ALERT MEMORANDUM

SDNY Court Dismisses Several SEC Claims Against SolarWinds and its CISO

July 26, 2024

In October 2023, the SEC brought a highly-publicized case against SolarWinds Corp. and its Chief Information Security Officer ("CISO") for allegedly misleading disclosures and deficient controls related to a cyberattack that SolarWinds disclosed in December 2020. It had never brought a case against a CISO before. Last week, Judge Paul A. Engelmayer of the Southern District of New York dismissed significant portions of the SEC's case. Judge Engelmayer found that the SEC's claims based on the Company's post-incident disclosures, which the agency claimed minimized the attack, were ill-pled and amounted to inappropriate second-guessing. In an issue of first impression, Judge Engelmayer also dismissed the SEC's internal controls claims, holding that *accounting* controls could not be reasonably read to encompass *cybersecurity* controls. He also held that the SEC inadequately pled disclosure controls failures by the Company. Nonetheless, the district court upheld the SEC's allegations that, for years before the attack, SolarWinds had posted materially misleading statements about its supposedly strong cybersecurity measures on its website. The SEC's new cyber disclosure rules that took effect in December 2023, as well as ongoing requirements for adequate disclosure controls, underscore the need for public companies to remain vigilant on cybersecurity matters despite the recent ruling.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

NEW YORK

Francesca L. Odell
+1 212 225 2530
flodell@cgsh.com

Jonathan S. Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Michael Kowiak
+1 212 225 2929
mkowiak@cgsh.com

WASHINGTON

Matthew C. Solomon
+1 202 974 1680
msolomon@cgsh.com

Thomas A. Bednar
+1 202 974 1836
tbednar@cgsh.com

Background of the *SolarWinds* Decision

SolarWinds Corp. is a U.S.-based software company that sells a variety of products to customers, including federal and state governments and many Fortune 500 companies. In December 2020, SolarWinds learned that it had suffered a significant cyberattack, during which state-sponsored threat actors had corrupted the security of a software product that many of its customers had subsequently downloaded, in what came to be known as the "SUNBURST" attack. At least two purchasers observed suspicious behavior in connection with the compromised product whose vulnerability was not yet known—and informed SolarWinds of that fact—in the months leading up to SolarWinds's learning of the full scope of the attack.

In October 2023, the SEC filed a complaint against SolarWinds and its CISO, alleging that they made false statements in violation of the antifraud provisions of the federal securities laws, by touting the strength of their cybersecurity practices in the period before they learned of the SUNBURST incident, and by misleadingly minimizing the extent of the intrusion after discovering the incident. The SEC also claimed that SolarWinds had such poor cybersecurity and incident reporting procedures that the defendants violated the internal controls and disclosure controls provisions of the securities laws.

The Decision

On July 18, 2024, the district court granted in part and denied in part SolarWinds's motion to dismiss the operative complaint.[1]

i. Dismissed Claims

Judge Engelmayer dismissed most of the SEC's claims against SolarWinds.

Pre-Incident Blog Posts, Podcasts, and Press Releases. The court dismissed the SEC's allegation that certain of the Company's pre-incident blog posts, podcasts, and press releases "misleadingly touted SolarWinds'[s] cybersecurity practices," by emphasizing its "commitment to high security standards" and by claiming that the Company "makes sure everything is backed by sound security processes, procedures, and standards."[2] The court ruled that these statements were "non-actionable . . . puffery" that was "too general" to be actionable, because "[n]one of these challenged materials purport to describe SolarWinds'[s] cybersecurity practices or general business practices at a level of detail at which a reasonable investor would have relied on them in making investment decisions."[3]

Pre-Incident Cybersecurity Risk Disclosure. The court also dismissed claims related to the cybersecurity risk disclosure in SolarWinds's Form S-1 and incorporated in subsequent filings. The SEC had alleged the cybersecurity risk disclosure "concealed the gravity of the cybersecurity risks that SolarWinds faced," including because it was "unacceptably boilerplate and generic" and because SolarWinds did not update it to reflect the information it learned from customers in June and October 2020 regarding cyber incidents involving its software product.[4]

In dismissing this claim, the court explained the cautionary disclosure "enumerated in stark and dire terms the risks the company faced were its cybersecurity measures to fail," and stated that if "the SEC . . . mean[t] to fault SolarWinds for not spelling out these risks in greater detail, the case law does not require more."[5] Judge Engelmayer added that "[i]n light of this fulsome disclosure, SolarWinds did not have a duty to disclose the fact of individual cyber

[1] Judge Engelmayer noted at the outset of his decision that this matter does not implicate or affect the SEC's new cybersecurity rules. Those rules took effect after the events at issue in *SolarWinds*, and require companies to file a Form 8-K announcing a material cyber incident within four business days of determining there has been a material breach, and to provide annual disclosure of cybersecurity governance and risk management. *See* Cleary Alert Memo, *New SEC Disclosure Rules for Cybersecurity Incidents and Governance and Key Takeaways* (Aug. 2, 2023).

