JENNER&BLOCK

# Key Takeaways from the Motion to Dismiss Ruling in *SEC v. SolarWinds et al.*

**Client Alerts**

July 24, 2024
By: Shoba Pillay, Charles D. Riely, H. Kurt von Moltke

The SEC's high-profile litigation against SolarWinds and its Chief Information Security Officer (CISO), Timothy G. Brown, reached a critical turning point on July 18, 2024, when a district court in the Southern District of New York issued a ruling granting in large part, but denying in part, the defendants' motion to dismiss. In its extensive opinion and order spanning 107 pages, the court: (1) denied the defendants' motion to dismiss with respect to securities fraud claims premised on the company's Security Statement posted on its website, permitting the SEC to continue pursuing those claims; (2) dismissed the SEC's securities fraud claims based on certain statements made by Brown in press releases, blog posts, and podcasts; (3) dismissed the SEC's securities fraud claims premised on risk factor disclosures; (4) dismissed the SEC's securities fraud claims regarding certain of the misleading disclosures made after the incident; (5) dismissed the SEC's internal accounting controls claim; and (6) dismissed the SEC's disclosure controls and procedure claim.[1]

The decision will have an important impact on how the SEC uses the securities laws to address alleged misleading company statements about cybersecurity practices, risks and incidents. This client alert discusses the important points of the ruling and key takeaways for public companies.

## Background

As we noted in our prior client alert, the SEC filed its initial complaint against SolarWinds and its CISO Brown in October 2023, alleging that the defendants misled the company's investors and customers by overstating the company's cybersecurity practices and concealing mounting cybersecurity risks between October 2018 and January 2021.[2] According to the SEC, these risks came to light after a massive cyberattack on SolarWinds and its customers, known as SUNBURST, which exploited some of the company's cybersecurity risks.[3]

The SEC's complaint focused on SolarWinds' flagship network monitoring product, Orion, which purportedly had abilities ranging from reducing network outages to improving network performance.[4] Orion was used by virtually all Fortune 500 companies and many US government agencies.[5] The SEC alleged that SolarWinds overstated the strength of its cybersecurity practices and prevention measures, and then made materially misleading statements after learning of a massive breach

regarding Orion that impacted many of its key customers.[6] The SEC also alleged that SolarWinds lacked sufficient internal accounting controls and disclosure controls, citing the company's deficient cybersecurity controls.[7]

In February 2024, after the defendants moved to dismiss the original complaint and numerous industry groups filed amicus briefs criticizing the charges, the SEC amended its complaint to detail specific practices that SolarWinds and its CISO had allegedly "touted" as part of its robust cybersecurity measures, as covered in our prior client alert. In defending its novel internal accounting controls charge, the amended complaint also detailed "[t]he cybersecurity controls at issue here were 'internal accounting controls' in that they were plans, procedures, and records of SolarWinds concerned with the safeguarding of corporate assets. Cybersecurity policies must be designed and implemented to provide shareholders with reasonable assurances that access to corporate assets—including technology assets, computer code and software for distribution to customers—are limited to authorized users, and thus support the twin goals of corporate accountability and management stewardship over corporate assets underlying Rule 13(b)(2)(B)."[8]

On May 15, 2024, the court held a hearing on the defendants' motion to dismiss, considering arguments from each side, as discussed here.

**The Court's Ruling**

In a careful ruling, the court reviewed each aspect of the SEC complaint at issue in the motion to dismiss to determine if the SEC's claims survived. In so doing, the court categorized the securities fraud allegations into two sets of disclosures: (1) disclosures made prior to the SUNBURST attack; and (2) disclosures made once the company discovered the SUNBURST attack.[9] These allegations formed the basis of the SEC's misrepresentation charges pursuant to Section 10(b) and Rule 10b-5(b) of the Securities Exchange Act of 1934 ("Exchange Act") and Section 17(a)(2) of the Securities Act of 1933 ("Securities Act"), and/or the SEC's scheme liability charges pursuant to Rules 10b-5(a) and (c) of the Exchange Act and Sections 17(a)(1) and (3) of the Securities Act.[10] The court also reviewed the SEC's claims under Section 13(b)(2)(B) of the Exchange Act and Exchange Act Rule 13a-15(a), faulting SolarWinds for deficient internal accounting and disclosure controls, respectively.[11]

As detailed below, the court largely denied the motion to dismiss with respect to pre-SUNBURST disclosures and granted the motion to dismiss with respect to post-SUNBURST disclosures.[12] The court also dismissed the claims alleging ineffective internal accounting and disclosure controls as ill-pled.[13] The narrowed case will now proceed against SolarWinds and its CISO.

