IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

IN RE SOLARWINDS CORPORATION SECURITIES LITIGATION	§ § § § § § § §	MASTER FILE NO. 1:21-CV-138-RP

DEFENDANTS' MOTION TO DISMISS CONSOLIDATED COMPLAINT

Paul R. Bessette
Texas Bar No. 02263050
Michael J. Biles
Texas Bar No. 24008578
S. Saliya Subasinghe
Texas Bar No. 24093226
Jessica England
Texas Bar No. 24105841
KING & SPALDING LLP
500 W. 2nd Street, Suite 1800
Austin, TX 78701
Tel: (512) 457-2050
Fax: (512) 457-2100
pbessette@kslaw.com
mbiles@kslaw.com
ssubasinghe@kslaw.com
jengland@kslaw.com

Counsel for SolarWinds Corp. and Tim Brown

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION

On December 14, 2020, SolarWinds reported a cyberattack on its Orion software (the "Cyberattack"). SolarWinds later disclosed that a nation-state actor (which the U.S. Government confirmed to be the Russian Foreign Intelligence Service—the SVR[1]) injected malicious code called "Sunburst" into new releases of Orion software, which, if installed on a customer's server connected to the internet, could allow the attacker to compromise the server.[2] Investigators, government officials, and the press have uniformly characterized the Cyberattack as "the largest and most sophisticated" cyber espionage operation the world has ever seen requiring "at least a thousand very skilled, capable engineers."[3] Plaintiff's Complaint attempts to convert this sophisticated cyber-crime perpetuated against SolarWinds into a class action claim for securities fraud against the Company, its executives, and its largest shareholders.

The Court should dismiss the Complaint because it fails to satisfy the heightened standards for pleading a Section 10(b) claim imposed by the Private Securities Litigation Reform Act ("PSLRA"). In particular, Plaintiff fails to adequately plead the elements of (1) scienter, (2) falsity, and (3) loss causation.

---

[1] A *White House Press Brief*, issued on April 15, 2021, is attached as Exhibit 1 to the Declaration of Michael J. Biles ("Biles Decl.").

[2] On this motion to dismiss, the Court may consider documents incorporated in the Complaint by reference, the contents of relevant disclosure documents filed with the SEC, Congressional testimony, and other matters subject to judicial notice. *See Ind. Elec. Workers' Pension Trust Fund IBEW v. Shaw Grp., Inc.*, 537 F.3d 527, 533 (5th Cir. 2008*); Lovelace v. Software Spectrum, Inc.*, 78 F.3d 1015, 1018 (5th Cir. 1996); s*ee also In re U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 830–31 (S.D. Tex. 2010) (finding Congressional testimony appropriate for judicial notice under Fed. R. Evid. 201); *U.S. ex rel. Lam v. Tenet Healthcare Corp.*, 481 F. Supp. 2d 673, 680 (W.D. Tex. 2006) ("Courts have the power to take judicial notice of the coverage and existence of newspaper and magazine articles," as well as "the fact that the market is aware of information contained in news articles.").

[3] *See, e.g.,* Biles Decl. Ex. 2, Mr. Smith, 2/23/21 Senate Hearing at 13, 50.

No Scienter: The Complaint fails to plead particularized facts that raise a "strong inference" that any of the SolarWinds Defendants[4] made a challenged statement with scienter, *i.e.*, a culpable state of mind embracing intentional or severely reckless deceit on investors. This unique and heightened pleading standard does not draw all inferences in plaintiff's favor, but requires courts to consider opposing nonculpable inferences. *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 324 (2007). Claims can survive dismissal "only if a reasonable person would deem the inference of scienter cogent and at least as compelling as any opposing inference." *Id.* The Complaint does not contain a single factual allegation supporting any inference, much less a cogent and compelling inference, that the SolarWinds Defendants intended to deceive investors into believing that SolarWinds was immune to cyberattacks or otherwise spoke with severe recklessness such that investors would draw that conclusion.

Plaintiff's central allegation is that a former employee, Ian Thornton-Trump, made a presentation to several non-party employees in April 2017 that supposedly alerted the SolarWinds Defendants to purported deficiencies in SolarWinds' security protocols. This allegation fails to raise a "strong inference" of scienter for multiple reasons. First, Thornton-Trump, who at the time had only been at SolarWinds for a few months, made this presentation *eighteen months* before the alleged class period even started, so it has no relevance to the truth or falsity of the challenged statements. Plaintiff concedes that Thornton-Trump left SolarWinds in May 2017. Thus, he cannot credibly speak to the security measures in place at SolarWinds nearly a year and a half later, much less offer insight into any of the SolarWinds Defendants' knowledge of such matters when the challenged statements were made. Second, there are no facts demonstrating that Thornton-Trump's concerns were communicated to Thompson or Brown (the "Individual Defendants"). Third, Thornton-Trump did

[4] "SolarWinds Defendants" means SolarWinds Corp., Tim Brown, and Kevin Thompson. Defendant Thompson has filed a separate motion to dismiss, but he fully joins in the arguments in this brief.

not work with the Orion software that was affected by the Cyberattack. *See* Compl. ¶¶ 87–88 (admitting he was employed in the managed service provider side of the business). Fourth, Plaintiff does not allege that Thornton-Trump's presentation even addressed any of the six alleged deficiencies in SolarWinds' security environment that Plaintiff alleges rendered the challenged statements false or misleading. Nor do any of the facts pled about the presentation suggest that the Company's risk of a cyberattack was materially greater than the Company repeatedly disclosed. Instead, the main thrust of Thornton-Trump's presentation was the recommendation that SolarWinds hire a qualified professional to lead its cybersecurity efforts, which is exactly what SolarWinds did when it hired Defendant Tim Brown as Vice President of Security two months after the presentation.[5] So even had Plaintiff alleged any facts showing the Individual Defendants had knowledge of the presentation, which it has not, it would still not be relevant to their state of mind.

Plaintiff also relies on ten anonymous former employees ("FEs") who offer redundant criticisms of SolarWinds' security protocols. But the FEs do not raise a "strong inference" of scienter because (1) none of them worked in positions that would plausibly suggest they had personal knowledge about the Cyberattack or SolarWinds' security infrastructure; and (2) Plaintiff does not allege that any FE communicated his or her concerns to any Individual Defendant.

Finally, Plaintiff's allegation of stock sales by some Defendants does not raise an inference of scienter. Stock sales, by themselves, are insufficient to raise a "strong inference" of scienter; and stock sales that are not suspicious in timing or amount provide no inference at all. Thompson's sales are not suspicious because most were made after he announced his resignation, they were made pursuant to a 10b5-1 plan, and he retained the vast majority of his SolarWinds holdings at the end of the alleged class period. Likewise, the timing of stock sales by Defendants Silver Lake and Thoma Bravo (the

[5] Notably, Thornton-Trump expressed outrage that SolarWinds did not hire *him* for the security position. *See* Biles Decl. Ex. 3, 5/15/17 Thornton-Trump email; *see also* Compl. ¶ 88.

"PE Defendants") has no bearing on whether the SolarWinds Defendants possessed the requisite scienter. Regardless, no facts are alleged suggesting those sales are remotely suspicious. Finally, the absence of an allegation that Brown, the architect of SolarWinds' security infrastructure, sold *any* stock negates an inference of scienter.

No Material Misstatements: Despite spanning 270 paragraphs, the Complaint challenges only five alleged misstatements and omissions—three statements from SolarWinds' website, and two statements by Brown in interviews. Only the "maker" of a misleading statement can be liable under Section 10(b) of the Exchange Act and Rule 10b-5, and Plaintiff does not attribute the three website statements to any Individual Defendant. *See Janus Capital Grp., Inc. v. First Derivative Traders*, 564 U.S. 135, 137–38, 142 (2011). Consequently, Plaintiff fails to plead that the Individual Defendants "made" these statements and the Court should dismiss the Section 10(b) and Rule 10b-5 claims against them based on these statements.

