IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 1:23-cv-09518-PAE-BCM **ORAL ARGUMENT REQUESTED**

MEMORANDUM OF LAW IN SUPPORT OF
DEFENDANTS' MOTION TO DISMISS THE COMPLAINT

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Regulations

Other Authorities

PRELIMINARY STATEMENT

In December 2020, SolarWinds Corporation ("SolarWinds" or the "Company") learned it had suffered an extraordinarily sophisticated attack by the Russian government ("SUNBURST"). SolarWinds responded just as a public company should: it promptly and transparently disclosed the attack and continued to update investors as its investigation progressed. Nonetheless, more than three years later, the SEC seeks to revictimize the victim, by bringing securities fraud and controls charges against the Company and its Chief Information Security Officer ("CISO"), Tim Brown. The charges are as unfounded as they are unprecedented. The SEC is trying to unfairly move the goalposts for what companies must disclose about their cybersecurity programs and, with the controls charges, claim a mandate for regulating those programs that the agency does not have. The case is fundamentally flawed and should be dismissed in its entirety.

The SEC's fraud claims fail because it does not—and cannot—plausibly allege any materially misleading statements. First, SolarWinds' risk factors specifically warned that its systems "are vulnerable" to "sophisticated nation-state" actors—the very risk that materialized. The SEC complains these disclosures were insufficient, asserting that companies must disclose detailed vulnerability information in their SEC filings. But that is not the law, and for good reason: disclosing such details would be unhelpful to investors, impractical for companies, and harmful to both, by providing roadmaps for attackers. Second, when SUNBURST occurred, SolarWinds disclosed the key facts it knew about the attack and its severity, including that as many as 18,000 customers were at risk of compromise. Given those candid disclosures, the notion that SolarWinds concealed the seriousness of the attack is absurd. Third, the SEC alleges nothing that would render SolarWinds' statements about its security policies misleading. It points to documents supposedly reflecting gaps in the implementation of those policies, but no reasonable investor would have

understood SolarWinds' statements to imply a standard of perfection, especially when its risk factors warned that it was vulnerable to attack *despite* its security measures.

The SEC's fraud claims independently fail for lack of scienter. First, the SEC does not even try to suggest that the executives responsible for the risk factor disclosures—the Company's CEO and CFO—acted with fraudulent intent. Second, the SEC cannot plausibly allege that the initial disclosure about SUNBURST was intended to hide facts from investors, particularly given that the Company disclosed the allegedly omitted facts only weeks later after further investigation. Third, the SEC does not plausibly allege that Mr. Brown or anyone else who made statements about SolarWinds' security policies believed the statements to be inaccurate. At most, the allegations reflect employees working to *identify and correct* any deficiencies in implementing the policies—which is exactly what a cybersecurity program is supposed to do. None of the SEC's allegations suffice to show even negligence, let alone scienter.

As for the controls charges, the SEC fails to identify any disclosure controls that were unreasonably designed. And its theory of "internal accounting controls" violations amounts to a wholesale rewriting of the law. The agency is seeking to twist the concept of *accounting* controls into a sweeping mandate for it to regulate public companies' *cybersecurity* controls—a role for which the SEC lacks congressional authorization or substantive expertise.

Finally, the SEC's targeting of Mr. Brown is not only unwarranted but inexplicable. Mr. Brown is not even alleged to have played a role in the Company's risk factor disclosures, and there is no conduct alleged remotely suggesting that he ever sought to deceive investors. The SEC also fails to articulate any coherent theory of aiding-and-abetting liability against Mr. Brown. Mr. Brown is an experienced and well-respected professional who simply did his job during the events in question (and did it well). The SEC's gratuitous charges against him should be rejected.

BACKGROUND[1]

The relevant facts for purposes of this motion are straightforward: SolarWinds warned investors that its systems were vulnerable to cyberattack. In December 2020, SolarWinds suffered an attack—SUNBURST—which it promptly disclosed, identifying the outer universe of customers at risk. Yet the SEC now alleges that, despite these disclosures, the Company sought to hide its vulnerability to cyberattack and to conceal the seriousness of SUNBURST.

A. SolarWinds Repeatedly Warned Investors It Was Vulnerable to Cyberattack

SolarWinds is a developer of network monitoring software, which many businesses and government agencies use to manage their computer networks. ¶ 36. SolarWinds has (and had during the relevant timeframe) more than 300,000 customers, including nearly all the companies making up the Fortune 500. ¶ 36. One of its products is the Orion Platform, which consists of a suite of products used for network management. ¶ 37.

Like any technology-focused business, SolarWinds is vulnerable to the pervasive risk of cybersecurity attacks. Thus, when SolarWinds went public in October 2018, it disclosed this risk to its investors in its Form S-1 registration statement, along with the material consequences that could follow if an attack succeeded. The disclosure stated in relevant part:

> Our systems and those of our third-party service providers are vulnerable to damage and disruption from . . . traditional computer "hackers," malicious code (such as viruses and worms), employee theft or misuse, and denial-of-service attacks, as well as sophisticated nation-state and nation-state-supported actors (including advanced persistent threat intrusions). . . . Despite our security measures, unauthorized access to, or security breaches of, our software or systems could result in the loss, compromise or corruption of data, loss of business, severe reputational

[1] Except where otherwise noted, all facts stated are drawn from the Complaint, citations to which are styled as "¶ [paragraph number]." Any exhibits cited are attached to the Declaration of Serrin Turner, submitted herewith, and include "documents incorporated into the complaint by reference, legally required public disclosure documents filed with the SEC, and documents possessed by or known to the plaintiff and upon which it relied in bringing the suit," *ATSI Commc'ns, Inc. v. Shaar Fund, Ltd.*, 493 F.3d 87, 98 (2d Cir. 2007), or "matters of which judicial notice may be taken," *Leonard F. v. Israel Discount Bank of New York*, 199 F.3d 99, 107 (2d Cir. 1999).

> damage adversely affecting customer or investor confidence, regulatory investigations and orders, litigation, indemnity obligations, damages for contract breach, penalties for violation of applicable laws or regulations, significant costs for remediation and other liabilities.

¶ 131; Ex. 1, at 2–3. SolarWinds noted that the risk of a security breach, "including by . . . foreign governments," had "increased," as "intrusions around the world have increased" in terms of their "number, intensity and sophistication." ¶ 131.

SolarWinds also disclosed the specific risk of a sophisticated, prolonged attack that could impact its customers—like SUNBURST. "Because the techniques used to obtain unauthorized access or to sabotage systems change frequently," the Company explained, it "may be unable to anticipate these techniques or to implement adequate preventative measures," and "may also experience security breaches that may remain undetected for an extended period." *Id.* Such "security problems," the Company warned, could cause not only damage to its own systems, but also damage to "our customers' IT infrastructure or the loss or theft of our customers' proprietary or other sensitive information." *Id.* SolarWinds consistently repeated these warnings or incorporated them by reference in each of its quarterly and annual reports thereafter. ¶¶ 32, 136.

B. SolarWinds Discovered and Promptly Disclosed the SUNBURST Attack

On Saturday, December 12, 2020, SolarWinds learned it had been the victim of a cyberattack: a customer (itself a leading cybersecurity firm) informed the Company that it had located a vulnerability in the code for the Orion product, which had evidently been inserted by a threat actor. ¶ 183. The vulnerability—dubbed "SUNBURST"—provided a "backdoor" that the threat actor could use to infiltrate the "network environments of SolarWinds' customers who downloaded and installed the infected versions of the software to systems that were connected to the internet." ¶ 143. The threat actor had inserted the vulnerability into three different Orion software versions or "builds," which nearly 18,000 customers downloaded. *Id*. While unknown to

SolarWinds when it learned of the incident, the threat actor used the vulnerability to conduct attacks on roughly 100 of these customers. *Id.* The federal government concluded that Russia was the threat actor behind SUNBURST, and that the incident was "one of the most . . . sophisticated hacking campaigns ever conducted against the federal government and private sector." U.S. GAO, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents* ("GAO Report"), GAO-22-104746, at 1, 14 (Jan. 2022), https://www.gao.gov/assets/gao-22-104746.pdf.

Upon learning of SUNBURST, SolarWinds immediately launched an investigation, including engaging an outside cybersecurity firm to assist, and prepared an 8-K to inform the market of the situation. ¶¶ 185, 188. On Monday, December 14—the very next trading day—SolarWinds filed a detailed disclosure, explaining, among other things:

> SolarWinds Corporation ("SolarWinds" or the "Company") has been made aware of a cyberattack that inserted a vulnerability within its Orion monitoring products which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run. SolarWinds has been advised that this incident was likely the result of a highly sophisticated, targeted and manual supply chain attack by an outside nation state, but SolarWinds has not independently verified the identity of the attacker. SolarWinds has retained third-party cybersecurity experts to assist in an investigation of these matters, including whether a vulnerability in the Orion monitoring products was exploited as a point of any infiltration of any customer systems, and in the development of appropriate mitigation and remediation plans. SolarWinds is cooperating with the Federal Bureau of Investigation, the U.S. intelligence community, and other government agencies in investigations related to this incident.

Ex. 2, at 3. The 8-K explained that up to 18,000 customers had downloaded infected versions of Orion and that Orion accounted for nearly half the Company's revenue. *Id.* It also noted there had been "significant media coverage of attacks on U.S. governmental agencies and other companies, with many of those reports attributing those attacks to a vulnerability in the Orion products." *Id.* The 8-K identified "numerous financial, legal, reputational and other risks to SolarWinds" that could result from the attack. *Id.* SolarWinds also described the status of its remediation efforts and certain topics it was investigating, but stressed that its investigation was "preliminary and on-

going," and that it was "unable to share additional information at this time." *Id.* SolarWinds' stock price dropped nearly 25 percent over the next two days, ¶ 18, indicating investors understood the severity of the situation.