1. The Court Denied the Motion to Dismiss the SEC's Securities Fraud Claims Based on Pre-SUNBURST Disclosures in the Company's Security Statement

The court focused on specific practices that SolarWinds and Brown "touted" in a Security Statement posted on the company's web site that were allegedly misleading. These practices included representations regarding the company's (1) access controls; (2) password protections; (3) compliance with the NIST framework; (4) network monitoring; and (5) compliance with the secure development lifecycle.[14] In its amended complaint, the SEC asserted that Brown approved the Security Statement, and disseminated the Security Statement to customers, including in blog posts and presentations touting SolarWinds' strong cybersecurity practices.[15]

As a general matter, the court rejected the defendants' argument that the Security Statement was intended for customers, versus investors, and therefore could not support a securities fraud charge. The court then concluded that the Security Statement contained actionable misrepresentations for "at least two" of the above-referenced practices—namely, access controls and password protection policies—as discussed below.[16]

- **Access Controls:** The court found that the SEC's amended complaint chronicled "diverse findings contradicting SolarWinds' public representations."[17] For example, the amended complaint alleged that between 2017 and 2020, SolarWinds was "freely granting administrative rights to employees and conferring access rights way beyond those necessary for employees' specific job functions," which "blatantly contradicts" representations made in the Security Statement.[18] Accordingly, the court found that the SEC adequately pled that the Security Statement "misleadingly touted SolarWinds' access controls as strong."[19]

- **Password Protections:** The court found that the SEC adequately alleged that the Security Statement "materially misrepresented to the public that SolarWinds enforced a strong password policy."[20] Specifically, the SEC alleged that a SolarWinds company product used "password" as a default password, and that the password to one of the company's servers was "solarwinds123," in contrast to the Security Statement which read "[o]ur password best practices enforce the use of complex passwords that include both alpha and numeric characters."[21]

The court ultimately determined that the SEC adequately pled that the Security Statement's "overall portrait of SolarWinds' cybersecurity" was as a whole materially misleading when considering the two misrepresentations together.[22] The court did not specifically rule on SolarWinds' alleged misrepresentations regarding the other three cybersecurity practices, though it observed at the May 2024 hearing the allegation regarding the company's compliance with the NIST framework was "not [the SEC's] strongest one."[23]

With regard to *scienter* for the Security Statement, the court noted that the CISO "was privy to internal information contradicting the Statement's representations both as to the company's access controls and compliance with the password policy" as evidenced by presentations given by the

CISO about SolarWinds' cybersecurity deficiencies.[24] While this alone would have been enough to plead *scienter*, the court further observed that because of Brown's role at the company, "the only rational inference is that he knew of actual cybersecurity incidents, tending to undermine the Security Statement's top-line message," and concluded that Brown's knowledge was attributable to SolarWinds.[25]

The court also found that allegations that Brown "promoted the Security Statement in blogposts, podcasts, and press releases touting SolarWinds' strong cybersecurity measures," were sufficient to plead scheme liability against Brown and SolarWinds.[26]

2. The Court Dismissed the SEC's Securities Fraud Claims Based on the CISO's Pre-SUNBURST Disclosures in Press Releases, Blog Posts, and Podcasts Because They Were Non-Actionable Corporate Puffery

The court dismissed securities fraud claims against the defendants based on certain statements made by Brown in press releases, blog posts, and podcasts made before the SUNBURST attack.[27] For instance, the SEC alleged that in a 2020 blog post, Brown stated that SolarWinds "places a premium on the security of its products and makes sure everything is backed by sound security processes, procedures, and standards."[28] The court described each statement as "non-actionable corporate puffery" which are statements "too general to cause a reasonable investor to rely upon them."[29]

3. The Court Dismissed the SEC's Securities Fraud Claims Regarding the Company's Pre-Sunburst Form S-1 Cybersecurity Risk Disclosure and Rejected a Duty to Update This Disclosure Post-SUNBURST