Plaintiff also fails to plead that any of the five challenged statements was materially false or misleading. Plaintiff embraces the fallacy that because SolarWinds was a victim of a highly sophisticated and targeted nation-state cyberattack, the Company must not have taken cybersecurity seriously. But there are no well-pleaded facts supporting this allegation. Moreover, even had Plaintiff made such allegations, no reasonable investor would consider bland and universally espoused statements that a company's security team focuses on "heavy-duty hygiene" or works to make "sure that there is good basic hygiene" important to his investment decision. Compl. ¶¶ 220, 222. The same is true for the aspirational statements on SolarWinds' website that the Company "is committed to taking [its] customers['] security and privacy concerns seriously and makes it a priority" or that SolarWinds "strive[s] to implement and maintain security processes." *Id.* ¶¶ 216, 218. Plaintiff simply has not pointed (and cannot point) to any statement made by SolarWinds, notwithstanding its focus on implementing good cyber hygiene, that could have been interpreted by a reasonable investor to

mean the Company viewed itself as impervious to attack. Nor may Plaintiff, in cherry-picking isolated statements from a website or interview, ignore the plain and unambiguous warnings that SolarWinds repeatedly provided in its SEC filings that despite its security measures, SolarWinds "could suffer a loss of revenue and increased costs, exposure to significant liability, reputational harm and other serious negative consequences" if it experiences "cyberattacks against [its] systems or against [its] products, or other data security incidents or breaches." *See, e.g.*, Ex. 13, 2/25/19 10-K at 15.

Finally, rather than supplying particular facts to establish that challenged statements misled reasonable investors, Plaintiff's allegations are contradictory and self-defeating. For example, Plaintiff contends that SolarWinds did not have a "Security Team" but also alleges that Thornton-Trump was the Company's "global cybersecurity strategist" (Compl. ¶ 64) and Brown was SolarWinds' Vice President of Security (*id.* ¶ 16). Even further, Brown specifically mentions his "team" in one of the challenged statements (*id.* ¶ 220). Plaintiff also makes the facially incredible claims that "[s]ecurity was not even discussed within the Company." *Id.* ¶ 203. To accept this as true, the Court would have to believe that, despite Thornton-Trumps' concocted title, Brown's actual title, and Plaintiff's allegation that Brown "spoke frequently about the Company's supposed cybersecurity" (*id.* ¶ 4), Brown and others *never* discussed security issues within SolarWinds.

No Loss Causation: Plaintiff does not adequately plead loss causation because he does not plead a "facially 'plausible' causal relationship between the fraudulent statements and omissions and plaintiff's economic loss." *Lormand v. U.S. Unwired, Inc.*, 565 F.3d 228, 258 (5th Cir. 2009). No facts are pled suggesting that Russian Intelligence exploited any of the six security deficiencies alleged in the Complaint to perpetrate the Cyberattack. Moreover, the Cyberattack and the ensuing decline in SolarWinds' stock price were materializations of risks about which the Company explicitly and repeatedly warned investors.

* * *

The Complaint follows a growing trend of "event driven" securities litigation, where any calamity that befalls a public company is framed as a violation of the securities laws, whether it be an industrial accident, a defective product, or a cyberattack. But the purpose of the federal securities laws is to promote the disclosure of material business information—not to provide investor insurance against losses resulting from business risks. Subjecting cyberattack victims, who never promised invulnerability to such crimes, to class action securities fraud claims would undermine the PSLRA's intent and fuel securities litigation in the wake of every cyberattack.

For these reasons, the Court should dismiss the Complaint with prejudice.

FACTUAL BACKGROUND

A. SolarWinds and the Individual Defendants

SolarWinds, an Austin-based company with over 3,340 employees, is the world's leading provider of information technology ("IT") infrastructure management software to companies, governments, and organizations. Biles Decl. Ex. 4, 5/10/21 10-Q at 10, 22.; Biles Decl. Ex. 5, SolarWinds Company overview webpage. SolarWinds offers over 70 unique software products that allow organizations to monitor and manage the performance of their IT environments. Biles Decl. Ex. 4, 5/10/21 10-Q at 10. Worldwide, SolarWinds has over 320,000 customers in 190 countries, and sells its products to over 22,000 managed services providers ("MSPs")[6] serving over 450,000 organizations. *See id.* at 20; Biles Decl. Ex. 5, SolarWinds webpage.

Defendant Thompson served as Chief Financial Officer at several companies before joining SolarWinds in July 2006 as Chief Financial Officer and Treasurer. Biles Decl. Ex. 7, 10/18/18 Prospectus at 112. He became the Company's President in January 2009 and Chief Executive Officer in March 2010. *Id.* In February 2016, SolarWinds was acquired by the PE Defendants. *Id.* at 2.

[6] An MSP provides services, such as network, application, infrastructure and security, on customers' premises, in their MSP's data center (hosting), or in a third-party data center. *See* Biles Decl. Ex. 6, Gartner IT definition of MSP.

While the Company was private, SolarWinds strengthened its security posture by hiring key personnel to build up its security team, implemented new security protocols, and strengthened its security infrastructure. *See* Biles Decl. Ex. 8, Mr. Thompson, 2/26/21 Congressional Hearing at 53; Biles Decl. Ex. 9, 4/25/17 press release. The Company dedicated more of its budget to security initiatives than any of its peers during this time period and invested in security at "a level meaningfully higher than the industry average." Biles Decl. Ex. 8, Mr. Thompson, 2/26/21 Congressional Hearing at 30, 53. As part of an initiative to make their security even stronger in 2016 and 2017, the Company brought in two experienced professionals to add to the team: a Chief Technology Officer—Joseph Kim—and a Chief Information Officer—Rani Johnson. *Id.* at 53.

In mid-2017, SolarWinds hired Defendant Brown as Vice President of Security. *Id.* at 12–13, 53; Biles Decl. Ex. 9, 4/25/17 press release; *see also* Compl. ¶ 16. Brown joined SolarWinds with over 20 years of experience in security, having previously served as Dell's Chief Technology Officer and Executive Director of Security and one of eight Dell Fellows.[7] *Id*; *see also* Decl. Ex. 11, Tim Brown author webpage.

SolarWinds remained private for two years before it conducted an IPO in October 2018. *See generally* Biles Decl. Ex. 7, 10/18/18 Prospectus.

B. SolarWinds warns investors that it is vulnerable to a cybersecurity breach and that the consequences could be severe.

Cybersecurity breaches like the Cyberattack are a risk that all companies face in today's world. As Mr. Brown explained, "[s]ecurity experts have increasingly emphasized the risks inherent in the software supply chain," and it is well-understood that "no software is perfect or vulnerability-free forever." Biles Decl. Ex. 12, Tim Brown article. As SolarWinds explained to its customers, "despite

[7] Being named a Dell Fellow is a high accolade that "recognizes engineers for their outstanding and sustained technical achievements, engineering contributions and advancement of the industry." Biles Decl. Ex. 10, 11/16/15 Interview with Tim Brown.

their best effort, vendors will have some security incidents." *Id.* SolarWinds repeatedly warned investors of these risks in its SEC filings. For example, in its October 2018, IPO Offering Documents filed with the SEC, SolarWinds stated:

> ***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). ***The risk of a security breach or disruption, particularly through cyberattacks or cyber intrusion, including by computer hacks, foreign governments, and cyber terrorists, has generally increased in number, intensity and sophistication of attempted attacks, and intrusions around the world have increased.*** … 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 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.[8]

SolarWinds also cautioned that it "may be unable to anticipate [threat actors'] techniques or to implement adequate preventative measures" because "the techniques used to obtain unauthorized access or to sabotage systems change frequently and generally are not identified until they are launched against a target." Biles Decl. Ex. 7, 10/18/18 Prospectus at 25. SolarWinds specifically explained that a breach could "remain undetected for an extended period" due to the sophistication of some cyberattacks, which could have an even greater impact on its business. *Id.* at 25. Despite the precautions SolarWinds had in place to prevent such a breach, the Cyberattack was a materialization of the exact risk that SolarWinds disclosed in numerous SEC filings during the Class Period.

C. SolarWinds is the victim of the most sophisticated cyberattack in history.

On December 14, 2020, SolarWinds announced that it had been the victim of the Cyberattack on its Orion Software Platform ("Orion"). Biles Decl. Ex. 15, 12/14/20 8-K. The Company's

[8] Biles Decl. Ex. 7, 10/18/18 Prospectus at 25–26 (emphasis added); *see also* Ex. 13, 2/25/19 10-K at 15; Ex. 14, 2/24/20 10-K at 15. These risk disclosures were repeated and incorporated by reference in every annual and quarterly financial statement filed with the SEC since the Company went public in 2018.

investigation, which is still ongoing, revealed that the hacker employed "novel and sophisticated techniques indicative of a nation-state actor and consistent with the goal of cyber espionage via a supply-chain attack." Biles Decl. Ex. 16, 5/7/21 8-K. "[T]he threat actor compromised credentials and conducted research and surveillance in furtherance of its objectives through persistent access to [SolarWinds] software development environment and internal systems," for at least nine months prior to initiating a test run. *Id.* In October 2019, the threat actor undertook a test run of its ability to inject code into Orion during the building process. *Id.* After determining that its test run was successful, it inserted malicious code, called "Sunburst," into the versions of Orion that SolarWinds released between March and June 2020. *Id.* SolarWinds has not identified "Sunburst" in any of its more than 70 other non-Orion products and tools. Biles Decl. Ex. 18, 3/1/21 10-K at 2; *see also* Biles Decl. Ex. 2, Mr. Ramakrishna, 2/23/21 Senate Hearing at 11 ("After extensive investigations, we have not found Sunburst in our more than 70 non-Orion products."). The details of the Cyberattack have taken months to understand because the threat actors "were very, very careful about covering their tracks, cleaning up after themselves." Biles Decl. Ex. 8, Mr. Ramakrishna, 2/26/21 Senate Hearing at 21.