SolarWinds filed multiple follow-up disclosures to update investors about the incident, including Forms 8-K filed on December 17, 2020, Ex. 3, and January 11, 2021, Ex. 4. The January 8-K provided a detailed timeline of the attack and explained the Company's ongoing coordination with "law enforcement, the intelligence community, governments and industry colleagues." *Id.* The Company also disclosed that, as part of its ongoing investigation, it was "reviewing historical and current customer inquiries," and had "identified two previous customer support incidents that, with the benefit of hindsight, we believe may be related to SUNBURST." *Id.* It noted that, when the two customers previously reported the incidents, the Company was unable to discover the SUNBURST vulnerability or otherwise identify the root cause of the reports. *Id.* As the SEC stated at the initial case conference, this January 8-K marks the end of what the Complaint defines as the "Relevant Period," which extends from the Company's IPO in October 2018 to January 12, 2021, the day after this 8-K was filed. ¶ 1; Hr'g Tr. 4:21–5:8, Dec. 14, 2023, ECF No. 32.

C. After Nearly Three Years of Investigation, the SEC Brings This Lawsuit

While other federal agencies worked cooperatively with SolarWinds in investigating SUNBURST and mitigating the impacts of this nation-state attack, the SEC instead fixated on finding targets to charge with securities violations. It not only investigated SolarWinds (for nearly three years), but also requested, under threat of enforcement, information from many of SolarWinds' *customers*, and questioning *their* disclosures.[2] The SEC has never before brought an

[2] *See* Christopher Bing et al., *Wide-ranging SolarWinds Probe Sparks Fear in Corporate America*, Reuters (Sept. 10, 2021), https://www.reuters.com/technology/exclusive-wide-ranging-solarwinds-probe-sparks-fear-corporate-america-2021-09-10; *see also* SEC, *In the Matter of*

action in federal court against any public companies over their cybersecurity disclosures or brought "internal accounting controls" violations based on alleged deficiencies in their cybersecurity controls with no nexus to accounting. Nor has it ever individually charged a CISO.[3]

The Complaint brings claims for fraud and false statements (under Securities Act § 17(a), Exchange Act §§ 10(b) & 13(a), and Rule 10b–5), disclosure controls violations (under Rule 13a–15(a)), and internal accounting controls violations (under Exchange Act § 13(b)(2)(B)), against both the Company and Mr. Brown, along with aiding-and-abetting charges against Mr. Brown. ¶¶ 203-37. As to the fraud and false statement claims, the SEC alleges, first, that SolarWinds' risk factors were misleading because SolarWinds supposedly had various deficiencies in its cybersecurity controls that made it not merely vulnerable, but "very vulnerable" to, or at "increased risk" of, attack. ¶¶ 133-34. Second, the SEC alleges that SolarWinds' initial 8-K about SUNBURST misleadingly omitted that SolarWinds had linked SUNBURST to certain previous customer support incidents (the same ones mentioned in the Company's follow-up 8-K four weeks later). ¶¶ 187-89. Third, the SEC alleges that various statements SolarWinds directed to customers, on its website and in certain blog posts, press releases, and podcasts, misrepresented its security policies. ¶ 125. As to disclosure controls, the SEC alleges the Company lacked reasonable controls for escalating potentially material incidents to senior management. ¶¶ 201-02. As to "internal accounting controls," the SEC alleges that SolarWinds lacked reasonable controls to restrict access to its "information technology network environment, source code, and products," which it describes as "the Company's most critical assets." ¶¶ 194-95.

Certain Cybersecurity-Related Events (HO-14225) FAQs (last modified Nov. 30, 2022), https://www.sec.gov/enforce/certain-cybersecurity-related-events-faqs.

[3] It should be noted that, during the Relevant Period, Mr. Brown was not CISO but Vice President of Security Architecture, ¶ 1, a non-executive position.

LEGAL STANDARDS

Under Rule 12(b)(6), courts accept well pleaded factual allegations as true, but "the Federal Rules do not require courts to credit a complaint's conclusory statements without reference to its factual context." *Ashcroft v. Iqbal*, 556 U.S. 662, 686 (2009). "[W]here a conclusory allegation in the complaint is contradicted" by a properly considered document, "the document controls and the allegation is not accepted as true." *Amidax Trading Grp. v. S.W.I.F.T. SCRL*, 671 F.3d 140, 147 (2d Cir. 2011); *see Gillis v. QRX Pharma*, 197 F. Supp. 3d 557, 583–84 (S.D.N.Y. 2016) (Engelmayer, J.) (rejecting fraud claims premised on mischaracterized document).

Under Rule 9(b), a complaint must "state with particularity the circumstances constituting" alleged fraud. *S.E.C. v. Rio Tinto plc*, 2019 WL 1244933, at *6 (S.D.N.Y. Mar. 18, 2019). This standard applies to SEC enforcement actions. *See id*. Thus, the SEC must "(1) specify the statements that [it] contends were fraudulent, (2) identify the speaker, (3) state where and when the statements were made, and (4) explain why the statements were fraudulent," and "allege facts giving rise to a 'strong inference of fraudulent intent.'" *Novak v. Kasaks*, 216 F.3d 300, 306 (2d Cir. 2000). This standard also applies to non-fraud claims "premised on allegations of fraud," *Rombach v. Chang*, 355 F.3d 164, 171 (2d Cir. 2004), where they allege the same "false and misleading statements and omissions" and "pertain to the exact same underlying events," *Lighthouse Fin. Grp. v. Royal Bank of Scot. Grp., PLC*, 902 F. Supp. 2d 329, 339 (S.D.N.Y. 2012).

ARGUMENT

I. The Fraud and False-Filing Claims Should Be Dismissed

To state a claim for securities fraud under Exchange Act § 10(b) and Rule 10b–5, the SEC must allege that defendants "(1) made a material misrepresentation or a material omission as to which [they] had a duty to speak . . . ; (2) with scienter; (3) in connection with the purchase or sale of securities." *S.E.C. v. Monarch Funding Corp.*, 192 F.3d 295, 308 (2d Cir. 1999). Section 17(a)

requires essentially the same elements, except that negligence suffices for injunctive relief under subsections (a)(2) or (a)(3). *Id.*; *S.E.C. v. Ginder*, 752 F.3d 569, 574 (2d Cir. 2014). A false-filing claim under Exchange Act § 13(a) requires material misstatements specifically in SEC filings, but it does not require scienter. *Rio Tinto plc*, 2019 WL 1244933, at *17. Here, all these claims fail because the SEC does not plausibly allege any material misrepresentation or omission. And the fraud claims doubly fail because they do not adequately allege scienter (or even negligence).

A. The Complaint Fails to Allege a Material Misrepresentation or Omission

The SEC bases its fraud and false-statement claims on three categories of statements: (1) statements to investors in its risk factors before SUNBURST; (2) statements to investors after SUNBURST about the attack; and (3) general cybersecurity-related statements on the Company's website and elsewhere. It fails to plausibly allege that any were materially misleading.

1. The Risk Factors Were Not Materially Misleading

Perhaps the SEC's most puzzling claim is that SolarWinds' risk factor disclosures before SUNBURST were somehow materially misleading. The disclosures in fact warned investors of the precise risk at issue. They specifically advised that SolarWinds' systems were "vulnerable" to various cyber threats, including "advanced persistent threat intrusions" from "sophisticated nation-state and nation-state-supported actors." The Company further warned it may be unable to stop an attack "[d]espite our security measures," and that these "security problems" could lead to various material consequences, including "damage to our own systems or our customers' IT infrastructure or the loss or theft of our customers' proprietary or other sensitive information." ¶ 131; Ex. 1, at 3. Any reasonable investor reading these disclosures would have understood that SolarWinds was vulnerable to a cyberattack—including one like SUNBURST. If a company's disclosures "were sufficient to pick up the . . . risk that later materialized"—as these disclosures were—then as a

matter of law they cannot be materially misleading. *Garnett v. RLX Tech. Inc.*, 632 F. Supp. 3d 574, 599-602 (S.D.N.Y. 2022) (Engelmayer, J.).

Courts have found similar cybersecurity risk factors unactionable for this very reason. For example, in *In re Qudian Inc. Securities Litigation*, Judge Furman rejected a claim that the defendant had misrepresented its cybersecurity protocols, finding that, whatever affirmative representations the defendant made about its security measures, its offering materials plainly disclosed that those "security measures could be breached," that the defendant "may be unable . . . to implement adequate preventative measures" to stop an attack, and that material consequences could ensue. 2019 WL 4735376, at *8 (S.D.N.Y. Sept. 27, 2019). "In light of these disclosures," the court held, "it cannot be said that Plaintiffs plausibly identify a material misrepresentation." *Id.*; *see also In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189, 1226–27 (N.D. Ga. 2019) (finding statement that systems "could be vulnerable to . . . breaches of confidential information" not actionable, as it "warned of the precise risk that caused the Plaintiff's losses"). So too here.

The SEC articulates no coherent theory as to how SolarWinds' risk factors were misleading or what exactly SolarWinds should have said instead. Instead, the SEC vaguely complains that the disclosures were "generic," ¶ 7, "boilerplate," ¶ 130, or "hypothetical," ¶ 7. But "[t]hese statements conveyed substantive information about the risk that ultimately materialized. As such, they were meaningful cautionary language, not mere boilerplate." *In re Sanofi Sec. Litig.*, 87 F. Supp. 3d 510, 536 (S.D.N.Y. 2015) (Engelmayer, J.); *see also Rombach*, 355 F.3d at 175 (affirming dismissal where "some of the[] cautionary statements were formulaic" but "as a whole they provided a sobering picture"). Nor were the disclosures "hypothetical": they made clear the Company was *actually, presently at* risk of a cyberattack, explicitly stating that its systems "*are* vulnerable." Thus, a reasonable investor could not have been "misled into thinking that the risk

that materialized"—the risk of an attack like SUNBURST—"did not actually exist." *In re FBR Inc. Sec. Litig.*, 544 F. Supp. 2d 346, 361 (S.D.N.Y. 2008).