[2] *Securities and Exchange Commission v. SolarWinds Corp.*, 2024 WL 3461952, at *6, *33 (S.D.N.Y. July 18, 2024).

[3] *Id.* at *34.

[4] *Id.* at *34–35, *37–39.

[5] *Id.* at *35–36.

intrusions or attacks" that were reported to it by customers at a time when it was not known that those incidents were related to a broader attack on SolarWinds.[6]

Post-Incident Form 8-Ks. The court dismissed the SEC's allegations related to the Form 8-K disclosures SolarWinds made after it learned the full extent of the cyber incident that impacted its own networks in December 2020. The SEC claimed the disclosures misleadingly omitted "the fact that the malicious code . . . had already activated in . . . two instances" and referred to the possibility of the compromised software being exploited only in theoretical terms.[7] For example, one of the Form 8-Ks provided that the incident "could potentially allow an attacker to compromise the server on which the . . . products run."[8]

The decision rejected the SEC's claim and explained that the first Form 8-K SolarWinds filed after learning the full scope of the attack was not misleading because it did not foreclose the possibility that the infected software had led to cyber incidents for customers using the compromised product. Indeed, because the disclosure "captured . . . the severity of the . . . attack," this "made the absence of a reference to the two earlier incidents immaterial."[9] The court also noted that "[t]he disclosure was made at a time when SolarWinds was at an early stage of its investigation, and when its understanding of that attack was evolving."[10]

Internal Controls. The district court dismissed the SEC's claim that SolarWinds's allegedly inadequate cybersecurity practices violated the Exchange Act's internal controls provision, which requires an issuer to "devise and maintain a system of internal accounting controls" so that "access to assets is permitted only in accordance with management's general or specific authorization."[11] The SEC alleged that SolarWinds violated this provision because its poor password policies, access controls, and VPN management did not limit access to assets, including its "source code, databases, and products."[12] The district court agreed with SolarWinds that, as a matter of law, the internal controls provision's "requirement that a public issuer 'devise and maintain a system of internal accounting controls' is properly read to require that issuer to accurately report, record, and reconcile *financial* transactions and events," and, as such, "cannot reasonably be interpreted to cover a company's cybersecurity controls such as its password and VPN protocols."[13]

Disclosure Controls. The court also dismissed the claim that SolarWinds did not adequately "maintain disclosure controls and procedures" as required by a rule promulgated under the Exchange Act.[14] The SEC had alleged SolarWinds failed to design and implement an effective system of disclosure controls because it had misclassified and failed to escalate to management the customer-reported intrusions throughout 2020, which prevented assessment of whether public disclosure was required. The court rejected this claim because the facts as pled indicated that "SolarWinds had a system of controls in place to facilitate the disclosure of potentially material cybersecurity risks and incidents" and that this system "was designed to ensure that material cybersecurity information was timely communicated to the executives responsible for public disclosures."[15]

Even if SolarWinds's system had misclassified the two customer incidents as not meriting reporting upwards (which the court held the SEC had not adequately pled),[16] the court emphasized that "the SEC does not

[6] *Id.* at *37. The court also dismissed the SEC's claims under Section 13(a) of the Exchange Act.
[7] *Id.* at *44.
[8] *Id.*
[9] *Id.* at *46. The court found that the second Form 8-K that SolarWinds filed after learning the full scope of the incident was not misleading for similar reasons.
[10] *Id.* at *44.
[11] *See* Exchange Act Section 13(b)(2)(B), 15 U.S.C. §78m(b)(2)(B).
[12] *SolarWinds,* 2024 WL 3461952, at *48.
[13] *Id.* at *48, *50.
[14] *See* Exchange Act Rule 13a-15(a); 17 CFR §240.13a-15.
[15] *SolarWinds,* 2024 WL 3461952, at *53.
[16] The district court explained that although SolarWinds's incident response plan required escalation of incidents "affect[ing] multiple customers" to management, the SEC

plead any deficiency in the construction of this [incident classification] system."[17] Judge Engelmayer noted that perfection is not required for compliance with disclosure controls: The decision emphasized that "errors happen without systemic deficiencies."[18] In light of this, the court concluded that "[w]ithout more, the existence of two misclassified incidents is an inadequate basis on which to plead deficient disclosure controls."[19] Notably, in contrast to the accounting controls claim, the district court did not reject the SEC's disclosure controls claim as a matter of law.

ii. Claims That Survived

The Security Statement. The district court denied the motion to dismiss with respect to the statements made in a "Security Statement" posted by the Company on its website. The SEC had alleged that the statement was inaccurate in describing whether the Company: "(1) complied with the National Institute of Standards and Technology . . . Cybersecurity Framework for evaluating cybersecurity practices; (2) used a secure developmental lifecycle to create its software products; (3) employed network monitoring; (4) had strong password protections; and (5) maintained good access controls."[20]