Since the Cyberattack was first discovered, SolarWinds has taken extensive measures to investigate, contain, eradicate, and remediate the incident. By May 2021, SolarWinds reported that it had substantially completed this process and believed the threat actor was no longer active in its environments. Biles Decl. Ex. 16, 5/7/21 8-K. SolarWinds continues to work with industry experts to implement enhanced security practices designed to further strengthen and protect its products, environment, and customers against any future cyberattacks. *Id.*

The Cyberattack has been described as "the largest and most sophisticated operation" that the world has ever seen, and so sophisticated that it took "at least a thousand very skilled, capable engineers" to carry out such an attack. *See, e.g.*, Biles Decl. Ex. 2, Mr. Smith, 2/23/21 Senate Hearing at 13, 50; Biles Decl. Ex. 19, 12/17/20 CISA alert at 2 ("This threat actor has demonstrated

sophistication and complex tradecraft in these intrusions.").[9] The attack was so vast and widespread that "it was determined by analysts that 30 percent of the victims had no direct connection to SolarWinds, but were still targets of the broader campaign." Biles Decl. Ex. 8, Congressman Meijer, 2/26/21 Congressional Hearing at 61; *see also id.* Mr. Ramakrishna, at 61 (discussing other supply chain attacks around the world). SolarWinds, in particular, was an attractive target for a foreign government espionage campaign because of its strong customer base, including Fortune 500 companies and the U.S. Government. *See* Compl. ¶ 1. Despite the thousands of customers that use SolarWinds' Orion product, fewer than 100 were actually hacked through "Sunburst." Biles Decl. Ex. 16 5/7/21 8-K.

D. Plaintiff attempts to convert a Russian Intelligence criminal-espionage event into a securities-fraud claim against Defendants.

1. The "Security Statement"

Plaintiff challenges portions of SolarWinds' Security Statement posted several levels deep in its website stating that the Company "maintains a written Information Security policy," it has a "security team focuse[d] on information security," its "employees are provided with security training," it "maintains separate development and production environments," it "appl[ies] the latest security patches and updates," it implements "role based access controls," and it has a "password policy."[10] Plaintiff also challenges a statement that SolarWinds "follows the NIST Cybersecurity Framework,"

---

[9] As recognized by Congress members, Senators, and investigators, "even with the best cyber hygiene, even with the best protocols in place, because of how good and persistent and how much money a nation state like Russia has," every company is susceptible to such a sophisticated cyberattack. Biles Decl. Ex. 2, Senator Burr, 2/23/21 Senate Hearing at 37; *see also* Biles Decl. Ex. 8, Mr. Ramakrishna, 2/26/21 Congressional Hearing at 76 ("This particular issue was much more than just SolarWinds. It was a very sophisticated nation-state attack. . . . It has got very little relevance to the security hygiene of a particular company or the security investments of a particular company. It was a coordinated, patient, persistent attack that neither one company, no matter how large it is or how many resources it is deploying, or one federal government agency is able to coordinate."); Biles Decl. Ex. 20, 12/21/20 Bloomberg Article at 3 ("The reality is that sophisticated threat actors, no matter how good the defenses, will eventually succeed," said Costin Raiu, director of global research and analysis at the cybersecurity firm Kaspersky. "If the cost justifies the effort, the breach will happen.").

[10] Decl. Ex. 21, SolarWinds Security Statement webpage.

which is voluntary guidance for organizations to better manage and reduce cybersecurity risk,[11] purportedly on the grounds that SolarWinds did not conduct criminal background checks on all of its employees. *See* Compl. ¶ 215. Notably, however, the NIST Cybersecurity Framework does not mandate strict compliance with every suggested guideline. To the contrary, NIST explains that "[t]he Framework is guidance. It should be customized by different sectors and individual organizations to best suit their risks, situations, and needs."[12]

As explained below, Plaintiff fails to plead particular facts that, if true, would show that any challenged statement was false or misleading.

2. The Thornton-Trump Presentation

Thornton-Trump, whose allegations serve as the lynchpin of Plaintiff's Complaint, had a short tenure at SolarWinds—he joined "in early 2017" and resigned in May 2017 after he was passed over for a promotion. Compl. ¶ 64. Plaintiff alleges that, on April 22, 2017, Thornton-Trump delivered a PowerPoint presentation titled "Creating Security" to several non-party employees. Compl. ¶ 74. But Plaintiff does not allege that this presentation identified any of the six alleged security deficiencies that Plaintiff says rendered the "Security Statement" false and misleading. Biles Decl. Ex. 24, Thornton-Trump PowerPoint. Rather, it spends several slides discussing strategy on how to grow SolarWinds' business in the security space, and for those slides where it does discuss SolarWinds' infrastructure security, it identifies "four functional areas of security" and states that "[p]arts of these four functional areas exist [at SolarWinds] today." *Id.* at PDF pp. 9–11. Thornton-Trump's PowerPoint does not state that increased security protocols will prevent cyberattacks. To the contrary, he states that a "[d]ata breach of our company and customers is inevitable. The capabilities of external protagonists are equally matched by internal mistakes or malicious activity." *Id.* at PDF p. 4. Thornton-Trump

[11] *Id.*; Biles Decl. Ex. 22, 4/16/18 NIST, *Framework for Improving Critical Infrastructure Cybersecurity*.
[12] Decl. Ex. 23, NIST webpage at 1.

explains that SolarWinds will have to "accept failure" even if it makes the recommended security investments. Indeed, in interviews with the press, Thornton-Trump has conceded that the hackers who broke into the Company were "so sophisticated it would have been hard for anyone to defend against them." Biles Decl. Ex. 25, 4/16/21 NPR Article at 19.

The main thrust of Thornton-Trump's "Creating Security" presentation is the recommendation that SolarWinds hire a dedicated security professional. And an email cited in the Complaint shows that Thornton-Trump quit because SolarWinds did not hire him for the position: "the organization was not interested in accommodating me or retaining my services at my level of expectation … It's telling to me that my job and plan were essentially used for the VP architecture job which was posted prior to my departure. Yet I was not considered for the role." Biles Decl. Ex. 3, 5/15/17 Thornton-Trump email; Compl. ¶ 88. Thornton-Trump quit because SolarWinds did not consider him for the role; the Company instead hired Brown as the VP of Security shortly after Thornton-Trump quit and just two months after he made his PowerPoint presentation. *See id.*; Biles Decl. Ex. 20, 12/21/20 Bloomberg Article at 2.

3. The "solarwinds123" password event

Plaintiff alleges that in November 2019, "security researcher" Vinoth Kumar notified SolarWinds that he found the password to a SolarWinds server—"solarwinds123"—on a public message board. Biles Decl. Ex. 25, 4/16/21 NPR Article at 17; *see also* Compl. ¶¶ 103–112. Plaintiff does not allege that the "solarwinds123" password was linked to a server used to build source code for SolarWinds' software products or had anything to do with the Cyberattack on Orion. *Id.*; *see also* Biles Decl. Ex. 26, 12/15/20 Reuters Article at 4. ("Neither the password nor the stolen access is considered the most likely source of the current intrusion, researchers said."). Indeed, as reported in an NPR article quoted in the Complaint, the "solarwinds123" password "had nothing to do with [the Cyberattack] at all" because it was a password to a file-transfer server maintained by a third-party that

an intern shared on his GitHub account.[13] Biles Decl. Ex. 25, 4/16/21 NPR Article at 17; Compl. ¶ 169. Plaintiff does not and cannot allege any facts to connect this password event to the "largest and most sophisticated" cyberattack in history.