Still, the SEC insists that something was missing from the risk factors—it just cannot put its finger on what it was. It rummages through a grab bag of alleged "red flags," ¶ 137, variously claiming that SolarWinds failed to "disclose[] that known, unremediated issues with NIST compliance, SDL, access controls (including [a] known VPN vulnerability), or passwords existed," ¶ 134, or that there was a "backlog" of product vulnerabilities at one point and "inadequate staffing" to address them, ¶ 159, or that SolarWinds was "[unable] to determine the root cause" of a customer-reported incident in June 2020, ¶ 155, or that an allegedly similar issue was reported in October 2020 that it likewise could not resolve, ¶¶ 161, 163. In short, the SEC seems to believe that SolarWinds had a duty to disclose detailed information about supposed cybersecurity shortcomings, and that omitting such details from its risk factors was materially misleading.

SolarWinds emphatically disagrees with the SEC's characterizations of these alleged issues; but even accepting the allegations as true for purposes of this motion, the SEC's disclosure theory fails as a matter of law. SolarWinds had no duty to inform investors about granular cybersecurity concerns or day-to-day matters such as staffing levels. "A company is generally not obligated to disclose internal problems because the securities laws do not require management to bury the shareholders in internal details, and because public disclosure of internal management and engineering problems falls outside the securities laws." *In re N. Telecom Ltd. Sec. Litig.*, 116 F. Supp. 2d 446, 459 (S.D.N.Y. 2000) (quotation marks and citations omitted). Rather, the SEC's "risk factor" regulations require disclosure only of "the most significant factors that make an offering speculative or risky." Regulation S-K Item 503(c), 84 Fed. Reg. 12674, 12702 (Apr. 2, 2019).

SolarWinds disclosed its "most significant" cybersecurity risks: the risk of a successful attack and the various material consequences that could ensue. ¶ 131. By comparison, alleged "internal problems," such as an engineer's concern about a VPN configuration or a failure to determine the root cause of a customer report, cannot plausibly constitute "the most significant factors" making investment in the Company risky. These sorts of issues arise *routinely* in the daily operation of a cybersecurity program; disclosing them in investor filings would create a level of noise that would render the filings useless. *See In re Intel Corp. Sec. Litig.*, 2019 WL 1427660, at *13 n.17 (N.D. Cal. Mar. 29, 2019) (no duty to disclose specific vulnerabilities in computer chips); *In re N. Telecom Ltd.*, 116 F. Supp. 2d at 459 (no duty to disclose "software and customer problems"); *see also Tongue v. Sanofi*, 816 F.3d 199, 214 (2d Cir. 2016) ("Issuers must be forthright with their investors, but securities law does not impose on them an obligation to disclose every piece of information in their possession.").

Not only did SolarWinds have no standalone duty to disclose such information, but omitting it did not render the risk factors misleading. Having categorically disclosed that it was vulnerable to cyberattack, SolarWinds did not have to detail *how* it might be vulnerable. That information would have been merely cumulative of—not contrary to—the risk SolarWinds already disclosed. Indeed, the SEC acknowledges that the alleged vulnerabilities it cites perhaps "did not rise to the level of requiring disclosure on their own," suggesting instead that they somehow needed to be disclosed "collectively." ¶ 133. But the "collective" risk of any vulnerabilities—the risk of a cyberattack—is exactly what SolarWinds *did* disclose. No reasonable investor would view the omitted details "as having significantly altered the 'total mix' of information made available." *Basic Inc. v. Levinson*, 485 U.S. 224, 231–32 (1988); *see In re Intel*, 2019 WL 1427660, at *11, *13 n.17 (finding "reasonable investors would not be misled" by omission of information about

specific vulnerabilities "given the total mix of information" available, including broad warnings in risk factors); *Ong v. Chipotle Mexican Grill, Inc.*, 294 F. Supp. 3d 199, 230 (S.D.N.Y. 2018) ("Having addressed these issues in general terms, Defendants did not omit material facts by failing to address, in more granular terms, every eventuality."); *City of Austin Police Ret. Sys. v. Kinross Gold Corp.*, 957 F. Supp. 2d 277, 303 (S.D.N.Y. 2013) (Engelmayer, J.) (warnings about viability of defendant's mining operations were "sufficiently comprehensive" to cover specific geologic risk that materialized).

Not only is the SEC's position that companies must disclose detailed vulnerability information unsupported by the law, it is both impractical and dangerous. No company ever achieves a state of perfect security; instead, managing cybersecurity risk is a continuous endeavor. That is, *every* company *always* has various cybersecurity risks it needs to address and areas in which it needs to improve, which evolve and fluctuate on a daily basis. Requiring companies to keep the investing public constantly apprised of these granular risks would be an impossible task that would flood investors with unnecessary details. *See Basic Inc.*, 485 U.S. at 231–32 (explaining that too low a materiality threshold would "bury the shareholders in an avalanche of trivial information"). Not only that, but such a duty would put companies' security at risk by exposing internal cybersecurity information to hackers, who could leverage it for malicious purposes—to the ultimate detriment of investors.

The SEC itself has recognized the folly of requiring companies to disclose detailed vulnerability information, including in guidance on cybersecurity disclosures operative during the Relevant Period, which stated:

> This guidance is not intended to suggest that a company should make detailed disclosures that could compromise its cybersecurity efforts—for example, by providing a "roadmap" for those who seek to penetrate a company's security protections. We do not expect companies to publicly disclose specific, technical

> information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident.

SEC, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Rel. Nos. 33-10459 & 34-82746, at 11 (Feb. 26, 2018), https://www.sec.gov/files/rules/interp/2018/33-10459.pdf. Yet, here, by faulting SolarWinds for failing to disclose such alleged issues as a weakness in its VPN configuration, or a failure to enforce strong passwords, the SEC is effectively asserting a new standard requiring disclosure of precisely the sort of "roadmap" information that its prior guidance acknowledged would be inimical to security. The inexplicable about-face only underscores that SolarWinds never had any duty to disclose such information during the Relevant Period, notwithstanding the SEC's attempts to concoct one now.[4]

Perhaps anticipating this criticism, the SEC outlines a fallback position: instead of asserting that SolarWinds' disclosures should have included more details, it asserts they should have included more adverbs and adjectives. Even though SolarWinds expressly disclosed that it was "vulnerable" to a cyberattack, the SEC faults the Company for not disclosing "that it was 'very vulnerable' to a cyberattack," or that it faced an "increasing" risk of attack. ¶¶ 1, 134. But securities law "is not concerned with such subtle disagreements over adjectives and semantics." *Kinross Gold Corp.*, 957 F. Supp. 2d at 298. As long as the fundamental risk has been disclosed—as it was here—the wordsmithing is immaterial. *See In re ProShares Tr. Sec. Litig.*, 728 F.3d 96, 103 (2d

[4] Even in new cybersecurity-related disclosure rules that the SEC promulgated only last year, the SEC specifically declined to require companies to disclose specifics about their cybersecurity "policies and procedures," as it sought to "avoid levels of detail that may go beyond information that is material to investors" and to "address commenters' concerns that those details could increase a company's vulnerability to cyberattack." SEC, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Rel. Nos. 33-11216 & 34-97989, at 61 (Sept. 5, 2023), https://www.sec.gov/files/rules/final/2023/33-11216.pdf. The SEC is effectively seeking through this action to impose more demanding disclosure rules than the ones it was able to establish through rulemaking—*after* the Relevant Period.

Cir. 2013) (rejecting attempt to "use a linguistic preference to read out of the [disclosures] a scenario which the . . . disclosures clearly contemplate"); *In re Equifax*, 357 F. Supp. 3d at 1227 (finding disclosure unactionable because "[t]he difference between disclosing that Equifax 'could be vulnerable' and that it was 'highly vulnerable' would not mislead a reasonable investor").[5]

Moreover, even this fallback position is impractical and dangerous. There is no defined standard by which companies can rate themselves as "vulnerable" versus "very vulnerable" (or "very, *very* vulnerable"), or their cybersecurity risks as "steady" versus "increasing" (or "sharply increasing," and so on). Requiring companies to attempt such distinctions would require them to feign an exactitude that does not exist. *That* would be misleading to investors. *See Kinross Gold Corp.*, 957 F. Supp. 2d at 298 (dismissing claim that defendant mining company should have said that tested ore was "very hard" instead of "relatively hard," as these were not alleged to be "industry terms of art that have fixed meanings"). Such information could also be leveraged for harmful purposes, as companies that rated themselves with the most alarming descriptors would stand out as the most promising targets for cyberattacks. These policy considerations underscore why there is no duty of disclosure the SEC can cite as the basis for its claims: the disclosures it suggests would help only hackers, not investors.[6]

---

[5] Further, the SEC's allegation that SolarWinds should have disclosed it faced an "increasing" risk of attack ignores that it specifically disclosed that "[t]he risk of a security breach . . . *has generally increased*" as "the number, intensity and sophistication of attempted attacks, and intrusions from around the world *have increased*." ¶ 131 (emphasis added). Whatever difference the SEC might perceive between this disclosure and its preferred wording is too trivial to be material.

[6] The SEC's allegations about the risk factors independently fail as to Mr. Brown because he did not "make" those statements, *Janus Capital Group, Inc. v. First Derivative Traders*, 564 U.S. 135, 142 (2011); *S.E.C. v. Kelly*, 817 F. Supp. 3d 340, 343–46 (S.D.N.Y. 2011), nor is he alleged to have disseminated them, *Lorenzo v. S.E.C.*, 139 S. Ct. 1094, 1101 (2019); *Rio Tinto*, 41 F.4th at 54. The Complaint does not allege Mr. Brown even read the disclosures, much less approved them.

2. The SUNBURST Disclosure Was Not Materially Misleading

The SEC also challenges SolarWinds' initial Form 8-K about SUNBURST, but its criticism amounts to more nitpicking that fails to plausibly allege any materially misleading statement.

