View on our website.

GIBSON DUNN

Securities Enforcement Update July 25, 2024

Dismissal of Much of SEC's SolarWinds Complaint Has Potentially Broad Implications for SEC Cybersecurity Enforcement

The SEC's action against SolarWinds related to a highly publicized compromise of the company in 2020 that was attributed to Russia's Foreign Intelligence Service who had inserted malware into a routine SolarWinds software update.

On July 18, 2024, the U.S. District Court for the Southern District of New York largely granted SolarWinds' motion to dismiss and dismissed most of the SEC's claims against the company and its former Chief Information Security Officer (CISO).[1] The SEC's action against SolarWinds related to a highly publicized compromise of the company in 2020 that was attributed to Russia's Foreign Intelligence Service (SVR) who had inserted malware into a routine SolarWinds software update. Although thousands of SolarWinds customers received the software update, the SVR used the compromise to access the environments of certain SolarWinds customers in the government and private sector (the "SUNBURST" incident).

The court dismissed most of the claims advanced by the SEC relating to its disclosures, including SolarWinds' Form 8-K filings, but did sustain claims against SolarWinds and its CISO alleging that a "Security Statement" posted on its website in 2017 may have been false or misleading.

The decision is noteworthy for several reasons:

- The court dismissed the SEC's claim that cybersecurity-related deficiencies were actionable under its rules relating to internal accounting and disclosure controls. The

court concluded that the claim was "ill-pled" because "cybersecurity controls are not—and could not have been expected to be—part of the apparatus necessary to the production of accurate" financial reports, noting that "[a]s a matter of statutory construction, [the SEC's] reading is not tenable."[2] This is noteworthy because the SEC just last month entered into a settlement in cybersecurity-related case under the theory that internal accounting controls-related regulations could encompass traditional IT assets that were unrelated to financial systems or financial/accounting data.[3] The Solar Winds decision will likely impact how the SEC thinks about its broad use of accounting controls as a basis to charge a violation related to a cyber incident.

- The court's decision makes clear that more than isolated disclosure failures are required to put the adequacy of a company's disclosure controls and procedures in issue. The decision also leaves open the question of whether, in a close case where the SEC may be inclined to allege fraud, the SEC will continue to be willing to enter into a settlement on the basis of a disclosure controls and procedures violation if the company was willing to do so in order to avoid a fraud charge, as has been their practice to date.
- While the decision is an encouraging sign that the SEC's aggressive attempts to hold CISOs individually liable for company conduct will be evaluated on the factual record and the law, the decision did not dismiss all claims against the CISO (allowing the claims based on allegations of contemporaneous knowledge of falsity of public statements to go forward), and companies and CISOs should remain vigilant in responding to cybersecurity incidents and ensuring the accuracy of all public statements that are made about cybersecurity.

Background

On October 30, 2023, the SEC filed a complaint against SolarWinds and its former CISO alleging that they made materially false and misleading statements and omissions on the company website, blog posts, press releases, Form S-1, and quarterly and annual SEC reports *prior* to the incident and did the same in two reports on Form 8-K in which the company disclosed the incident.[4] The SEC also conducted an investigation regarding the SUNBURST incident and issued a letter to certain companies because the SEC staff believed those entities were impacted by the SolarWinds compromise and requested that they provide information to the staff on a voluntary basis.[5] In February 2024, the SEC filed an amended complaint including factual details to support its allegations that SolarWinds and its CISO were aware of the company's weak security practices yet made contrary statements about its strength in SolarWinds' Security Statement.[6] The Defendants filed a motion to dismiss in March 22, 2024,[7] and the court issued its order on July 18, 2024.

July 18, 2024 Order

The court largely granted Defendants' motion to dismiss, sustaining only the SEC's claims alleging securities fraud based on allegations that the company made false or misleading representations in a "Security Statement" posted to SolarWinds' website. Specifically:

1. **Fraud and False and Misleading Statements**

The court dismissed most of the SEC's securities fraud claims regarding SolarWinds' statements about its strong security that it made in press releases, blog posts, podcasts and securities

filings. However, the court allowed the SEC's claims based on the Securities Statement on SolarWinds' website to proceed.[8]

The "Security Statement"

The court found that the SEC adequately pled that the Security Statement posted on SolarWinds' website contained materially misleading and false representations as to at least two of SolarWinds' cybersecurity practices: access controls and password protection policies. The court's holding was based on the allegations in the complaint that SolarWinds had made statements touting that it had strong access controls and password policies when its internal practices and discourse instead "portrayed a diametrically opposite representation for public consumption."[9] Specifically, the court found that the complaint alleged that the company's access controls had "deficiencies" that "were not only glaring—they were long-standing, well-recognized within the company, and unrectified over time," and its password policies were generally not enforced.[10] The court also found that the amended complaint "amply" alleged scienter, including that the former CISO knew of the substantial body of data that impeached the security statement's content as false and misleading.[11]

The court importantly explained that false statements on public websites can sustain securities fraud liability, as the security statement at issue appeared on SolarWinds' public website, accessible to all, including investors, and therefore was, according to the court, unavoidably part of the "total mix of information" that SolarWinds furnished to the investing public.[12] The court emphasized that for purposes of evaluating materiality, each representation should be considered collectively, rather than in isolation, as investors evaluate the whole picture.