4. The Palo Alto Networks email

Plaintiff alleges that Palo Alto Networks (a California-based cybersecurity company) notified SolarWinds in September 2020 of an "attempt[] to infiltrate [Palo Alto's] network through SolarWinds' software." Compl. ¶ 195. Plaintiff alleges that Palo Alto "described the activity it observed on its network" but does not allege that the attempted infiltration was successful or alerted SolarWinds to any security vulnerability in SolarWinds' software, much less that SolarWinds had been victimized in a sophisticated supply chain attack that compromised the Orion software and put SolarWinds clients who installed the compromised software at risk. *See id.*

5. Plaintiff's unidentified witnesses

Plaintiff attributes certain allegations to 10 unnamed former employees ("FEs") who, collectively, repeat the same general complaints about SolarWinds' security protocols. The FEs do not support Plaintiff's claims because none of them is alleged to have held a position where he or she would have known anything about the Cyberattack or SolarWinds' security infrastructure. It is telling that Plaintiff could not find a single former employee who worked on the Orion Software Platform or on security issues: FE 1 did not work on Orion-based products (Comp. ¶ 84 n.21); FEs 2, 3, 4, 7, 8, 9, and 10 worked in sales (*id.* ¶¶ 91–93 n.22–24; *id.* ¶¶ 98–101 n.27–31); and FEs 5 and 6 worked in recruitment and Human Resources (*id.* ¶¶ 94–97 n.25–26). Additionally, at least one of the FEs (in addition to Thornton-Trump) was a newly acquired employee from the LOGICnow acquisition. *Id.*

[13] GitHub is a web-based version-control and collaboration platform for software developers. *See* Biles Decl. Ex. 17, GitHub product overview webpage.

¶ 100 n.30. The FEs' allegations have nothing to do with the Cyberattack and are not remotely probative of the claims asserted in the Complaint.

LEGAL STANDARD

To state a claim under Section 10(b) of the Securities Exchange Act of 1934 ("Exchange Act") and the SEC's Rule 10b–5 promulgated thereunder, "a plaintiff must allege (1) a material misrepresentation or omission; (2) scienter (a 'wrongful state of mind'); (3) a connection with the purchase or sale of a security; (4) reliance; (5) economic loss; and (6) a 'causal connection between the material misrepresentation and the loss.'" *Mun. Emps.' Ret. Sys. of Mich. v. Pier 1 Imports, Inc.,* 935 F.3d 424, 429 (5th Cir. 2019) (*quoting Dura Pharms.,* 544 U.S. at 341–42). A section 10(b) claim is subject to both Federal Rule of Civil Procedure 9(b)'s requirement that fraud be pled "with particularity" and the stricter requirements of the PSLRA. *Abrams v. Baker Hughes, Inc.*, 292 F.3d 424, 430 (5th Cir. 2002).

The PSLRA "was enacted in response to an increase in securities fraud lawsuits perceived as frivolous." *Newby v. Enron Corp.*, 338 F.3d 467, 471 (5th Cir. 2003). The PSLRA requires a complaint to specify each allegedly misleading statement and the reason why it is misleading; if an allegation is made on information and belief, then the complaint must also state with particularity all facts on which the belief is formed. 15 U.S.C. § 78u–4(b)(1). It is insufficient for a plaintiff to merely allege "facts" without providing any underlying support in the form of either confidential witnesses or documentary evidence. *See ABC Arbitrage Plaintiffs Grp. v. Tchuruk*, 291 F.3d 336, 350 (5th Cir. 2002). The Fifth Circuit has found that the requirements of the PSLRA strengthen the requirements of Rule 9(b), and "requires a plaintiff to specify the statements contended to be fraudulent, identify the speaker, state when and where the statements were made, and explain why the statements were fraudulent." *Id.* The Court must dismiss a securities fraud claim failing to satisfy the pleading requirements of either the PSLRA or Rule 9(b). *See Fin. Acquisition Partners LP v. Blackwell*, 440 F.3d 278, 287 (5th Cir. 2006) (internal quotation marks omitted).

ARGUMENT

As discussed in greater detail below, the Complaint falls far short of satisfying the PSLRA's heightened pleading standards. Among the Complaint's pleading deficiencies for several essential claim elements, the most glaring is Plaintiff's failure to plead facts raising a strong inference that the Defendants acted with intent to deceive or severe recklessness—*i.e.*, the element of scienter. Plaintiff relies principally on allegations about Thornton-Trump's April 2017 presentation to unidentified non-parties, but those allegations (and others attributed to Thornton-Trump) address conditions purportedly prevailing ***eighteen months before*** the start of the Class Period and fail to supply facts contradicting any challenged statement, much less establish that any Defendant spoke with intent to deceive or severe recklessness. Plaintiff's allegations attributed to unnamed "former employees" of SolarWinds likewise fail to support a strong inference of scienter because they neither connect any Defendant to knowledge of information conflicting with the challenged statements nor even plead a basis for inferring the FEs' knowledge of SolarWinds' cybersecurity practices. Plaintiff's remaining allegations fail to plead that Defendants spoke with knowledge of information contradicting their statements or severe recklessness. Further, Plaintiff's "motive" allegations are fatally deficient for reasons explained below. Plaintiff also fails to plead a single misleading statement of material fact and fails to plead that the investment losses Plaintiff seeks to recover were caused by actionable misstatements or misleading omissions. Any one of Plaintiff's failures to plead scienter, falsity, or loss causation requires dismissal of the Complaint.

I. Plaintiff fails to plead the required strong inference of scienter.

To withstand dismissal on the pleadings, the PSLRA requires that a securities complaint "shall, with respect to each act or omission … state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind." 15 U.S.C. § 78u-4(b)(2)(A). The "required state of mind" is an "an intent to deceive, manipulate, defraud or severe recklessness." *Local 731 Int'l*

Bhd. of Teamsters Excavators & Pavers Pension Tr. Fund v. Diodes, Inc., 810 F.3d 951, 957 (5th Cir. 2016) (citation omitted). Pleading "severe recklessness" requires allegations showing more than "inexcusable negligence." *Id.* The facts pled with particularity must establish "an extreme departure from the standards of ordinary care," in which the danger that challenged statements will mislead investors "is either known to the defendant or is so obvious that the defendant must have been aware of it." *Markman v. Whole Foods Market, Inc.*, 269 F. Supp. 3d 779, 785–86 (W.D. Tex. 2017) (Yeakel, J.) (finding allegations insufficient to satisfy PSLRA scienter pleading standard).

Adequately pleading scienter thus requires particular factual allegations establishing each defendant's contemporaneous knowledge of undisclosed information that conflicts with or contradicts his or her challenged statements. *See Tuchman v. DSC Commc'ns Corp.*, 14 F.3d 1061, 1069 (5th Cir. 1994) (holding scienter was not adequately pled where the complaint "failed to allege any facts that show that [defendant's] statements were belied by his actual knowledge of contradictory facts").[14] Further, because the Fifth Circuit has rejected the "group pleading" approach to scienter, only allegations addressing "the state of mind of the corporate officials who make, issue, or approve the statement[,] rather than the collective knowledge of all the corporation's officers and employees," are relevant. *Diodes*, 810 F.3d at 957 (internal quotation marks and citation omitted). Where, as here, the Complaint does not allege that any particular person other than the Individual Defendants is responsible for the challenged statements, the Court should only consider whether the Complaint adequately pleads an Individual Defendant's scienter. *See Southland Sec. Corp. v. INSpire Ins. Solutions, Inc.*, 365 F.3d 353, 366–67 (5th Cir. 2004) (finding corporate scienter not adequately pleaded where scienter of individual defendants was not sufficiently alleged).

[14] *See also Abrams*, 292 F.3d at 432–33 (allegations that failed to show defendants' knowledge of information "contradict[ing]" or "contrary to" challenged statements failed to support a strong inference of scienter); *accord Shaw Grp.*, 537 F.3d at 540.

The Court must "consider the entire complaint, including documents incorporated into the complaint by reference and matters subject to judicial notice" and weigh "plausible inferences supporting as well as opposing a strong inference of scienter." *Diodes*, 810 F.3d at 956–57; *see also Tellabs*, 551 U.S. at 323. To survive dismissal the inference of scienter must be "cogent and compelling, not simply reasonable or permissible." *Diodes*, 810 F.3d at 957 (internal quotation marks and citation omitted). As shown below, Plaintiff's allegations fall far short of these exacting pleading standards.