First, the SEC critiques SolarWinds' statement that SUNBURST "could potentially allow an attacker to compromise the server on which the Orion products run," asserting that it should have said the vulnerability "definitively allowed" an attacker to compromise a customer's Orion server. ¶ 187. However, the statement in the 8-K was indisputably true—SUNBURST *could* allow an attacker to compromise a customer's Orion server—and the SEC alleges no facts that would render it misleading. To the contrary, the Complaint acknowledges that SUNBURST merely provided a "*backdoor* into the network environments of SolarWinds' customers who downloaded and installed the infected versions of the software to systems that were *connected to the internet*." ¶ 143 (emphasis added). The presence of this downloaded backdoor on a customer's Orion server did not mean it would—or even could—actually be utilized by the attacker. If the server were not, at a minimum, "connected to the internet," the attacker would not be able to access the server at all, including the backdoor on it.[7] Further, even if a customer's Orion server were connected to the internet, the customer could have controls in place capable of blocking the attacker from accessing it—such as a firewall only allowing connections to the server from whitelisted IP addresses. Given these possible scenarios, the statement that SUNBURST "could potentially" allow an Orion server to be compromised cannot be considered misleading, and the SEC's preference for starker (and in fact inaccurate) language cannot serve as a basis for liability. *See Singh v. Schikan*, 106 F. Supp.

[7] Nor does the Complaint allege Orion must run on an internet-connected server. *See id; see also* SolarWinds, *FAQ: Security Advisory*, at Question 2, https://www.solarwinds.com/sa-overview/securityadvisory/faq#question2 (last updated Apr. 6, 2021) ("The Orion Platform is fully functional without an internet connection.").

3d 439, 448 (S.D.N.Y. 2015) ("[C]ompanies need not depict facts in a negative or pejorative light or draw negative inferences to have made adequate disclosures.").

Second, the SEC faults SolarWinds for two statements in the 8-K asserting that the Company was "still investigating" whether SUNBURST was successfully "exploited" as "a point of any infiltration of any customer systems." ¶¶ 188-89. The SEC contends these statements were false because, as of the filing of the 8-K, Mr. Brown allegedly had mentally "linked" two earlier-reported customer incidents to the customer report that SolarWinds received about SUNBURST.[8] ¶ 184. However, there is no contradiction between this allegation and the challenged statement.

To begin with, the SEC fails to allege facts sufficient to show that, in "linking" the earlier customer reports to the customer report identifying SUNBURST, Mr. Brown had concluded that SUNBURST was successfully "exploited" as a point of "infiltration" of any of these customers. The SEC glosses over a key distinction: again, SUNBURST could be present as a backdoor on a customer system without being successfully exploited to infiltrate the customer's network. As the Complaint notes, the threat actor "utilized" SUNBURST to conduct attacks only "on approximately 100 of the 18,000" customers who downloaded the vulnerability. ¶ 143. The SEC makes no specific allegations that the threat actor *exploited* SUNBURST in this way to *infiltrate* any customers who previously reported suspicious activity to SolarWinds—much less that Mr. Brown *knew* this by the time of the 8-K.[9] The SEC claims only that Mr. Brown "linked" the earlier

---

[8] The SEC states that "SolarWinds knew the vulnerability in the Orion products had been successfully exploited on at least three prior occasions," ¶ 189, but the only factual support for this otherwise conclusory allegation is the allegation that Mr. Brown, specifically, had linked two earlier-reported customer incidents to the customer report about SUNBURST that SolarWinds received on December 12, 2020, *see* ¶¶184, 190.

[9] Similarly, the SEC alleges no facts implying that the suspicious activity reported by the customers necessarily indicated the exploitation of the backdoor, as opposed to the mere presence of it on the customers' systems. As the federal government has noted, the backdoor would independently

incidents to "*the malicious code* provided by [the cybersecurity firm that discovered SUNBURST] in December," ¶ 184—i.e., that he linked the incidents to the *backdoor itself*. That does not imply he had concluded the backdoor had been "exploited" to "infiltrate" those customers—which means something different. Indeed, the customer involved in one of the earlier-reported incidents, Palo Alto Networks, itself publicly stated after SUNBURST was discovered that its security controls had "successfully prevent[ed]" the "compromise" of its network by the threat actor,[10] underscoring the distinction between having the backdoor on one's system and being "exploited" or "infiltrated" through it. In light of that distinction, the SEC cannot claim that SolarWinds' use of these terms was misleading. *See Wochos v. Tesla, Inc.*, 985 F.3d 1180, 1194 (9th Cir. 2021) (no misrepresentation where complaint failed "to plead sufficient facts to establish that the actual term used had the distinctive, and false, meaning that Plaintiffs claim"); *Rombach*, 355 F.3d at 174 (complaint must "demonstrate with specificity why and how" the statements were misleading).

In any event, whatever Mr. Brown's understanding was at the time of the 8-K regarding whether any customers had been exploited and infiltrated via SUNBURST, it does not imply that *the Company* was not continuing to investigate the matter. After all, the 8-K was filed *the first business day* after the Company learned about SUNBURST. ¶¶ 185-86. Whatever suspicions any individual employees might have had that initial weekend when the 8-K was prepared—at which point the Company obviously would have been scrambling to respond to SUNBURST's discovery and focused on remediating the vulnerability—SolarWinds was entitled, and would be expected, to conduct a more thorough and formal investigation before reaching any definitive conclusions.

---

generate activity on a victim's system, regardless of any exploitation, including beaconing out to the threat actor's infrastructure to signal that it was present on the system. *See* GAO Report at 14–16 & fig. 2.

[10] Palo Alto Networks, *Rapid Response: Navigating the SolarStorm Attack* (Dec. 17, 2020), https://www.paloaltonetworks.com/blog/2020/12/solarwinds-statement-solarstorm.

As the 8-K asserted (and as the SEC does not question), upon learning of SUNBURST, the Company immediately "retained third-party cybersecurity experts to assist in an investigation of these matters." ¶ 188; Ex. 2, at 3. That investigation would barely have had time to get off the ground when the 8-K was issued. The Complaint thus cannot plausibly allege that SolarWinds and its third-party experts were *not* "still investigating" whether and to what extent any customers were successfully infiltrated; and Mr. Brown's alleged beliefs about a "link[]," ¶ 184, hardly preclude that possibility. *See In re DraftKings Inc. Sec. Litig.*, 650 F. Supp. 3d 120, 169–71 (S.D.N.Y. 2023) (Engelmayer, J.) (dismissing claim for failure to allege specific facts making statement false); *Gillis*, 197 F. Supp. 3d at 597 (dismissing claim where "the information which the [complaint] faults defendants for omitting does not contradict the[ir] statements").

More fundamentally, the SEC does not plausibly explain why either supposed misstatement—that SUNBURST "could allow" an attacker to compromise a customer's Orion server, or that SolarWinds was "still investigating" whether and to what extent any exploitation had occurred—is material. The SEC asserts that the 8-K "failed to disclose . . . the true impact of SUNBURST," ¶ 190, but the 8-K plainly disclosed the seriousness of the incident. It explained that: (i) a vulnerability had been inserted into Orion, likely "by an outside nation state" as part of a "highly sophisticated . . . supply chain attack"; (ii) the vulnerability had been live since March 2020, meaning the attacker had had nine months to exploit it; (iii) *as many as 18,000* SolarWinds customers had downloaded the infected software; (iv) revenue from Orion represented 45 percent of total corporate revenue; and (v) there were "numerous financial, legal, reputational and other risks to SolarWinds related to the security incidents," which the disclosure enumerated. Ex. 2, at 3. Moreover, far from suggesting the threat of customer compromise was merely "theoretical," ¶ 187, the 8-K specifically noted there had been "significant media coverage of attacks on U.S.

governmental agencies and other companies, with many of those reports attributing those attacks to a vulnerability in the Orion products," Ex. 2, at 3.

Against these sobering disclosures, the alleged omission—that a mere *two* of the 18,000 potentially affected customers had previously reported incidents linked to SUNBURST—was insignificant. The disclosure that up to 18,000 customers were at risk of compromise was far more revealing of the scope of the incident. Indeed, this outer-bound figure vastly *overstated* the effect of the incident, as the number of customers compromised in fact turned out to be much smaller, on the order of 100. ¶ 143. In short, the alleged omissions would not have significantly altered the total mix of information, which already made clear that SUNBURST was a serious incident that exposed many customers to potential compromise by a sophisticated nation-state actor. *See In re Citigroup, Inc. Sec. Litig.*, 330 F. Supp. 2d 367, 378 (S.D.N.Y. 2004) (dismissing claim where omission was not "material in the context of [defendant]'s overall business"), *aff'd sub nom. Albert Fadem Tr. v. Citigroup, Inc.*, 165 F. App'x 928 (2d Cir. 2006); *cf. Beleson v. Schwartz*, 419 F. App'x 38, 40 (2d Cir. 2011) (fact of impending bankruptcy immaterial given disclosure that company had lost over $500 million, which "adequately informed [investors] of the dire nature of [its] financial condition"). The fact that SolarWinds' stock price lost nearly a quarter of its value in the wake of the initial 8-K, ¶ 193, only confirms that it made the gravity of the situation clear. By comparison, when the Company disclosed the two prior customer reports in its January 8-K a few weeks later, the stock price barely moved, and even rose in the following days. *See* Ex. 6.

3. The Security Policy Statements Were Not Materially Misleading

Lacking any basis to allege that SolarWinds' statements directed *to investors* were materially misleading, the SEC tries to scrounge up fodder for its Complaint elsewhere, citing various statements about SolarWinds' security policies directed *to customers*—in a podcast, a blog post, press releases, and a "Security Statement," Ex. 5, and related webpages—which it alleges

misrepresented the quality of the Company's cybersecurity, ¶ 125.[11] To be clear, SolarWinds had a robust cybersecurity program and categorically disputes all of the SEC's assertions otherwise. However, for purposes of this motion, SolarWinds' overall cybersecurity posture is not at issue. The question is whether the particular policy statements the SEC cites are adequately alleged to be materially misleading. They are not, for several reasons.