The court rejected the SEC's allegation that the company's risk factor disclosure was misleading because "it concealed the gravity of the cybersecurity risks that the SolarWinds faced."[30] While the SEC described the risk disclosure as "boilerplate," the court observed that the risk factor disclosure "set out in some detail the unique risks" to a cybersecurity company such as SolarWinds, including both generic risks and more specific risks given SolarWinds' business model.[31] The court noted that the case law did not require SolarWinds to spell out its cybersecurity risks in greater detail, or to set out in "substantially more specific terms scenarios under which its cybersecurity measures could prove inadequate."[32] As the court noted, "[s]pelling out a risk with maximal specificity may backfire in various ways[.]"[33]

With regard to the duty to update the risk factor disclosure, the court similarly rejected the SEC's arguments that SolarWinds should have updated its risk factor disclosure once it learned of unusual activity involving its Orion product.[34] The court noted that the risk factor disclosure already warned investors that "SolarWinds was not positioned to, and could not be expected to, anticipate or

prevent all such intrusions," which the court found to be a "fulsome disclosure" of cyber incidents as "regrettably, a fact of life."[35] While the SEC argued that risk disclosures are inadequate where the risk has already transpired, the court found that the allegations did not support the conclusion that SolarWinds at the time of the disclosure was aware of a cyberattack, "let alone a serious or pervasive one."[36]

The court also found that the SEC failed to adequately plead that Brown acted with *scienter* in not amending the cybersecurity disclosure, in part because the SEC did not allege that "Brown consciously or deliberately withheld information from the persons responsible for creating the risk disclosure."[37] Even if the SEC could allege a material misrepresentation in the cybersecurity risk disclosure, Brown, who did not certify the SEC filings, had an additional argument against liability under Section 10(b), which requires a defendant to have "made" the allegedly material misstatements.[38] The court noted, however, this would not bar a claim against Brown for aiding and abetting liability based on the sub-certifications he signed.[39]

4. The Court Dismissed the SEC's Securities Fraud Claims Based on Post-SUNBURST Disclosures Describing the Incident

The court dismissed the SEC's claims alleging that SolarWinds' Form 8-K disclosure was "materially misleading because it did not disclose the earlier malicious activity reports" and therefore "gave the wrong impression that SUNBURST was a purely theoretical problem."[40] The court observed that the Form 8-K disclosure was filed just two days after SolarWinds discovered the vulnerability, at an "early stage of its investigation," and was not inaccurate or misleading.[41] Instead, the court found that the "lengthy Form 8-K disclosure, read as a whole, captured the big picture: the severity of the SUNBURST attack."[42]

5. The Court Dismissed the SEC's Internal Accounting Controls Claim

The court dismissed the SEC's claim against SolarWinds for deficient internal accounting controls, reasoning that "cybersecurity controls are outside the scope of Section 13(b)(2)(B)" of the Exchange Act.[43] This case was the first time the SEC brought an accounting control claim based on a company's alleged cybersecurity failings. Numerous industry groups criticized the SEC use of the internal accounting controls provisions of the Exchange Act to charge the defendants for failing to protect company assets from cybersecurity attacks. At the hearing on the motion to dismiss, the court similarly questioned whether Section 13(b)(2)(B) applied beyond tangible, countable assets.[44] The SEC argued that adequate cybersecurity controls were necessary to provide reasonable assurances required under Section 13(b)(2)(B) that the company's assets were safeguarded from unauthorized use.[45]

The court rejected the SEC's rationale, explaining that as a matter of statutory construction, Section 13(b)(2)(B) could not be read to cover cybersecurity controls.[46] Section 13(b)(2)(B) requires issuers "to accurately report, record, and reconcile *financial* transactions and events," but does not "govern *every internal system* a public company uses to guard against unauthorized access to its assets."[47] While cybersecurity controls are "vitally important," they are not "part of the apparatus necessary to the production of accurate [financial] reports."[48] The court therefore declined to adopt the SEC's broad reading of Section 13(b)(2)(B), which "would have sweeping ramifications" that could not be squared with the statutory text.[49]