A. The allegations about Thornton-Trump fail to support a strong inference of scienter.

Plaintiff leans heavily on allegations that Thornton-Trump perceived various cybersecurity deficiencies during his short tenure at SolarWinds and made a presentation in April 2017 about cybersecurity risks and recommendations to some SolarWinds executives (who are not parties to this litigation). *See* Compl. ¶¶ 181–83; *see also id.* ¶¶ 6, 63–83, 85–89, 99 n.29, 111 n.34, 114, 117, 121, 123, 125, 132, 141. As shown below, these allegations fail to raise any inference—much less the required cogent and compelling inference—that the SolarWinds Defendants acted with scienter.

First, Plaintiff alleges that Thornton-Trump joined SolarWinds in "early 2017" as part of the MSP business—which is not related to Orion or the Cyberattack—but then quickly resigned in May 2017. *Id.* ¶¶ 64, 67–68, 88. Thus, Thornton-Trump worked at SolarWinds for only a few months in a business unrelated to the Cyberattack and resigned seventeen months *before* the start of the purported Class Period. Plaintiff does not plead that Thornton-Trump has any knowledge whatsoever about the state of SolarWinds' cybersecurity *during* the time period addressed by the challenged statements.[15] The allegations attributed to Thornton-Trump—*e.g.*, that he was a "global cybersecurity strategist" (*id.* ¶ 64), but that there "was no security team, there was no password policy, there was no documentation

[15] Notably, in his April 22, 2017 presentation, Thornton-Trump states that SolarWinds could make "significant progress and achievement [could] be realized within a year." Biles Decl. Ex. 24, Thornton-Trump PowerPoint at PDF p. 3.

regarding data protection and controls, and the Company did not limit user access controls, exposing the Company's 'crown jewels' to a potential cyberattack" (*id.* ¶ 6)—are thus not probative of either the truth and accuracy of the challenged statements addressing SolarWinds' cybersecurity *during* the purported Class Period, nor of the SolarWinds Defendants' contemporaneous knowledge about the challenged statements. *See Shah v. GenVec, Inc.*, No. DKC 12-0341, 2013 WL 5348133, at *5 n.7 (D. Md. Sept. 20, 2013) (alleged witness whose "employment was terminated in January 2009 . . . could have had no credible basis of knowledge as to events occurring internally at GenVec in 2010"); *accord Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 996 (9th Cir. 2009) (witnesses who "were not employed . . . during the time period in question" did not support a string inference of scienter). For this reason alone, these allegations fail to raise an inference of scienter.

Second, Plaintiff's allegations about Thornton-Trump's purportedly critical assessments of SolarWinds' cybersecurity are internally-conflicted and self-defeating. On the one hand, Plaintiff alleges Thornton-Trump claims that "'[t]here was no corporate security' at SolarWinds and no dedicated security positions at all at SolarWinds." Compl. ¶ 66. Yet, Plaintiff also pleads that Brown, who has "decades of experience in the security technology field," has served as "SolarWinds' Vice President of Security Architecture since 2017" and is "responsible for … security for [its] infrastructure." *Id.* ¶ 16. Such internally conflicting and contradictory allegations cannot support a strong inference of scienter. *See, e.g., Hampshire Equity Partners II, L.P. v. Teradyne, Inc.*, No. 04 Civ. 3318, 2005 WL 736217, at *3 (S.D.N.Y. Mar. 30, 2005) (fundamentally illogical and contradictory scienter allegations fail as a matter of law).

Third, Plaintiff does not allege that Thornton-Trump *ever* discussed any concerns he allegedly had about SolarWinds' cybersecurity with any Individual Defendant—or that *anyone* ever did so. Without any allegation that Thornton-Trump's concerns were conveyed to the Individual Defendants or to the persons at SolarWinds allegedly responsible for the challenged statements, the Complaint

fails to raise a strong inference of scienter against the SolarWinds Defendants. *See Southland*, 365 F.3d at 383 (allegation that did not concern "what any particular individual knew or was severely reckless in not knowing, at the time" of challenged statements was "unpersuasive of scienter").[16]

Fourth, setting aside Plaintiff's failure to plead that the Thornton-Trump presentation—or any of its substance—was conveyed to the Individual Defendants, the Complaint fails to plead a strong inference of scienter because its allegations about the presentation fail to identify any facts contradicting or conflicting with the challenged statements. *See Tuchman*, 14 F.3d at 1069; *Abrams*, 292 F.3d at 432–33. Plaintiff does *not* allege that any of the six challenged statements in SolarWinds' Security Statement is specifically addressed in the Thornton-Trump presentation. Instead, Plaintiff alleges that this presentation addressed the serious but universal (and publicly acknowledged) threat of cyberattack that SolarWinds (and virtually every company) faced (*see, e.g.*, Compl. ¶¶ 77, 80).[17] But that allegation fails to raise a strong inference of scienter because SolarWinds publicly warned investors about its vulnerability to cyberattacks and the serious risks and consequences of a successful attack.[18]

---

[16] *See also In re Heartland Payment Sys., Inc. Sec. Litig.*, No. 09–1043, 2009 WL 4798148, at *8 (D.N.J. Dec. 7, 2009) (finding scienter not pled where plaintiff failed to plead that "concerns [about cybersecurity] were ever relayed to any of the Defendants"); *In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig. Sec. Actions,* No. 8:19-md-2879, 2021 WL 2407518, at *35 (D. Md. June 11, 2021) (finding scienter not pled where allegations failed to address "what any of the Individual Defendants actually knew about Marriott's cybersecurity or the falsity of any statements").

[17] On its face, Thornton-Trump's presentation does not raise "red flags" that deficiencies in SolarWinds's security program exposed the Company to an imminent "catastrophic cyberattack," but instead simply stated the obvious: "we need to accept truths of the marketplace . . . [including that] Data breach of our company and customers is inevitable." *Compare* Biles Decl. Ex. 24, Thornton-Trump PowerPoint at PDF p. 4 *with* Compl. ¶ 76. That is exactly what SolarWinds warned in numerous public cautionary statements. *See supra* at 7–8 & n.8.

[18] *See, e.g.,* Biles Decl. Ex. 7, 10/18/18 Prospectus at 25–26 (warning, among other things, that: "Our systems and those of our third-party service providers are vulnerable to … computer "hackers," malicious code…, employee theft or misuse, and denial-of-service attacks, as well as sophisticated nation-state and nation-state-supported actors . . . . [W]e may be unable … to implement adequate preventative measures. We may also experience security breaches that may remain undetected for an extended period and, therefore, have a greater impact on the products we offer, the proprietary data contained therein, and ultimately on our business. The foregoing security problems could result in,

See In re Marriott, 2021 WL 2407518, at *37 (finding that allegations of cybersecurity "red flags," including multiple discoveries of data theft malware on internal systems, did not support inference of scienter where company "disclosed that it was at risk of a cyber-attack").

Plaintiff also alleges that Thornton-Trump's presentation recommended that SolarWinds (i) hire security-focused personnel (Compl. ¶ 76); (ii) develop a data breach response plan (*id.* ¶ 79); (iii) address alleged "silos of communication" and lack of "centralized" management and reporting (*id.* ¶ 75); and (iv) "commit culturally" to making cybersecurity a "core value" (*id.* ¶ 78). But these recommendations in April 2017 do not bear on the factual accuracy of immaterial statements *on different topics* made *eighteen months later* stating that SolarWinds had a security team, policies regarding information security and passwords, security training for employees, and role-based access, followed the NIST framework, focused on cyber hygiene, and made security "a priority." *See Zucco Partners*, 552 F.3d at 996; Shah, 2013 WL 5348133, at *5 n.7. These allegations thus fail to support a strong inference of scienter. *See In re Marriott*, 2021 WL 2407518, at *35 (allegations that fail to "demonstrate that Defendants made any statements with actual knowledge or reckless disregard that any statements were false or misleading" do not support a string inference of scienter).

B. The remaining "former employee" allegations also fail to establish any Defendant's scienter.

Plaintiff's allegations attributed to unnamed FEs (Compl. ¶¶ 84, 91–102, 113, 115, 118, 120–22, 126–30, 133–35, 138–39, 142–47, 184, 187) also fail to support a strong inference of scienter for at least four reasons. *First*, these allegations are silent as to the Individual Defendants' *contemporaneous* knowledge when the challenged statements were made. Plaintiff does not allege that any FE or other

---

among other consequences, damage to our own systems or our customers' IT infrastructure or the loss or theft of our customers' proprietary or other sensitive information. The costs to us to eliminate or address the foregoing security problems and security vulnerabilities before or after a cyber incident could be significant."); *see also* Compl. ¶ 33 (alleging that, at the March 5, 2020 Morgan Stanley Technology Media & Telecom Conference, "Defendant Thompson stated that 'the threat landscape is getting worse, not better . . . the reality is it's just going to get worse.'").

source identified in the Complaint ever raised any alleged concern about SolarWinds' cybersecurity with the Individual Defendants or witnessed anyone else doing so. For this reason alone, these allegations fail to support a strong inference of scienter. *See In re Marriott*, 2021 WL 2407518, at *35 (finding scienter not pled where "none of the Confidential Witness allegations are regarding what any of the Individual Defendants actually knew about Marriott's cybersecurity or the falsity of any statements"); *Heartland*, 2009 WL 4798148, at *8 (same).