First, many of the challenged statements are quintessential puffery that cannot ground a securities violation. All the statements cited from press releases, blog posts, and podcasts fit this mold, such as statements that SolarWinds was "focused on heavy-duty hygiene," ¶ 114, "places a premium on the security of its products and makes sure everything is backed by sound security processes, procedures and standards," ¶ 115, and has a "commitment to high security standards," ¶ 117. These statements "were merely generalizations regarding [SolarWinds'] business practices" and "are precisely the type of 'puffery' that" the Second Circuit has "consistently held to be inactionable." *ECA & Loc. 134 IBEW Joint Pension Tr. Of Chi. v. JP Morgan Chase Co.*, 553 F.3d 187, 205–06 (2d Cir. 2009) (affirming dismissal of claims based on statements that company was "highly disciplined" and "'set the standard' for 'integrity'"); *see Lopez v. CTPartners Exec. Search Inc.*, 173 F. Supp. 3d 12, 30 (S.D.N.Y. 2016) (Engelmayer, J.) (general statements about "culture, reputation, and compliance" unactionable); *In re Intel*, 2019 WL 1427660, at *8 ("Qualitative buzzwords . . . cannot form the basis of a false or misleading statement.").

Likewise, the high-level policies the SEC cites from the Security Statement—such as the statement that SolarWinds "follow[s] a defined methodology for developing secure software that

[11] The Complaint is devoid of any facts that indicate these customer-directed statements were material to investors. Rather, the SEC merely alleges that securities analysts who followed SolarWinds "considered the opinions of customers regarding SolarWinds products," ¶ 43, but fails to allege that any analyst considered any customer opinion regarding SolarWinds' security practices, let alone any opinions based on any SolarWinds statement challenged in the Complaint.

is designed to increase the resiliency and trustworthiness of our products," or that SolarWinds "follows the NIST Cybersecurity Framework with layered security controls"—are also "the kind of generic immaterial statements that the Second Circuit has consistently concluded cannot sustain a [fraud] claim at the motion to dismiss stage." *Arora v. HDFC Bank Ltd.*, 2023 WL 3179533, at *6 (E.D.N.Y. May 1, 2023) (finding statements that company had whistleblower and fraud-monitoring policies unactionable); *see also Plumber & Steamfitters Loc. 773 Pension Fund v. Danske Bank A/S*, 11 F.4th 90, 103 (2d Cir. 2021) (finding statement that defendant "takes the steps necessary to comply with internationally recognized standards, including Know Your Customer procedures" unactionable); *Ong*, 294 F. Supp. 3d at 232 (finding statement that company's "quality assurance department establishes and monitors our quality and food safety programs for our supply chain" unactionable). "The statements are too general to cause a reasonable investor to rely upon them," as they "did not, and could not, amount to a guarantee" that the Company would "prevent failures in its . . . practices." *ECA*, 553 F.3d at 206.

The SEC also fails to adequately allege that any of the representations in the Security Statement were false. It tries to manufacture falsity by citing internal SolarWinds documents it claims to reflect security deficiencies. But the SEC repeatedly mischaracterizes these documents; and in any event none of the documents show, as they must to imply falsity, that SolarWinds lacked any specific policy outlined in the Security Statement. In particular:

NIST Cybersecurity Framework: The SEC challenges the statement that SolarWinds "follows the NIST Cybersecurity Framework" ("NIST CSF"), ¶ 47, but it never alleges facts showing that SolarWinds did *not* follow the NIST CSF. Indeed, the SEC specifically acknowledges that SolarWinds "use[d] the NIST Framework . . . to conduct assessments" of its cybersecurity practices, ¶ 197—which is one way to "follow" a framework. The SEC alleges that SolarWinds

evaluated itself poorly under the NIST CSF, but the cited evaluations concern a different NIST publication—Special Publication 800-53—about which the Security Statement made no representations at all. ¶¶ 50-51 (citing evaluations of "NIST 800-53 controls").[12] In any event, the Security Statement did not say anything about what scores the Company gave itself under the NIST CSF; nor does the SEC allege that "following" the NIST CSF requires meeting any particular scores. The NIST CSF itself states that it is a "voluntary" and "flexible" framework that companies use "to help them identify, assess, and manage cyber risks"—and that it is *not* "a one-size-fits-all approach" with specific mandates or minimum requirements.[13] Because the reference to NIST CSF in the Security Statement "made no characterization at all with respect to the quality" of SolarWinds' controls, any purported low scores do not make the representation misleading. *In re Marriott Int'l, Inc.*, 31 F.4th 898, 903 (4th Cir. 2022).

Secure Development Lifecycle: The SEC asserts that "SolarWinds failed to follow an SDL [secure development lifecycle] throughout the Relevant Period," ¶ 61, but it alleges no facts sufficient to support that assertion. Instead, the SEC cites two emails from *before* the Relevant Period, prior to the Company's October 2018 IPO, reflecting that an engineering manager was "working with teams throughout 2018 to begin incorporating the SDL into their development lifecycle." ¶ 62; *see* ¶ 64. These emails indicate only that there was "improvement needed" in implementing the SDL, not that the Company had no SDL at all. But even if they did imply the lack of an SDL at the time, that would not make the Security Statement materially misleading to

---

[12] *Compare* NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, at v-vi ("NIST CSF") *with* NIST, *Special Publication 800.53, Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[13] *See* NIST CSF, *supra* note 12, at v-vi.

investors, as the Company had no public investors then who could have been misled. Nor do the emails imply that SolarWinds lacked an SDL *during* the Relevant Period; if anything, they show SolarWinds was working to ensure one was in place before it went public.

Besides these pre-Relevant Period emails, the SEC points only to documents that, at most, indicate that SolarWinds gave itself a two-out-of-five score for its SDL program in a NIST assessment at one point,[14] and that it identified certain gaps in the program on other occasions. ¶¶ 65-68. These facts do not suffice to allege falsity either. The Security Statement made no representations that SolarWinds' SDL program met a certain NIST score, or that the program would not have any gaps. Nor would a reasonable investor assume from a mere statement of policy that the policy was perfectly followed. *See In re Braskem S.A. Sec. Litig.*, 246 F. Supp. 3d 731, 756 (S.D.N.Y. 2017) (Engelmayer, J.) ("There is an important difference between a company's announcing rules forbidding bribery and its factually representing that no officer has engaged in such forbidden conduct."); *In re Constellation Energy Grp., Inc. Sec. Litig.*, 738 F. Supp. 2d 614, 631 (D. Md. 2010) (concluding that "[a] reasonable investor could not assume" from general statements about its internal controls "that the company would never lapse in these tasks").

Passwords: As to passwords, the SEC cites language from the Security Statement about the Company's password policy and "best practices," and alleges that those statements were false because "SolarWinds failed to enforce or comply with its own password policy on multiple occasions." Compl. at 23 (capitalization altered). This allegation also fails to state a securities fraud claim. The documents cited by the SEC from within the Relevant Period convey, at most, that

[14] The SEC misleadingly characterizes this score as implying simply that SolarWinds "does not routinely measure or enforce policy compliance." ¶ 65. The quoted document makes clear that a score of "2" in fact signified that "[t]he organization has a consistent overall approach to meeting the security control objectives," even if documentation and measurement were inconsistent. *See* Ex. 7. Thus, if anything, the score implies that SolarWinds *did* follow an SDL.

there was a certain "system" where passwords were not automatically required to have certain parameters, ¶ 81, and other "situations where 'password requirements were not met,'" ¶¶ 83-84.[15] Again, such alleged deficiencies do not make a policy statement "false." No reasonable investor would construe the password policy statement as "a guarantee" that the Company would "prevent failures in its . . . practices." *ECA*, 553 F.3d at 206. Indeed, the fact that the Company was identifying deficiencies confirms that it *had* a policy in place and was working to correct any deviations from it. *See Ong*, 294 F. Supp. 3d at 232 ("These allegations do not conflict with Defendants' statements regarding the food-safety programs and procedures that Chipotle had in place, but merely quibble with Chipotle's execution of those programs and procedures.").

Access Controls: The SEC asserts that the Security Statement "falsely claimed that the Company maintained strong access controls," but it again fails to allege specific facts that would render any specific representations about access controls in the Security Statement misleading to investors. ¶¶ 88-112. The SEC again relies significantly on documents predating the Relevant Period. ¶¶ 94-96. Otherwise, the SEC cites a NIST self-assessment in which the Company found a "need to improve" its processes and procedures relating to access controls, ¶ 97, and an email and attachment allegedly reflecting deficiencies found for a particular "system,"[16] ¶ 99. Again,

---

[15] The SEC mischaracterizes these documents, including a September 2019 email, ¶ 81, which it portrays as relating to the Company's "network authentication system." The Complaint makes clear in a subsequent allegation regarding the same email that it instead related to a SolarWinds *software product*—not the Company's *network*. ¶ 99 (referencing "controls for the product"). The SEC also cites an assessment done under a set of federal standards known as "FedRAMP," ¶ 82, but it does not explain what aspect of the Company's operations the assessment concerned, or how it contradicts anything in the Security Statement, which does not say anything about whether the Company's password controls met any FedRAMP standards.

[16] The email is the same email cited as part of the SEC's password allegations, which the SEC again misleadingly characterizes as relating to a SolarWinds "system," while only later in the paragraph acknowledging that it in fact relates to a SolarWinds "product." ¶ 99. The SEC also again cites a "FedRAMP" assessment, ¶ 98, without explaining what it specifically concerns or how it contradicts any specific representation in the Security Statement about access controls.

policy gaps do not mean that no policy exists. The SEC does not even explain how the deficiencies identified in the cited documents relate to any of the representations about access controls in the Security Statement. For example, the SEC cites a vague notation about access to critical systems being "inappropriate," ¶ 97, but does not explain what this issue was. Similarly, the SEC tacks on allegations about a purported "security gap" relating to the Company's VPN configuration, ¶¶ 102-111, but the Security Statement said nothing about the Company's VPN, *see* Ex. 5.