Press Releases, Blog Posts, and Podcasts

The court dismissed the SEC's claims that SolarWinds made false and misleading statements related to the 2020 incident in press releases, blog posts, and podcasts explaining that each qualifies as non-actionable corporate puffery, "too general to cause a reasonable investor to rely upon them."[13] As the court noted, while public statements, such as the website security statement, can serve as the basis for a material misstatement when they contain a degree of specificity, general statements by an issuer about the strength of their cybersecurity program were not sufficient to support a fraud violation.

Pre-Incident Public Filings

The court dismissed each of the SEC's claims that SolarWinds' cybersecurity risk disclosures in its SEC filings did not accurately reflect the risks that the company faced. The court found that, viewed in totality, the risk disclosures sufficiently alerted the investing public of the types and nature of the cybersecurity risks SolarWinds faced and the consequences these could present for the company's financial health and future.[14] The court also held that, on the facts pled, SolarWinds was not required to amend its cybersecurity risk disclosures for certain cyber incidents as the company's cybersecurity risk disclosures already warned investors of the risks "in sobering terms."[15]

In the court's view, issuers are not required to disclose cybersecurity risks with "maximum specificity," as, according to the court, spelling out a cybersecurity risk may backfire in various ways, such as by arming malevolent actors with information to exploit or by misleading investors as other disclosures might be disclosed with relatively less specificity.[16]

Post-incident Form 8-K

The court found that the SEC did not adequately plead that the post-incident Form 8-K was materially false or misleading, as the disclosure fairly captured the known facts and disclosed what was required for reasonable investors. The court also acknowledged that the impact on stock prices indicated that the market "got the message" (noting SolarWinds' share prices dropped more than 16% the day of the announcement, and another 8% the next day),[17] and emphasized that SolarWinds published the disclosure just two days after discovering the compromise, when it was still in the early phases of its investigation and had a limited understanding of the attack.

2. **Internal Accounting Controls**

The court found that the SEC's attempt to bring a claim under Section 13(b)(2)(B) of the Exchange Act (relating to internal accounting controls) was unsupported by legislative intent, as the surrounding terms that Congress used when drafting Section 13(b)(2)(B), which refer to "transactions," "preparation of financial statements," "generally accepted accounting principles," and "books and records," are uniformly consistent with financial accounting. [18] The court's deep skepticism of the claim that Congress intended to confer the SEC with such authority is reflected in the analogy that doing so would be tantamount to "hid[ing] elephants in mouseholes."[19] The court also found that the few courts that interpreted the term "internal accounting controls" as used in this section "have consistently construed it to address financial accounting."[20] In this respect, the court's conclusion is consistent with the views expressed in several dissents by Commissioners in other settled enforcement actions in which the SEC has used the internal accounting controls provision to impose liability for non-financial related conduct.[21]

3. **Disclosure Controls and Procedures**

The court sided with SolarWinds in rejecting the SEC's claims that the company failed to maintain and adhere to appropriate disclosure controls for cybersecurity incidents. The court was unwilling to accept the SEC's argument that one-off issues—even if the company misapplied its existing disclosure controls in considering cybersecurity incidents—gave rise to a claim that the company failed to maintain such controls. Importantly, this case relates to conduct prior to the adoption of the SEC's 2023 cybersecurity rules, which have made it even more important for companies to maintain appropriate controls.

The court acknowledged that SolarWinds had misclassified the severity level of two incidents under its Incident Response Plan (IRP) and failed to elevate a vulnerability to the CEO and CTO for disclosure.[22] However, the court found that these instances—without more—did not support a claim that SolarWinds maintained ineffective disclosure controls.

The SEC did not plead deficiency in the "construction" of SolarWinds' IRP, nor did it allege routine misclassification of incidents or frequent errors as a result of applying that framework.[23] The court implied that disclosure controls do not have to be perfect—they should provide *reasonable assurance* that information is being collected for disclosure consideration. The court thus found that the one-off issues identified by the SEC in applying the IRP and associated cybersecurity disclosure controls were not, without more, sufficient to "plausibly impugn [a] company's disclosure controls systems."[24]

Key Takeaways

Internal Accounting Controls.

