements about their cybersecurity practices, including those outside filings with the Commission, as well as related policies for spokespeople, as public statements are viewed holistically and not in isolation.[11] These reviews should consider the accuracy of these statements, including any potential stakeholder interpretations, in order to identify and remedy any materially misleading misstatements or omissions. Attention should also be given to issuers' cyber-related risk factors and other disclosures that are intended to offer protection under the federal securities laws.

[11] As the court held in *SolarWinds*, public statements are intended for investors as well as consumers, and "false statements on public websites can sustain securities fraud liability."

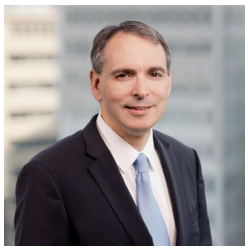
Contributors

Meredith B. Cross
PARTNER

meredith.cross@wilmerhale.com
+1 212 295 6644

Stephanie Avakian
PARTNER

stephanie.avakian@wilmerhale.com
+1 202 663 6471



Benjamin A. Powell
PARTNER

benjamin.powell@wilmerhale.com
+1 202 663 6770

Joseph K. Brenner
SENIOR COUNSEL

joe.brenner@wilmerhale.com
+1 202 663 6158

C. Alex Bahn
PARTNER

alex.bahn@wilmerhale.com
+1 202 663 6198

Lillian Brown
PARTNER

lillian.brown@wilmerhale.com
+1 202 663 6743

Jenna El-Fakih
SENIOR ASSOCIATE

jenna.el-fakih@wilmerhale.com
+1 213 443 5416

Amy Gopinathan
SENIOR ASSOCIATE

amy.gopinathan@wilmerhale.com
+1 202 663 6761

Liz Graffeo
COUNSEL

liz.graffeo@wilmerhale.com
+1 720 598 3481

Tamar Y. Pinto
ASSOCIATE

tamar.pinto@wilmerhale.com
+1 617 526 6151

Alan J. Wilson
PARTNER

alan.wilson@wilmerhale.com
+1 202 663 6474

Jonathan Wolfman
PARTNER

jonathan.wolfman@wilmerhale.com
+1 617 526 6833