* * *

Ultimately, the Court need not delve into these details, because whatever representations the Security Statement made to customers about SolarWinds' security measures, the Company's risk factor disclosures render those representations immaterial. As the disclosures stated, "unauthorized access to, or security breaches of, our software or systems," and the various material consequences accompanying such an incident, could occur "*[d]espite* our security measures." Ex. 1, at 3 (emphasis added). The disclosures thus specifically warned investors that they could not rely on the Company's security measures—whatever they might be—to protect against the risks associated with a cyberattack. *See In re Marriott*, 31 F.4th at 903 (rejecting claim based on website's representations about data-privacy protections because "Marriott's risk disclosures to the SEC—the content actually directed to investors—specifically warned that the company's systems 'may not be [sufficient]'"); *In re Intel*, 2019 WL 1427660, at *11 (rejecting claim based on statements touting security features given, inter alia, "the risk warnings about security vulnerabilities in Intel's SEC filings"); *In re Heartland Payment Sys., Inc. Sec. Litig.*, 2009 WL 4798148, at *5 (D.N.J. Dec. 7, 2009) (rejecting claim based on statement emphasizing company's "high level of security," given that "the cautionary statements in the Form 10–K—warning of the

possibility of a breach and the consequences of such a breach—make clear that Heartland was not claiming that its security system was invulnerable").

B. The Complaint Fails to Allege a Strong Inference of Scienter

The SEC's fraud claims are independently subject to dismissal because they fail to raise a "strong inference of scienter," meaning "an intent to deceive the investing public." *Acito v. Imcera Grp., Inc.*, 47 F.3d 47, 54 (2d Cir. 1995). To meet this burden, the SEC must allege "facts to show either (1) that defendants had the motive and opportunity to commit fraud, or (2) strong circumstantial evidence of conscious misbehavior or recklessness." *ECA*, 553 F.3d at 198.

The only motive the SEC offers—"to obtain and retain business," ¶ 42—fails as a matter of law because it can be imputed to "virtually every company," *Acito*, 47 F.3d at 54, and identifies no "concrete and personal way" in which the alleged fraud would benefit Mr. Brown or any SolarWinds executives, *Novak*, 216 F.3d at 307.[17] Where, as here, "motive is not apparent . . . the strength of the circumstantial allegations [of conscious misbehavior or recklessness] must be correspondingly greater." *Kalnit v. Eichler*, 264 F.3d 131, 142 (2d Cir. 2001). And recklessness here means "conscious recklessness—*i.e.*, a state of mind *approximating actual intent*, and *not merely a heightened form of negligence*." *S. Cherry St., LLC v. Hennessee Grp. LLC*, 573 F.3d 98, 109 (2d Cir. 2009). The Complaint alleges no facts that would support any such strong inference.

[17] If the SEC seeks to establish motive based on Mr. Brown's stock sales during the Relevant Period, *see* ¶ 33, those allegations are also insufficient. Alleged trading does not support an inference of scienter unless the activity is "unusual." *Ark. Pub. Emps. Ret. Sys. v. Bristol-Myers Squibb Co.*, 28 F.4th 343, 355 (2d Cir. 2022). That depends, in turn, on the resulting profits, the portion of holdings involved, any change of volume in sales, the amount of insiders selling, and the timing of the sales. *See In re Aratana Therapeutics Inc. Sec. Litig.*, 315 F. Supp. 3d 737, 762 (S.D.N.Y. 2018) (Engelmayer, J.). The SEC alleges no such factors here, instead only alleging the gross proceeds Mr. Brown received—which is insufficient. *See In re Skechers USA, Inc. Sec. Litig.*, 444 F. Supp. 3d 498, 525 (S.D.N.Y. 2020) (holding that it is not enough to "only recite the amount of proceeds [defendant] obtained, which by itself says 'nothing about his motive'").

1. The Risk Factor Allegations Do Not Support Scienter

Putting aside that the risk factors were entirely accurate, the SEC fails to adequately allege scienter on behalf of anyone involved in making them. The disclosures were made by "the Company's CEO and CFO," ¶ 130; no one else (including Mr. Brown) is alleged to have had any role in formulating or approving them. Yet the SEC pleads almost nothing about SolarWinds' CEO or CFO—certainly nothing suggesting scienter.

The *only* allegation about the CFO is that he signed the risk factor disclosure, which is not enough. "[I]t is 'well established that a defendant's position does not, without more, support a conclusion that the defendant had access to information contradicting an alleged misrepresentation.'" *In re DraftKings*, 650 F. Supp. 3d at 178. As for the CEO, the Complaint alleges just two things: (1) he was "updated" by executives who saw a presentation, ¶¶ 84, 100, and he "received" another presentation, ¶ 97, mentioning alleged deficiencies in access and password controls; and (2) another executive once told him "[u]ndersized staff" was a "key risk," ¶ 159. These allegations do not suggest the CEO had reason to know the risk factors were "false," let alone that he intended for them to deceive investors. There is an obvious benign explanation for why the CEO would approve the risk factors, even if he had learned of certain deficiencies: he could have believed in good faith that, whatever deficiencies had been identified, the disclosures were sufficient because they disclosed that Company's systems were "vulnerable" to cyberattack "despite our security measures." *See In re Centerline Holdings Co. Sec. Litig.*, 613 F. Supp. 2d 394, 404 (S.D.N.Y. 2009) (no strong inference where it was "arguable that [defendants] did not have a duty to disclose" omitted information), *aff'd*, 380 F. App'x 91 (2d Cir. 2010).[18]

[18] Nor does the SEC add anything by alleging that "SolarWinds executives could have reasonably anticipated that SolarWinds would be subject to a material cyberattack." ¶ 129. If that is not an impermissible "fraud by hindsight" theory, it is hard to imagine what would be. *Novak*, 216 F.3d

Rather than allege scienter by the officials who made the disclosure statements, the SEC variously tries to allege scienter on the part of a "member of SolarWinds' sales team," ¶ 166, "SolarWinds and Mr. Brown," ¶¶ 161, 164, 177, Mr. Brown alone, ¶¶ 175, 180, or just "SolarWinds employees . . . collectively," ¶¶ 181, 192. But this mix-and-match strategy fails because it does not suggest that anyone *who made the disclosure statements* did so recklessly or with intent to defraud investors. "[I]t is not enough to *separately* allege misstatements by some individuals and knowledge belonging to some others where there is no strong inference that, in fact, there was a connection between the two." *Silvercreek Mgmt., Inc. v. Citigroup, Inc.*, 248 F. Supp. 3d 428, 440 (S.D.N.Y. 2017); *Nordstrom, Inc. v. Chubb & Son, Inc.*, 54 F.3d 1424, 1435 (9th Cir. 1995) ("[T]here is no case law supporting an independent 'collective scienter' theory.").[19]

The allegations about individuals other than the CEO and CFO also fail because they do not support an inference of scienter on behalf of these non-speakers themselves. The Complaint alleges that Mr. Brown and other SolarWinds employees "knew about the extensive risks and vulnerabilities to SolarWinds' Orion platform," ¶ 167, but this allegation cannot show that those employees knew (or were reckless or negligent in not knowing) that the cybersecurity risk disclosures were misleading—particularly given that the employees had no alleged role in drafting the disclosures, and the disclosures already warned that SolarWinds' systems were "vulnerable"

---

at 309 ("[A]llegations that defendants should have anticipated future events and made certain disclosures earlier than they actually did do not suffice to make out a claim of securities fraud.").

[19] The SEC also nominally asserts fraud on a theory of scheme liability. ¶¶ 204(a), 211(a). But scheme liability requires allegations of deceptive conduct "*beyond* misstatements and omissions," *S.E.C. v. Rio Tinto plc*, 41 F.4th 47, 49 (2d Cir. 2022), such as "sham agreements, sham transactions, sham companies, or undisclosed payments," *In re Turquoise Hill Res. Ltd. Sec. Litig.*, 625 F. Supp. 3d 164, 253 (S.D.N.Y. 2022). The SEC alleges no such thing here. Its contention that SolarWinds "disseminated" its statements to customers, ¶¶ 39, 42, 115-17, is insufficient because the dissemination here is not meaningfully distinct from making the statements themselves. *See In re Turquoise Hill*, 625 F. Supp. 3d at 248; *Menaldi v. Och-Ziff Cap. Mgmt. Grp. LLC*, 277 F. Supp. 3d 500, 519–20 (S.D.N.Y. 2017) (plaintiff cannot merely "repackage the misrepresentation allegations" as the basis for the alleged scheme).

to attack. Any allegation of scienter is distinctly misplaced as to Mr. Brown, who is specifically alleged to have "routinely shared" presentations about cybersecurity risks with senior executives, ¶ 84, which is incompatible with any intent to hide such risks. Notably, despite years of investigation, the SEC identifies just one tangential statement that could suggest some sort of dishonesty: during a call with a customer, an unnamed "Employee F" allegedly messaged a colleague that he "just lied." ¶ 162. Putting aside that this allegation says nothing about Mr. Brown, SolarWinds, *or* the challenged risk factors, Employee F's alleged misrepresentation *to a customer* "cannot be conflated with an intent to defraud the shareholders." *Kalnit*, 264 F.3d at 141.

2. The SUNBURST Disclosure Allegations Do Not Support Scienter

The Complaint does not support a strong inference of scienter for the SUNBURST disclosure either. Even accepting the SEC's allegation that Mr. Brown immediately "linked" certain customer reports to SUNBURST, that does not raise a strong inference that Mr. Brown or SolarWinds sought to hide "the true impact of SUNBURST" from investors. Rather, the only plausible inference is that SolarWinds did not disclose the allegedly omitted information "because it was investigating the extent of the problem." *In re NVIDIA Corp. Sec. Litig.*, 768 F.3d 1046, 1065 (9th Cir. 2014); *see also Iqbal*, 556 U.S. at 680 (unlawful motive not plausibly alleged where it is merely "consistent" with facts "more likely explained by[] lawful . . . behavior").