6. The Court Dismissed the SEC's Disclosure Controls and Procedures Claim

Finally, the court addressed the SEC's claim under Exchange Act Rule 13a-15(a). The SEC alleged that SolarWinds failed to maintain effective disclosure controls and procedures, because the company's Incident Response Plan ("IRP") misclassified network breaches reported by SolarWinds customers in May and October 2020, and that Brown failed to elevate a VPN vulnerability in June 2018.[50]

Although Rule 13a-15(a) requires an issuer to maintain procedures covering "a broader range of information than is covered by an issuer's internal controls related to financial reporting," the court dismissed the SEC's claim, noting that the amended complaint did not allege the company's IRP was deficient or frequently yielded errors.[51] In fact, the SEC acknowledged that SolarWinds had a system of controls in place and that the IRP was "designed to ensure that material cybersecurity information was timely communicated to executives responsible for public disclosures."[52] Rather, the Rule 13a-15(a) claim was based on an improper classification of the initial incidents as not requiring escalation to the appropriate management team members.[53] Without more, the two misclassified incidents could not support the SEC's claims for deficient disclosure controls.[54] With respect to Brown's failure to elevate the VPN issue in June 2018, the court similarly concluded that "this one lapse . . . does not, without more, plausibly impugn the company's disclosure controls systems."[55]

**Key Takeaways**

- **The *SolarWinds* ruling confirms that the SEC can bring fraud claims against a company about its cybersecurity disclosures that can withstand a motion to dismiss.** This is the first time a court has analyzed the SEC's disclosure theories in the context of cybersecurity. While the *SolarWinds* ruling dismissed the majority of the SEC's claims, the court permitted the SEC to proceed with fraud claims against both defendants premised on material misrepresentations in the company's Security Statement. Accordingly, public companies should be cognizant that cybersecurity enforcement by the SEC remains a heightened risk.

- **The *SolarWinds* ruling makes clear that the SEC can bring fraud claims against a company regarding the strength of its cybersecurity practices.** The claim that has survived is a classic SEC disclosure theory positing that an issuer's statement that it follows certain practices is materially misleading when it has reason to know it is not following them as described or is otherwise falling behind by a "wide margin." Accordingly, public companies should carefully assess any disclosures that refer to best practices to ensure that they align with their policies and actual practices.

- **The *SolarWinds* ruling reinforces that a company's public statements regarding cybersecurity practices—whether made in formal or informal forums—can be actionable under the federal securities laws**. The court emphasized that the Security Statement, while originally intended for customers, was made available on its website and accessible to all, including investors. Accordingly, public companies may want to consider whether it may be appropriate to limit the access to representations about their cybersecurity practices to certain customers or groups of customers.

- **The *SolarWinds* ruling rejected the need for more specificity in a company's risk factor disclosures regarding cybersecurity based on the unique factual allegations in this case**. The court engaged in a detailed and thoughtful analysis of the company's risk factor disclosures, parsing through pre-incident disclosures and post-incident disclosures. With regard to pre-incident disclosures, the court generally dismissed the argument that companies should spell out the precise ways in which their vulnerabilities could result in cyberattacks. With regard to post-incident disclosures and any duty to update cybersecurity risk factors, however, the court focused on specific facts and circumstances of the allegations, ultimately concluding that the SEC failed to allege that the company was aware that it had been the victim of a cyberattack at the time of the disclosures. Accordingly, public companies should be cognizant that perils remain with regard to risk factor disclosures, particularly with respect to post-incident statements, and that materially misleading statements may lead to SEC enforcement actions.

- **The *SolarWinds* ruling casts doubt over the SEC's continued reliance on novel charges and theories.** The court's decision rejected the SEC's internal accounting controls theory in the cybersecurity context, noting that "cybersecurity controls do not fit within the statute," as well as the disclosure controls and procedures claim, noting that the allegations did not discuss failures in the construction of the controls or in the internal disclosure process. The internal accounting charge was the first-of-its-kind in the cybersecurity context, while the disclosure controls and procedure charge has been a standard claim that the SEC has brought in this area. Accordingly, public companies should be aware that there is uncertainty as to whether and how the SEC will adjust these claims and theories in future cybersecurity matters.

- **Finally, the *SolarWinds* ruling confirms that CISOs have an important part in the overall disclosure obligations of a company under the federal securities laws**. This is the first time

a court decision has made clear that a CISO can be the predicate for a federal securities fraud claim. This is a particular concern where a CISO is approving, reviewing, or creating statements that are designed to or are reasonably likely to reach the company's investors, or signing sub-certifications regarding cybersecurity. Accordingly, companies and their CISOs should be aligned on a CISO's disclosure and controls obligations and practices.