Second, these allegations fail because the Complaint does not plead facts "with sufficient particularity to support the probability that [the FEs] would possess the information pleaded to support the allegations of false or misleading statements." *ABC Arbitrage*, 291 F.3d at 357-58; *see also Cent. Laborers' Pension Fund v. Integrated Elec. Servs.*, Inc., 497 F.3d 546, 552 (5th Cir. 2007).[19] The FEs are *all* alleged to have had either *customer-facing sales/support roles* or *human resources roles*. *See* Compl. nn.21–28, 30–31. None of them is alleged to have had responsibilities for SolarWinds' internal cybersecurity nor any relevant personal knowledge of, or reliable basis on which to assess, SolarWinds' overall corporate cybersecurity posture.[20] Allegations that five of the ten FEs were unaware of

[19] Particularly egregious and deficient are Plaintiff's allegations sourced only to "current and former employees of SolarWinds" (Compl. ¶ 147), which fail to supply even basic information such as job descriptions, individual responsibilities, or specific employment dates. *See Cent. Laborers*, 497 F.3d at 552.

[20] Nor does Plaintiff plead that the Individual Defendants were ever informed of, much less agreed with, any of the FEs' alleged criticisms of SolarWinds' security practices (Compl. ¶¶ 84, 91, 95–97, 100–02, 118, 126–27, 135, 138–39, 142, 144–46). *See Heartland*, 2009 WL 4798148, at *8; *see also In re Marriott*, 2021 WL 2407518, at *35; *In re HomeBanc Corp. Sec. Litig.*, 706 F. Supp. 2d 1336, 1350 (N.D. Ga. 2010) (dismissing complaint where plaintiff failed to establish that defendants agreed with others' assessments of "massive and systematic problems"). In any event, allegations that some FEs disagreed with particular security practices or felt that those practices were deficient, at most allege disagreement with managerial judgments or possible mismanagement. Such allegations do not plead securities fraud. *See, e.g., Santa Fe Indus. v. Green*, 430 U.S. 462, 479-80 (1977) (allegations of mismanagement or the failure to disclose the same are insufficient to plead a Section 10(b) violation); *accord Cutsforth v. Renschle*r, 235 F. Supp. 2d 1216, 1242-44 (M.D. Fla. 2002); *Craftmatic Sec. Litig. v. Kraftsow*, 890 F.2d 628, 640 (3d Cir. 1989); *In re Winn-Dixie Stores, Inc. Sec. Litig.,* 531 F. Supp. 2d 1334, 1347 (M.D. Fla. 2007); *In re Donna Karan Int'l Sec. Litig.*, 1998 WL 637547, No. 97-cv-2011, at *9 (E.D.N.Y. Aug. 14, 1998).

SolarWinds' security team (Compl. ¶¶ 95, 98, 115) do not support the conclusion that SolarWinds had no such team.[21] To the contrary, Plaintiff affirmatively alleges that Brown, the leader of SolarWinds' security team, had been serving as its "Vice President of Security Architecture since 2017" and was responsible for "security of [SolarWinds'] infrastructure." *Id.* ¶ 16. And it is neither surprising nor probative of the Individual Defendants' scienter that these FEs, given their alleged roles, did not recall any security training, particular security-related policies, or hearing from Thompson about cybersecurity matters, in "quarterly business review" meetings or in other contexts (*id.* ¶¶ 91–95; 97–102; 118; 120–21; 126–30; 142; 143–46).[22]

Third, the Fifth Circuit has held that "courts must discount allegations from confidential sources" generally. *Shaw Grp.* 537 F.3d at 535. That is especially true where, as here, the Complaint pleads insufficient facts demonstrating the bases for the unnamed sources' personal knowledge of the sweeping allegations attributed to them. *Id.* at 539–40.

Finally, the FE allegations are insufficient in other respects to raise a strong inference of scienter. Some are simply too vague to plead the existence of information contradicting any challenged statement, much less any Individual Defendant's knowledge of any such information,[23] even if Plaintiff had pled a plausible basis to infer that these FEs had personal knowledge to back up their

---

[21] During the Class Period, the total number of persons employed by SolarWinds ranged from roughly 2,500 to over 3,250. *See* Biles Decl. Ex. 7, 10/18/18 Prospectus at 23 (2,540 employees as of June 30, 2018); Ex. 14, 2/24/20 10-K at 10 (3,251 employees as of December 31, 2019). It is entirely unremarkable that five former sales and HR employees would profess ignorance of the security team.

[22] *See Shaw Grp.*, 537 F.3d at 539–40 (finding allegations failed to support scienter where complaint "lack[ed] sufficient detail to support the probability that [unnamed sources were] in a position to know about" the degree to which "problems" they asserted pervaded the company); *see also Cal. Pub. Emps.' Ret. Sys. v. Chubb Corp.*, 394 F.3d 126, 155 (3d Cir. 2004) (rejecting use of statements from local branch office employees to substantiate allegations about nationwide company practices); *Zucco Partners*, 552 F.3d at 996 (plaintiff failed to plead that human resources employee had "firsthand knowledge of the workings of the finance or corporate departments" at issue).

[23] *See, e.g.*, Compl. ¶ 91 ("Same sh*t, different day"); *id.* ¶ 93 (after SolarWinds came public "nothing changed with respect to security"); *id.* ¶ 102 ("no radical change to address Thornton-Trump's concerns").

assessments (and Plaintiff has not). *See Shaw Grp.*, 537 F.3d at 538 (allegations about a "letter detailing problems" with company's accounting software was "too vague to allow an inference of scienter"); *Pier 1 Imports,* 935 F.3d at 433 (vague allegation "that there were amorphous 'inventory problems'" but that did "not explain what those problems were" did not support an inference of scienter). Other allegations do not conflict with, and certainly are not pled with the required particularity to contradict, the challenged statements.[24]

In short, Plaintiff's FE allegations fail to "demonstrate that Defendants made any statements with actual knowledge or reckless disregard that any statements were false or misleading," and thus fail to support a strong inference of scienter. *In re Marriott*, 2021 WL 2407518, at *35; *Heartland*, 2009 WL 4798148, at *7.

C. Allegations that a rogue employee published credentials for accessing a SolarWinds' server do not support scienter.

Plaintiff's allegations that SolarWinds received word, on November 19, 2019, that an employee (eventually identified as a former intern) had posted credentials and a link for accessing SolarWinds' Update Server to the GitHub website in June 2018 (Compl. ¶¶ 105–09, 112, 185) likewise fail to support any inference of scienter for three reasons.

First, the allegations about this "solarwinds123" password are simply a red herring—Plaintiff does not and cannot plead any facts suggesting that the "solarwinds123" password or the Update Server was used in the Cyberattack. Indeed, a threat actor *could not* access SolarWinds's IT environment via the Update Server because that server is maintained by a third party and is used by SolarWinds' customers to download non-Orion software products. Having access to the Update

[24] *See, e.g.*, Compl. ¶¶ 92, 101, 134–35 (alleging ability to download files to Company computers or "view … products that [FE] did not work on"); *id.* ¶¶ 91, 101, 133, 135 (alleging access to unspecified "files" or "parts" of the network/system); *id.* ¶¶ 98, 143 (alleging laptops were left unlocked or in public areas); *id.* ¶ 100 (alleging lack of multi-factor authentication); *id.* ¶¶ 96–97, 138–39 (alleging lack of employee background checks).