- Notably, on June 18, 2024 the SEC claimed in a settlement that another company that had experienced cyber incidents violated rules relevant to internal accounting controls. The SEC alleged that the company failed to "provide reasonable assurances…that access to company assets is permitted only in accordance with management's…authorization."[25] The SEC's claims and approach in that settlement were seen as particularly aggressive as the predicate cybersecurity incident (for which the controls would be relevant) did not impact financial systems or corporate financial and accounting data. That settlement also evoked a notable dissent from two Commissioners arguing that the internal accounting controls provision did not apply to a company's overall cybersecurity program.
- The court in this case comprehensively repudiated the SEC's effort to bring an internal accounting controls violation based on Section 13(b)(2)(B) in the context of cybersecurity-related actions. The court found the SEC's position that their authority to regulate an issuer's "system of internal accounting controls" includes authority to regulate cybersecurity controls "not tenable," and unsupported by the statute, legislative intent, or precedent. [26] The court held that the statute cannot be construed to broadly cover all systems public companies use to safeguard their valuable assets and that the statute's reach is limited as it governs systems of "internal *accounting* controls."[27]
- As such, the SolarWinds decision calls into question—and may signal an end to—the SEC's recent attempts to adopt an expansive reading of its rules relating to internal accounting controls to govern cybersecurity controls—whether or not such cybersecurity controls are relevant to the production of financial reports.

Disclosure Controls and Procedures.

- The decision also calls into question the SEC's ability to rely on claims of inadequate disclosure controls and procedures in similar circumstances, given that the court found that more than a single disclosure failure is required to put the adequacy of a company's disclosure controls and procedures in issue.
- While this fact-based finding provides reassurance that good-faith, day-to-day mistakes at a company may not be actionable, it remains important to design and maintain disclosure controls that provide for appropriate escalation and consideration.

Assessing Fraud Claims Based on Public Disclosures.

- When evaluating the accuracy of public disclosures in the context of a securities fraud claim, representations are to be evaluated based on a holistic assessment, rather than each statement in isolation. The court rearticulated the long-standing view the investing public "evaluates the information available to it 'as a whole.'" Nevertheless, a securities fraud claim may be pursued where there is evidence that the company—or a CISO or other company officer—is aware of inaccuracies at the time such statements are made.

[1] Opinion and Order, *SEC v. SolarWinds Corp. and T. Brown*, 1:23-cv-09518-PAE (S.D.N.Y. July 18, 2024) (hereinafter "Order").

[2] Order at 3, 94–102.

[3] *See* Gibson Dunn Client Alert, "SEC as Cybersecurity Regulator" (June 20, 2024), available at https://www.gibsondunn.com/wp-content/uploads/2024/06/sec-as-cybersecurity-regulator.pdf?v2; R.R. Donnelley & Sons, No. 3-21969 (S.E.C. June 18, 2024) (order instituting cease and desist proceedings), available at https://www.sec.gov/files/litigation/admin/2024/34-100365.pdf.

[4] Complaint, *SEC v. SolarWinds Corp. and T. Brown*, No. 23-cv-9518 (Oct. 30, 2023), https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf.

[5] In the Matter of Certain Cybersecurity-Related Events (HO-14225) FAQs, U.S. Securities and Exchange Commission, available at https://www.sec.gov/enforce/certain-cybersecurity-related-events-faqs.

[6] Am. Compl., *SEC v. SolarWinds Corp. and T. Brown,* No. 23-cv-9518-PAE (S.D.N.Y. Feb. 20, 2024).

[7] Mem. of Law in Support of Mot. to Dismiss, *SEC v. SolarWinds Corp. and T. Brown,* No. 23-cv-9518-PAE (S.D.N.Y. Mar. 22, 2024).

[8] *See* Order at 3.

[9] Order at 54.

[10] Order at 54.

[11] Order at 61.

[12] Order at 51 (citation omitted).

[13] Order at 68 (citation omitted).

[14] Order at 71–79.

[15] Order at 75.

[16] Order at 73.

[17] Order at 90.

[18] Order at 96.

[19] Order at 100.

[20] Order at 97–98.

[21] 2023 Year-End Securities Enforcement Update - Gibson Dunn (end notes 20–22); SEC Statement, The SEC's Swiss Army Statute: Statement on Charter Communications, Inc. (Nov. 14, 2023), available at https://www.sec.gov/news/statement/peirce-uyeda-statement-charter-communications-111423#_ftn6.

[22] Order at 102–106.

[23] Order at 104.

[24] Order at 106.

[25] R.R. Donnelley & Sons, No. 3-21969 (S.E.C. June 18, 2024) (order instituting cease and desist proceedings), available at https://www.sec.gov/files/litigation/admin/2024/34-100365.pdf.

[26] Order at 96.

[27] Order at 96–97.

The following Gibson Dunn lawyers prepared this update: Mark Schonfeld, David Woodcock, Ronald Mueller, Brian Lane, Vivek Mohan, Stephenie Gosnell Handler, Sophie Rohnke, Michael Roberts, Sarah Pongrace, and Ashley Marcus.

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 Securities Enforcement, Privacy, Cybersecurity & Data Innovation, or Securities Regulation & Corporate Governance practice groups:

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)

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 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)
Brian J. Lane – Washington, D.C. (+1 202.887.3646, blane@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)