The court found that the SEC adequately alleged that the Security Statement was misleading regarding access controls where it stated that "[e]mployees are granted access . . . based on their specific job function" and were "provided access to sensitive data on a 'need-to-know . . . basis,'" while in reality SolarWinds "was . . . freely granting administrative rights to employees and conferring access rights way beyond those necessary."[21] As to password policies, the court found the SEC had adequately pled the Security Statement was misleading when it stated that "[o]ur password best practices enforce the use of complex passwords," when in fact "the company's stated password policy was generally not enforced," as "employees . . . routinely used simple, unencrypted passwords" such as "solarwinds123."[22] SolarWinds was allegedly aware of these issues but did not timely resolve them.[23]

Judge Engelmayer found that the SEC had adequately alleged the Security Statement to have been material, noting that while "the business risks presented by such penetrable cybersecurity might well have been material for a company that sold old-fashioned products (*e.g.*, furniture or cars)," they "were undeniably material" in the case of SolarWinds "[g]iven the centrality of cybersecurity to [its] business model as a company pitching sophisticated software products to customers for whom computer security was paramount."[24] The court brushed aside SolarWinds's argument that the Security Statement could not serve as the basis for the SEC's claims because it was not meant for investors, observing that "[i]t is well established that false statements on public websites can sustain securities fraud liability" because they are "part of the 'total mix of information' that SolarWinds furnished the investing public."[25]

Takeaways

There are several important takeaways from Judge Engelmayer's decision.

- First, the *SolarWinds* decision strikes a blow to the SEC's assertion that cybersecurity controls are part of the internal controls over financial reporting

had not pled that the Company had "definitively determined that the two [prior customer-related] incidents were related." As a result, the SEC had not adequately pled that these incidents were misclassified under SolarWinds's internal framework. *Id.* at *53.

[17] *Id.*

[18] *Id.*

[19] *Id.* The court also rejected a disclosure controls claim related to the failure to escalate a VPN security concern to the CEO and CTO in 2018, because the fact that "this one lapse was not elevated to the company's top rung does not, without more, plausibly impugn the company's disclosure controls systems." *Id.* at *54.

[20] *Id.* at *4.

[21] *Id.* at *27.

[22] *Id.* at *28–29.

[23] The decision did not decide whether the other three categories of alleged misstatements in the Security Statement were misleading.

[24] *SolarWinds,* 2024 WL 3461952, at *28, *30.

[25] *Id.* at *26.

mandated by the securities laws. While the SEC could appeal the *SolarWinds* decision, and may try to secure different rulings from other judges on this issue, the persuasive logic in Judge Engelmayer's ruling may cause the SEC to press pause on pursuing cybersecurity controls as internal controls. Given that companies are now required to make additional disclosures regarding cybersecurity incidents and governance, the SEC may instead focus on companies' disclosures and disclosure controls. Judge Engelmayer's decision left both of these paths potentially open to the SEC, and the SEC had generally brought its cybersecurity cases under these provisions prior to *SolarWinds.* It is also possible the SEC does not completely surrender pursuing cybersecurity controls cases, but instead narrows its focus to cyber vulnerabilities that are more closely related to a company's financial reporting systems.[26]

- Second, this case serves as a reminder that companies can be liable in an SEC enforcement action for public statements that are not contained in SEC filings and that may not even be intended for investors. This includes marketing materials, security statements, ESG statements, and any other public statement that is part of the "total mix of information" available to investors.
- Third, the *SolarWinds* decision illustrates that to some courts there may be a difference between highly general statements that tout strong cybersecurity, which may be dismissed as mere puffery, and concrete statements of fact about specific cybersecurity practices, which can give rise to a fraud claim if the company is not actually following those practices with consistency. Compare Judge Engelmayer's dismissal of claims related to generic statements by SolarWinds that it "places a premium on the security of its products" and "makes sure everything is backed by sound security processes" with his denial of the motion to dismiss related to statements such as Solarwinds's representation that its "password best practices enforce the use of complex passwords that include both alpha and numeric characters."[27]
- Fourth, Judge Engelmayer's opinion illustrates the importance of providing supplemental disclosures when the victim of a cyberattack determines additional material information about an incident. The district court cited an additional Form 8-K that SolarWinds filed in January 2021—which provided further details about the attack that it had reported the previous month—as evidence of a lack of scienter regarding any possible material omission in its earlier SEC filings. Although the court did not treat the fact of this additional filing as a central reason for dismissing the claims related to the Form 8-Ks, this point still highlights the importance of filing follow-up disclosures after a cyberattack, as appropriate.

…

CLEARY GOTTLIEB

[26] *See, e.g.*, Exchange Act Release No. 34-55929 (June 20, 2007) (Interpretive Release) (citing IT general controls as "controls that perform automated matching, error checking or edit checking functions," or that "post[] correct balances to appropriate accounts or ledgers").

[27] *SolarWinds,* 2024 WL 3461952, at *28–29, *33–34.