Server would not have enabled the threat actor to access the Orion software build process and inject malicious code into Orion (the method by which the Cyberattack was perpetrated). *See* Biles Decl. Ex. 16, 5/7/21 8-K. Further, Plaintiff alleges that Brown caused the password to be changed "within an hour of being notified" of the issue (Compl. ¶ 112) and does not allege that the Update Server password was ever used to harm SolarWinds or *any* of its customers, that there remained any ongoing vulnerability to disclose, or that there was any reason for the Individual Defendants to believe the vulnerability had not been fully addressed. Plaintiff's insinuation that SolarWinds' correction of the problem without publicly reporting it somehow supports an inference of scienter thus fails. *See Heartland*, 2009 WL 4798148 at *8 (finding scienter not pled where "[a]ssuming that Defendants were aware of [a prior] attack, it does not follow necessarily that they believed that [the company's] security systems were deficient or that any problems created by the … attack had not been addressed"). Indeed, in *Heartland*, unlike here, the plaintiff alleged that the undisclosed attack directly led to and facilitated the massive data theft that ultimately gave rise to the case. *Id.* at *1. Here, where Plaintiff does not and cannot allege any connection whatsoever between the Update Server password apparently published by an intern (without authorization) and the Cyberattack, any possible inference of scienter is far weaker than that found lacking in *Heartland*.

Second, Plaintiff pleads that SolarWinds was first notified about the publication of the credentials and link *well after* all of the challenged statements were made. *Compare* Compl. ¶ 106 (alleging notice of the unauthorized posting on November 19, 2019) *with* ¶¶ 37, 200–23 (challenging statements made between August 28, 2018 and April 30, 2019).[25] Plaintiff's allegations thus say

[25] The Complaint is silent as to when either of the Individual Defendants first learned (i) that the password at issue was "solarwinds123" and (ii) that it had purportedly remained unchanged for over two years. Compl. ¶ 109. No facts are pled to suggest that the Individual Defendants learned such information before November 19, 2019, which further undercuts any inference of scienter. *See Tellabs*, 551 U.S. at 326 ("omissions and ambiguities count against inferring scienter").

nothing at all about the Individual Defendants' contemporaneous knowledge at times the challenged statements were made and therefore fail to support an inference of scienter for that reason as well. *See In re Marriott*, 2021 WL 2407518, at *39 (allegations not addressing what defendants knew "at the time the allegedly false or misleading statements were made" did not support an inference of scienter). Plaintiff "cannot plead scienter by hindsight." *Id.* (rejecting allegations about findings of cybersecurity shortcomings after challenged statements were made).[26]

Third, neither the alleged facts that an intern published his password to the Update Server on GitHub nor that the password itself was "solarwinds123" plead information conflicting with the challenged statements. At most, these allegations plead discrete violations of SolarWinds' password practices. Such allegations do not amount to securities fraud. *See Santa Fe*, 430 U.S. 479-80 (allegations of arguable mismanagement fail to plead a Section 10(b) claim). They say nothing at all about whether SolarWinds had a password policy and enforced its password practices referenced in the Security Statement, much less the accuracy of other challenged statements addressing entirely different subjects. Moreover, SolarWinds publicly warned investors that its systems were "vulnerable to … employee theft or misuse"—the very risk that materialized in the GitHub incident. Biles Decl. Ex. 7, 10/18/18 Prospectus at 25. Plaintiff's allegations are consistent with the challenged statements and SolarWinds' cautionary warnings, and they do not support an inference of scienter. *See In re Marriott*, 2021 WL 2407518, at *37.

D. Plaintiff's "motive" allegations are insufficient to establish scienter.

Plaintiff's allegations about sales of SolarWinds stock by Thompson and the PE Defendants (Compl. ¶¶ 191–96) and other alleged motives to deceive investors (*id.* ¶¶ 190–91, 197) also fail to support a strong inference of scienter.

[26] Plaintiff also fails to plead any factual basis for inferring the Individual Defendants' awareness that other "SolarWinds employees' passwords were leaking out on GitHub in 2019." Compl. ¶ 124.

1. The alleged stock sales do not support a strong inference of scienter.

First, as the Fifth Circuit has held, "insider trading, by itself, cannot create a strong inference of scienter." *Diodes*, 810 F.3d at 960 (observing that "corporate executives, whose compensation often includes company stock, will trade those securities in the normal course of events") (internal quotation marks and citation omitted); *accord Southland*, 365 F.3d at 368. At most, insider sales, if adequately pled to be "suspicious" in timing or amount, can *enhance* an inference of scienter arising from *other* allegations. *Diodes*, 810 F.3d at 960; *see also Southland*, 365 F.3d at 368. Because none of Plaintiff's other allegations gives rise to *any* inference of scienter, there is nothing for the stock sales allegations to enhance.

Second, Plaintiff's failure to plead *any* SolarWinds stock sales whatsoever by Brown, who Plaintiff alleges served as the Company's "Vice President of Security Architecture since 2017," was "responsible for … security for [SolarWinds'] infrastructure," and was "intimately involved in the Company's cybersecurity" (Compl. ¶¶ 16, 188), undermines any possible inference of scienter from allegations that other Defendants sold stock. *See Diodes*, 810 F.3d at 960 ("[E]ven unusual sales by one insider do not give rise to a strong inference of scienter when other defendants did not sell some or all of their shares during the Class Period.") (quoting *Abrams*, 292 F.3d at 435).[27]

Third, Plaintiff fails to adequately plead that Thompson's or PE Defendants' stock sales were "suspicious" in their timing or amounts. Plaintiff alleges that Thompson sold approximately 25% of his SolarWinds stock holdings in November 2020, shortly ahead of SolarWinds' announcement of his

[27] *See also Southland*, 365 F.3d at 369 ("The fact that other defendants did not sell their shares during the relevant class period undermines" plaintiffs' allegations that certain executives' sales support an inference of scienter.); *Eizenga v. Stewart Enters., Inc.*, 124 F. Supp. 2d 967, 986 (E.D. La. 2000) ("[T]he fact that other officers did not sell shares during the relevant period undermines the plaintiffs' motive theory.") (citation omitted); *Druskin v. Answerthink*, 299 F. Supp. 2d 1307, 1336 n. 40 (S.D. Fla. 2004) ("The fact that [an executive] *who would have been an essential participant in any fraudulent scheme*, did not sell stock undermines any suggestion of knowledge on the part of the defendants due to any other claimed inside[r] [sales].") (emphasis added).

resignation in December 2020. Compl. ¶¶ 15, 192.[28] As courts have recognized, it is neither suspicious nor unusual that an executive holding as much company stock as Thompson did (over 3 million shares just before the November 2020 sales)[29] would sell shares in the lead up to his departure, and for this reason alone, the November 2020 sales fail to support an inference of scienter as to Thompson.[30] Further, by Plaintiff's own allegation, Thompson retained the vast majority of his substantial equity stake in SolarWinds (holding over 2.3 million shares)[31] after the November 2020 sales (Compl. ¶ 192), which further negates any inference of scienter. *See, e.g., Southland*, 365 F.3d at 368-69 (sales in which executives divested between 26.62% and 33.27% of their shares were not suspicious). And SEC Form 4s memorializing Thompson's November 2020 sales reflect that the sales were made on Thompson's behalf pursuant to a prearranged trading plan under SEC Rule 10b5-1 (Biles Decl. Ex. 30, 11/18/20 Thompson Form 4; Ex. 31, 12/17/20 Thompson Form 4), which further negates any inference of scienter from these sales.[32]

Plaintiff's allegations concerning PE Defendants' stock sales (¶¶ 191, 194) fare no better. To start, the timing of the PE Defendants' stock sales has no bearing on whether *SolarWinds or the Individual*

---

[28] Although Plaintiff alleges that SolarWinds "announced" Mr. Thompson's resignation on December 9, 2020 (¶ 15), Mr. Thompson had previously discussed his planned departure and SolarWinds' search for new CEO during the Company's public quarterly earnings calls held on August 6, 2020 and October 27, 2020. *See* Biles Decl. Ex. 27, 8/6/20 Earnings Call Transcript at 10–11; Ex. 28, 10/27/20 Earnings Call Transcript at 9, 14.

[29] *See* Biles Decl. Ex. 29, 10/27/20 Thompson Form 4; Ex. 30, 11/18/20 Thompson Form 4.

[30] *See, e.g.*, *Greebel v. FTP Software, Inc.*, 194 F.3d 185, 206 (1st Cir. 1999) ("It is not unusual for individuals leaving a company ... to sell shares."); *In re K-tel Int'l, Inc. Sec. Litig.*, 300 F.3d 881, 896 (8th Cir. 2002) (same); *In re Am. Italian Pasta Co. Sec. Litig.*, No. 05-0725-CV-W-ODS, 2006 WL 1715168, at *6 (W.D. Mo. June 19, 2006) (no scienter when officer sold 65% of holdings before resigning); *Wietschner v. Monterey Pasta Co.*, 294 F. Supp. 2d 1102, 1116–17 (N.D. Cal. 2003) (impending retirement and 10b5-1 plan mitigated against inference of scienter); *see also Shaw Grp.*, 537 F.3d at 543–44 (executives large stock sales following expiration of "lock-up" period was not suspicious); *Southland*, 365 F.3d at 369 (director/officer sales "during a secondary public offering" not deemed suspicious).