As noted above, whatever Mr. Brown might have personally and preliminarily suspected about whether and how SUNBURST was linked to any customer reports, the Company had only learned of SUNBURST a mere two days before filing the initial 8-K; and it was reasonable for it to conduct further investigation, assisted by an outside forensics firm, before drawing any firm conclusions about such an issue. After all, it would not benefit investors to "jump the gun with half-formed stories." *Higginbotham v. Baxter Int'l, Inc.*, 495 F.3d 753, 761 (7th Cir. 2007). The 8-K itself said exactly that: "So as not to compromise the integrity of any investigations,

SolarWinds is unable to share additional information at this time." Ex. 2, at 4. A company intending to deceive investors would not *tell them* it was withholding information. The plausible inference instead is that—just as the 8-K said—the Company was "still investigating" the issue (among many others), and simply needed more time to conduct that investigation. *See Slayton v. Am. Exp. Co.*, 604 F.3d 758, 777 (2d Cir. 2010) ("Ordering an investigation as soon as [defendants] learned [of the issue], and directing [management] to use conservative assumptions, was a prudent course of action that weakens rather than strengthens an inference of scienter." (quotation marks omitted)); *In re Pretium Res. Inc. Sec. Litig.*, 256 F. Supp. 3d 459, 479 (S.D.N.Y. 2017) (similar).

This benign explanation is confirmed by the follow-up disclosure SolarWinds made only weeks later—tellingly unmentioned in the Complaint—which specifically disclosed the very "link" the SEC alleges SolarWinds sought to hide. That January 2021 8-K disclosed that SolarWinds had "identified two previous customer support incidents that, with the benefit of hindsight, we believe may be related to SUNBURST." Ex. 4, at 5. The SEC evidently recognizes that this disclosure runs counter to its fraud allegations, which is why it takes the position that the disclosure "ends the alleged scheme." Hr'g Tr. 4:21–5:8 (explaining that "at that point that is sort of enough that is revealed that the SEC is no longer alleging that the scheme continued after that point"). But the idea that SolarWinds engaged in a "scheme" to conceal information only to reveal it a few weeks later is, of course, absurd. The only plausible inference is that there was never any "scheme" to begin with. *See Gregory v. ProNAi Therapeutics Inc.*, 297 F. Supp. 3d 372, 402 n.13 (S.D.N.Y. 2018) (Engelmayer, J.) (allegation that company failed to disclose drug trial results "earlier than it did" could not form basis for scienter).

Other considerations also undermine any inference of scienter: SolarWinds disclosed the attack the first trading day after learning about it, reported the maximum number of customers

possibly affected, noted the importance of Orion to the business, and flagged the "numerous financial, legal, reputational and other risks to SolarWinds" emanating from the attack. These are not the acts of a company behaving recklessly or seeking to cover up bad facts, *see Rombach*, 355 F.3d at 176–77 (proactive disclosure weakened inference of recklessness), and it is not remotely plausible that SolarWinds would embark on a scheme to lie to investors while making such disclosures, *see In re Bausch & Lomb, Inc. Sec. Litig.*, 592 F. Supp. 2d 323, 343 (W.D.N.Y. 2008) (rejecting scienter where company "immediately launched a massive independent investigation" and "voluntarily reported the matter"). Courts regularly "refuse to infer scienter, even on a recklessness theory, when confronted with [such] illogical allegations." *In re GeoPharma, Inc. Sec. Litig.*, 411 F. Supp. 2d 434, 446 n.83 (S.D.N.Y. 2006) (collecting cases).

3. The Security Policy Statements Do Not Support Scienter

Finally, the Complaint does not support a strong inference that SolarWinds or Mr. Brown sought to deceive investors through statements to customers about SolarWinds' security policies.

The SEC's only specific scienter allegation as to these statements is wholly unpersuasive: the SEC cites an email (mentioned above) that flagged there was "improvement needed" on implementing the Company's SDL policy and stated that "[w]e will be working with teams throughout 2018 to begin incorporating the SDL into their development lifecycle." ¶ 8.a. The SEC seizes on this email as if it were some kind of smoking gun, straining to characterize it as evidence of a "scheme" to "conceal the present falsity of the representations [in the Security Statement's SDL section] and work toward making them true eventually." *Id.* But the email is from January 2018—ten months before the Company's IPO—when the Company had no public investors who could have been deceived in the first place. And it was sent by an unnamed engineer not alleged to have made the representations in the Security Statement, whose intent cannot be imputed to SolarWinds or Mr. Brown. *See Silvercreek*, 248 F. Supp. 3d at 440. Most importantly, the SEC

ignores that the email reflects an effort to *ensure that SolarWinds' stated policy was being fully followed*—the very opposite of an intent to deceive. That is why the SEC's assertion that the email "reflects a culture of recklessness, negligence, and scienter," ¶ 63, is not only baseless, but backwards: part of *having* a policy involves using it to identify and correct gaps in compliance. That process is a hallmark of a culture *of security*, rather than any nefarious "scheme." *See Yates v. Mun. Mortg. & Equity, LLC*, 744 F.3d 874, 887–89 (4th Cir. 2014) (frequent meetings to review problems was "a sign of diligence rather than evidence of a nefarious purpose"); *In re Wachovia Equity Sec. Litig.*, 753 F. Supp. 2d 326, 363 (S.D.N.Y. 2011) (no scienter based on internal policy violations where no evidence they were "knowingly sanctioned" or the product of "recklessness").

The same goes for other allegations relating to the Security Statement. The allegations do not support a strong inference that anyone—let alone Mr. Brown or someone whose intent could be imputed to SolarWinds as a whole—believed the assertions in the Security Statement to be false. At most, the documents cited by the SEC simply reflect employees identifying areas where stated policies could be improved. That is a far cry from believing that a "policy was never followed" at all. *Lewy v. SkyPeople Fruit Juice, Inc.*, 2012 WL 3957916, at *20 (S.D.N.Y. Sept. 10, 2012). It cannot be the law that, every time a public company identifies a gap in a stated policy, it is liable for securities fraud. Policies are not guarantees of perfect compliance. No reasonable person would interpret them that way, and there is no reason to believe anyone at SolarWinds intended them that way. *See Retail Wholesale & Dep't Store Union Local 338 Ret. Fund v. Hewlett–Packard Co.*, 52 F. Supp. 3d 961, 970 (N.D. Cal. 2014) ("[I]t simply cannot be that every time a violation of [ethics] code occurs, a company is liable under federal law for having chosen to adopt the code at all."); *see also In re Poseidon Concepts Sec. Litig.*, 2016 WL 3017395, at *15

(S.D.N.Y. May 24, 2016) (no scienter where auditing deficiencies did "not suggest the existence of an audit that was 'so deficient as to amount to no audit at all'").[20]

II. The Disclosure Controls Claim Should Be Dismissed

The SEC's perfunctory attempt to allege a disclosure control claim is meritless. Exchange Act Rule 13a-15(a) requires a company to have "disclosure controls and procedures" that are "designed to ensure that information required to be disclosed by the issuer" is accurately and timely disclosed. 17 C.F.R. § 240.13a–15(e). The SEC's theory seems to be that there *must have been* a disclosure controls violation because certain "issues"—including the alleged "VPN vulnerability" and the earlier-reported customer incidents that Mr. Brown allegedly later linked to SUNBURST—"went unreported." ¶ 202.[21] These allegations fail to state a claim.

As an initial matter, disclosure controls apply only to issues that are "required to be disclosed." 17 C.F.R. § 240.13a–15(e). SolarWinds did not have to disclose information about its VPN configuration, as explained above in Section I.A.1. And the information about the two customers impacted by SUNBURST, though also not *required* to be disclosed, *see supra*, Section I.A.2, *was* disclosed once the Company had the chance to conduct further investigation after learning of SUNBURST. Accordingly, neither issue could ground any disclosure violation.

More fundamentally, the SEC's theory fails because it misunderstands the elements required to establish a disclosure controls violation. Rule 13a–15 requires only that companies

---

[20] The SEC fails to adequately plead negligence for similar reasons it fails to plead scienter: the makers of the statements had no reason to believe the statements were incorrect. The SEC also cannot plausibly allege that the Company or Mr. Brown deviated from the standard of care in light of SolarWinds' robust disclosures and efforts to enforce security policies. *See Zappia v. Myovant Scis. Ltd.*, 2023 WL 8945267, at *6 (S.D.N.Y. Dec. 28, 2023) (dismissing securities claim under *Iqbal* for failing to plausibly allege "negligent[] rather than accidental[] or reasonabl[e]" conduct).

[21] The SEC also references "the fact that the vulnerability inserted by the attackers had been previously exploited on multiple occasions" as a separate "issue," but this is merely an indirect reference to the previously reported customer incidents.

maintain controls "*designed* to ensure that information required to be disclosed" is timely reported. 17 C.F.R. § 240.13a–15 (emphasis added). Disclosure controls need not be perfectly effective, and individual failures to disclose do not by themselves evidence unreasonable design. *See Arora*, 2023 WL 3179533, at *7 (allegations that internal controls "did not prevent or detect the [alleged] scheme" were insufficient to support claim that controls were falsely certified to be effective); *In re Banco Bradesco S.A. Sec. Litig.*, 277 F. Supp. 3d 600, 648 (S.D.N.Y. 2017) ("[A]llegations that those controls must have been deficient because they may have failed to detect some weaknesses in its financial reports or disclosures in some instances, are not sufficient.").

The SEC does not plausibly allege any factual basis to conclude that SolarWinds' disclosure controls were unreasonably designed. The SEC acknowledges that SolarWinds *had* disclosure controls in place, including an Incident Response Plan ("IRP") with parameters for escalating potentially material incidents. ¶ 202. The SEC's only attempt to identify a defect in the design of these controls is its allegation that the IRP required escalation only of "incidents that impacted multiple customers." *Id.* But that allegation is flatly rebutted by the IRP itself, which makes clear that impact on multiple customers was simply one escalation criterion—not the *only* one.[22] Nor does the SEC explain why this criterion is supposed to be unreasonable; obviously not *every* customer incident can be escalated to management, especially in a company like SolarWinds, which has hundreds of thousands of customers. Absent some explanation of what was wrong with the *design* of the Company's disclosure controls, the SEC has no basis to bring a disclosure controls claim. *See Arora*, 2023 WL 3179533, at *7 (dismissing claim based on internal controls because the allegations failed to explain "how or why they were deficient") (collecting cases);

[22] The IRP provides for escalation of not only any "compromise that affects multiple customers," but also any compromise to which "other customers are susceptible," and any compromise of "data that should be protected from general access" or "accounts with elevated privileges." Ex. 8, at 2. Employees were "encouraged to report" an even wider variety of incidents. *Id.* at 3.