**Conclusion**

The *SolarWinds* ruling has confirmed the SEC's enforcement role in cybersecurity, albeit on a much narrower scale than its original case. Given the evolving enforcement landscape, public companies should consult with counsel who are familiar with cyber-risk management, SEC enforcement and SEC disclosure practices to ensure that their disclosures minimize potential exposure in light of *SolarWinds*.

## Footnotes

[1] Order, *SEC v. SolarWinds & Brown*, No. 1:23-cv-09518 (S.D.N.Y. July 18, 2024), ECF No. 125.

[2] Complaint, *SEC v. SolarWinds & Brown*, No. 1:23-cv-09518 (S.D.N.Y. Oct. 30, 2023), ECF No. 1.

[3] *Id.* ¶¶ 2, 11.

[4] *See id.* ¶¶ 2–18.

[5] *Id.* ¶ 36.

[6] *Id.* ¶¶ 38–193.

[7] *Id.* ¶¶ 194–202.

[8] Amended Complaint ¶ 321, *SEC v. SolarWinds & Brown*, No. 1:23-cv-09518 (S.D.N.Y. Feb. 16, 2024), ECF No. 85.

[9] Order at 2–3.

[10] *Id.* at 3.

[11] *Id.* at 2–3.

[12] *Id.* at 3.

[13] *Id.*

[14] Order at 7.

[15] Amended Complaint ¶¶ 58, 220, 222.

[16] Order at 52.

[17] *Id.* at 56.

[18] *Id.* at 53.

[19] *Id.* at 52.

[20] *Id.* at 56.

[21] *Id.* at 57.

[22] *Id.* at 52.

[23] *Id.*; Transcript of Oral Argument at 31, *SEC v. SolarWinds & Brown*, No. 1:23-cv-09518 (S.D.N.Y. May 15, 2024).

[24] Order at 62.

[25] *Id.* at 63–64.

[26] *Id.* at 65.

[27] *Id.* at 67; *see* Amended Complaint ¶¶ 219-25.

[28] Order at 67.

[29] *Id.* at 67–68.

[30] *Id.* at 69.

[31] *Id.* at 71.

[32] *Id.* at 73.

[33] *Id.*

[34] *Id.* at 75.

[35] *Id.*

[36] *Id.* at 78.

[37] *Id.* at 79–81.

[38] *Id.* at 80 n. 40.

[39] *Id.*

[40] *Id.* at 85–94.

[41] *Id.* at 87–88.

[42] *Id.* at 90.

[43] *Id.* at 96, 100. The court also dismissed the SEC's aiding and abetting claim against Brown. *Id.* at 102 n. 51.

[44] Transcript of Oral Argument at 77–78.

[45] Order at 99.

[46] *Id.* at 96.

[47] *Id.* at 98, 100.

[48] *Id.* at 98, 101–102.

[49] *Id.* at 100.

[50] *Id.* at 103.

[51] *Id.* at 102–107.

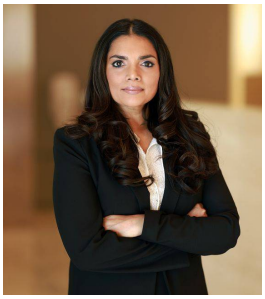
[52] *Id.* at 103.

[53] *Id.* at 103–106.

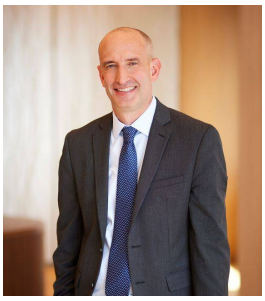
[54] *Id.* at 104.

[55] *Id.* at 106.

## Related Attorneys



**Shoba Pillay**
Partner
spillay@jenner.com
+1 312 923 2605



**Charles D. Riely**
Partner
criely@jenner.com
+1 212 891 1686

**H. Kurt von Moltke**
Partner
kvonmoltke@jenner.com
+1 312 840 7499

## Related Capabilities

Data Privacy and Cybersecurity

Investor and Securities Litigation



**Stay Informed** →