Higginbotham, 495 F.3d at 760 (rejecting controls claim where plaintiff failed to point to any different controls that should have been in place that would have been cost-effective).

III. The Internal Accounting Controls Claim Should Be Dismissed

The SEC's theory on internal accounting controls claim is not only meritless, it is a bald attempt to arrogate power Congress has not granted. Section 13(b)(2)(B) of the Exchange Act is a narrow provision requiring public companies to maintain "a system of internal accounting controls." Yet the SEC seeks to recast it as a boundless mandate for it to regulate public companies' *cybersecurity* controls—even controls for detecting *bugs in software products.* Relying on a clause that requires companies to have "internal accounting controls" that reasonably safeguard "access to assets," 15 U.S.C. § 78m(b)(2)(B), the SEC contends that "SolarWinds' information technology network environment, source code, and products were among the Company's most crucial assets"—ergo, any failure to reasonably protect those "assets" from hackers constitutes an "internal accounting controls" violation. ¶ 195. This specious argument reads "accounting" right out of the statute and has no support in the text, legislative history, or caselaw.

Section 13(b)(2)(B), titled "Books, Records, and Internal Accounting," requires companies to maintain "internal accounting controls" and "books, records, and accounts" that fairly reflect their "transactions" and disposition of "assets." Specifically, it requires companies to:

> devise and maintain 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.

15 U.S.C. § 78m(b)(2)(B) (emphasis added). This text makes clear that the provision governs only internal *accounting* controls—not internal controls generally. The text equally makes clear that the "assets" it concerns are those related to *accounting*, *i.e.*, the sort of assets that would be involved in a company's transactions and appear on its balance sheet. Nothing in the text suggests that it covers *cybersecurity* controls over *information-technology* "assets" with no nexus to accounting. *See Saks v. Franklin Covey Co.*, 316 F.3d 337, 345 (2d Cir. 2003) ("The text's plain meaning can best be understood by looking to the statutory scheme as a whole and placing the particular provision within the context of that statute.").

The ordinary meaning of the text is confirmed by the legislative history. Congress introduced the "internal accounting controls" provision as part of the Foreign Corrupt Practices Act of 1977, which it enacted in response to concerns about "bribery of foreign officials by United States business interests." *United States v. Kay*, 359 F.3d 738, 746 (5th Cir. 2004). Congress's explicit purpose was "to strengthen the accuracy of the corporate books and records and the reliability of the audit process which constitute the foundations of our system of corporate disclosure," in order "to prevent the use of corporate assets for corrupt purposes" and to provide "assurance that corporate recordkeeping is honest." S. Rep. No. 95-114, at 7 (1977). Thus, the focus was on bookkeeping, not anything broader (and certainly not cybersecurity).

Indeed, the specific language of Section 13(b)(2)(B) comes from a Statement on Auditing Standards published by the American Institute of Certified Public Accountants (AICPA). *See id.* at 8 (citing AICPA Statement on Auditing Standards No. 1, 320.28 (1973) ("SAS 1")). That Statement explained that "accounting controls" are limited to "the safeguarding of assets and the reliability of financial records." SAS 1 at 320.28. It further explained that "safeguarding assets" in this context does not broadly mean protecting assets "against something undesirable," *id.* at

320.14, but rather means protecting assets against "loss"—of the sort that could cause *accounting* discrepancies, such as "understatement of sales through failure to prepare invoices," "overpayments to vendors or employees arising from inaccuracies in quantities of materials," or "physical loss of assets such as cash, securities, or inventory." *Id.* at 320.15 & 320.19; *see also In re Ikon Office Sols., Inc. Sec. Litig.*, 277 F.3d 658, 672 n.14 (3d Cir. 2002) ("'Internal accounting controls' refers to the mechanism by which companies monitor their accounting system (their individualized method of processing transactions) for errors and irregularities in order to safeguard company assets and ensure that records are sufficiently reliable.").

Section 13(b)(2)(B) thus does not authorize the SEC to bring suit based on purported "shortcomings to SolarWinds' cybersecurity controls." ¶ 198. If Congress had meant to authorize the SEC to serve as some sort of roving cybersecurity commissioner for public companies, it would have said so in plainer terms, and there would have been some discussion of it in the legislative history. Any such mandate would have sweeping implications for public companies, as well as for the SEC—which lacks the expertise or resources to perform such a role. Congress does not legislate this way; it "does not hide elephants in mouseholes by altering the fundamental details of a regulatory scheme in vague terms of ancillary provisions." *Sackett v. Env't Prot. Agency*, 598 U.S. 651, 667 (2023) (cleaned up); *see also West Virginia v. EPA*, 142 S. Ct. 2587, 2610 (2022) (courts are skeptical of "claims to discover in a long-extant statute an unheralded power representing a transformative expansion in [an agency's] regulatory authority") (cleaned up).

No court has endorsed the SEC's revisionist reading of the statute. Courts have instead uniformly dismissed Section 13(b)(2)(B) claims that are not directed at controls specifically related to *accounting*. *See, e.g.*, *S.E.C. v. Felton*, 2021 WL 2376722, at *12 (N.D. Tex. 2021) (dismissing claim because "the SEC does not identify a single internal control that governed the handling of

sales, inventory, exchanges, returns, recognition of revenue, etc." (quotation marks omitted)); *S.E.C. v. Patel*, 2009 WL 3151143, at *26 (D.N.H. 2009) (dismissing claim where allegations said "nothing about manual or automated reviews of records, methods to record transactions, reconciliation of accounting entries, or anything else that might remotely qualify as an internal accounting control"); *see also In re Equifax*, 357 F. Supp. 3d at 1230 ("Even if Equifax's data breach protocol was vastly deficient, this does not establish that it had insufficient internal controls over financial reporting."). This Court should likewise dismiss the SEC's claim here.

IV. The Aiding-and-Abetting Claims Should Be Dismissed

Finally, the SEC's aiding-and-abetting claims against Mr. Brown all fail. Liability for aiding and abetting requires the knowing or reckless provision of substantial assistance to achieve a primary violation. *S.E.C. v. Apuzzo*, 689 F.3d 204, 211 (2d Cir. 2012). The SEC fails to allege any aiding-and-abetting theory that is coherent, let alone legally sound.

The aiding-and-abetting allegations center on Mr. Brown signing certain "sub-certifications" for purposes of compliance with the Sarbanes–Oxley Act, attesting to the adequacy of certain subsets of SolarWinds' cybersecurity controls. ¶¶ 208, 215, 222, 229, 236. The theory, however, is not pled with sufficient particularity and is difficult to discern, as the SEC does not explain how signing allegedly false sub-certifications would substantially assist any alleged primary violations. To be clear, the SEC does not (and cannot) allege the sub-certifications signed by Mr. Brown were directed at or disseminated to the public. Rather, the SEC merely alleges that these *internal* attestations were "relied on" by SolarWinds executives. ¶¶ 20, 175. The theory thus seems to be that Mr. Brown substantially assisted SolarWinds executives in committing primary violations by making false statements to those executives. That is nonsense.

Substantial assistance means that the defendant "associated himself with the venture, participated in it as in something that he wished to bring about, and sought by his action to make

it succeed." *Apuzzo*, 689 F.3d at 214, 217. As to the fraud and false statement claims, the SEC does not adequately allege how Mr. Brown could have "associated himself with" and "participated in" the venture, or "sought by his action to make it succeed," by making false certifications *to his principals*. The allegation is illogical: if the executives were deceived by the certifications, that would negate any scienter on their part, so there would be no primary violation in the first place.[23] As to the disclosure controls claim, the primary violation is the alleged failure to maintain reasonably designed disclosure controls; but neither Mr. Brown's sub-certifications nor any other conduct alleged on his part concern the design of SolarWinds' disclosure controls, let alone suggest that he sought for them to be designed unreasonably. And as to the internal accounting controls claim, the Complaint does not plausibly allege that Mr. Brown signed these sub-certifications because he knew and "wished to bring about" that SolarWinds had allegedly inadequate controls. That is particularly true because the certifications were *internal*, and thus did not plausibly help conceal any inadequacies from the public. The SEC also fails to identify what controls Mr. Brown's sub-certifications covered. It only vaguely alleges that they pertained to "Security," ¶ 179, and there is thus no basis to allege that those sub-certifications somehow helped SolarWinds maintain any particular controls the SEC deems insufficient.

CONCLUSION

For all the above reasons, the Complaint should be dismissed in its entirety.

Dated: January 26, 2024

Respectfully submitted,

/s/ Serrin Turner
Serrin Turner
Nicolas Luongo

[23] There is also no plausible way to square the SEC's aiding-and-abetting theory with its repeated allegations that Mr. Brown told SolarWinds executives about cybersecurity concerns in quarterly presentations and other communications. *See* ¶ 84; *see also* ¶¶ 68, 96-97, 100, 120, 132, 150, 168-170, 172. It makes no sense that Mr. Brown would inform executives about such concerns in these communications and yet seek to deceive them in the sub-certifications that he signed.

LATHAM & WATKINS LLP
1271 Avenue of the Americas
New York, NY 10020
Telephone: (212) 906-1200
Facsimile: (212) 751-4864
serrin.turner@lw.com
nicolas.luongo@lw.com

Sean M. Berkowitz (*pro hac vice*)
Kirsten C. Lee (*pro hac vice*)
LATHAM & WATKINS LLP
330 N. Wabash, Suite 2800
Chicago, IL 60611
Telephone: (312) 876-7700
Facsimile: (617) 993-9767
sean.berkowitz@lw.com
kirsten.lee@lw.com

Michael Clemente (*pro hac vice* motion forthcoming)
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004
Telephone: (202) 637-2200
Facsimile: (202) 637-2201
michael.clemente@lw.com

Counsel for Defendants SolarWinds Corp. and Timothy G. Brown