[31] *See* Biles Decl. Ex. 31, 12/17/20 Thompson Form 4.

[32] *See Hopson v. MetroPCS Commc'ns, Inc.*, No. 3:09-CV-2392-G, 2011 WL 1119727, at *14 (N.D. Tex. Mar. 25, 2011); *Congregation of Ezra Sholom v. Blockbuster, Inc.*, 504 F. Supp. 2d 151, 165 (N.D. Tex. 2007); *but see In re ArthroCare Corp. Sec. Litig.*, 726 F. Supp. 2d 696, 722–24 (W.D. Tex. 2010) (Sparks, J.).

Defendants—the only defendants against whom a Section 10(b) claim is asserted—possessed the requisite scienter. In any event, no facts are alleged suggesting that those sales are remotely suspicious. As one court recently observed, the central business purpose of a private-equity fund "is to invest in companies and ultimately sell them." *In re Envision Healthcare Corp. Sec. Litig.*, No. 3:17-CV-01112, 2019 WL 6168254, at *26 (M.D. Tenn. Nov. 19, 2019). Plaintiff's allegations effectively concede as much. *See* Compl. ¶ 23 ("The Private Equity Firms are known for identifying short-term profit-centers in software companies and leveraging them to sell all or part of their investment at a profit."). "It is, therefore, not suspicious that [PE Defendants] would divest [themselves] of stock in large sales." *Envision*, 2019 WL 6168254, at *26.

Nor does Plaintiff's vague allegation that a SolarWinds client, Palo Alto Networks, notified SolarWinds in September 2020 of an attempt to infiltrate Palo Alto's network "through SolarWinds' software" (Compl. ¶ 195) suffice to plead that Thompson's stock sales in November 2020 (*id.* ¶ 192) and PE Defendants' stock sales in December 2020 (*id.* ¶¶ 19–20; 194) were suspiciously timed. *First*, and by itself dispositive, Plaintiff does not allege *any* facts establishing whether or when any information about the "attempted breach" *of Palo Alto's* network was conveyed to Thompson or to the PE Defendants. *Second*, nothing pled about this alleged (unsuccessful) attempt to infiltrate a client's network suggests that knowledge of Palo Alto's notice would have prompted Defendants' stock sales. Indeed, if as Plaintiff's theory requires, Thompson and PE Defendants (i) were informed of the September 2020 notice from Palo Alto and (ii) viewed it as reason to unload SolarWinds stock, it is entirely implausible that they would have delayed selling until mid-November and early December, respectively. The far more "cogent and compelling" inference is that Defendants' November and

December 2020 stock sales were made based on other factors and not "suspiciously" timed because of the September 2020 attack on Palo Alto.[33]

2. Plaintiff's other "motive" allegations fail.

Plaintiff's remaining "motive" allegations (Compl. ¶¶ 190–91, 197) also fail to support a strong inference of scienter. Allegations that "savings" from not implementing allegedly needed reforms allowed SolarWinds to meet analysts' estimates (*id.* ¶190) are based entirely on hindsight. Plaintiff does not plead facts suggesting that the costs of reforms SolarWinds has announced since the Cyberattack or any need to undertake those reforms were known at the time that the challenged statements were made. Nor does Plaintiff plead that Defendants could have known in advance that SolarWinds would miss analyst estimates in prior periods had it undertaken some or all of the reforms earlier. These speculative allegations fail to support scienter. *See Southland*, 365 F.3d at 383 (scienter depends on what defendants knew *at the time* of challenged statements); *accord Abrams*, 292 F.3d at 432; *see also In re Marriott*, 2021 WL 2407518, at *39 (Plaintiff "cannot plead scienter by hindsight.").

Further, the "savings" allegations (Compl. ¶ 190), like those about Defendants' public offerings of SolarWinds stock (*id.* ¶ 191) and Thompson's performance-based compensation (*id.* ¶ 197) are generic and generalized motive allegations of the type that courts have repeatedly held contribute no inference of scienter. *See, e.g., Eizenga*, 124 F. Supp. 2d at 986 ("[A]ssertions that would almost universally be true, such as the desire to raise capital, . . . economic self-interest, and the desire to . . . protect one's executive position" are "inadequate of themselves to plead motive.") (*quoting Coates*

[33] Plaintiff's allegation that the SEC is investigating Thompson's and PE Defendants' stock sales (Compl. ¶ 196) also fails to support a strong inference of scienter. *See, e.g.*, *NECA–IBEW Pension Fund v. Hutchinson Tech., Inc.*, 536 F.3d 952, 962 (8th Cir. 2008) ("The mere existence of an SEC investigation does not suggest that any of the allegedly false statements were actually false . . . [,] nor does it add an inference of scienter."); *City of Austin Police Ret. Sys. v. ITT Educ. Servs., Inc.*, 388 F. Supp. 2d 932, 942 (S.D. Ind. 2005) ("[T]he mere existence of [a regulatory investigation] cannot support any inferences of wrongdoing or fraudulent scienter on the part of the company or its senior management.").

v. Heartland Wireless Communications, Inc., 55 F. Supp. 2d 628, 644 (N.D. Tex. 1999) (collecting cases)); *Tuchman*, 14 F.3d at 1068-69 ("It does not follow that because executives have components of their compensation keyed to performance, one can infer fraudulent intent."); *Shaw Grp.*, 537 F.3d at 543 ("To demonstrate motive, plaintiffs must show concrete benefits that could be realized by one or more of the false statements and wrongful nondisclosures alleged."). The more compelling inference derived from Thompson's desire to minimize expenses is simply that he was a competent steward of SolarWinds' financials.

E. Allegations about the general importance of cybersecurity and post Cyberattack reforms fail to raise a strong inference of scienter.

Plaintiff's hindsight allegations about post-Cyberattack security reforms SolarWinds is implementing (Compl. ¶¶ 198, 168–75) say nothing about Defendants' relevant knowledge at the times the challenged statements were made and thus do not support a strong inference of scienter. *See Southland*, 365 F.3d at 383; *Abrams*, 292 F.3d at 432; *In re Marriott*, 2021 WL 2407518, at *39. Likewise, Plaintiff's allegations that SolarWinds "repeatedly discussed the importance of cybersecurity" (Compl. ¶ 186), that cybersecurity was "critical" to SolarWinds' customers (*id.* ¶ 189), and that Brown had responsibilities for oversight of cybersecurity matters (*id.* ¶ 188) suffer the same deficiency and fail to raise a strong inference of scienter. *See Heartland,* 2009 WL 4798148, at *7 ("[I]t is not automatically assumed that a corporate officer is familiar with certain facts just because these facts are important to the company's business; there must be other, individualized allegations that further suggest that the officer had knowledge of the fact in question."); *In re Marriott*, 2021 WL 2407518, at *41 ("[W]ithout additional detailed allegations regarding the Individual Defendants, [allegations about defendants' positions] do not establish an inference, let alone a strong one, that any of the Individual Defendants knew or was reckless in not knowing that any of their statements were false or misleading."); *Abrams*,

292 F.3d at 432 ("[A] pleading of scienter may not rest on the inference that defendants must have been aware of the misstatement based on their positions within the company.").

* * *

All told, the Complaint fails to raise a strong inference that Thompson or Brown—the only persons alleged to have made or approved any of the challenged statements—acted with intent to defraud or severe recklessness. Nor, for that reason, is Plaintiff able to allege scienter on the part of SolarWinds. Rather, the far more cogent and compelling inference is that the Individual Defendants were responsible stewards of a growing business operating in an industry distinctly susceptible to the risk of sophisticated cyber espionage, particularly where (i) there are no particularized facts alleged establishing their contemporaneous knowledge of information conflicting with the challenged statements; (ii) SolarWinds warned investors that its systems were "vulnerable" to precisely the sort of sophisticated cyberattack that befell the Company; and (iii) Plaintiff fails to plead any plausible motive for the SolarWinds Defendants to seek to defraud investors, or any sales of SolarWinds stock by the key executive alleged to have been responsible for oversight of the Company's "security architecture" and "infrastructure"—*i.e.*, Tim Brown. *See In re Marriott*, at *41–42. Accordingly, the Complaint must be dismissed.

II. Plaintiff fails to plead that SolarWinds made a materially false or misleading statement.

Plaintiff filed a lengthy 270-paragraph complaint, yet it alleges only five alleged misstatements: (1) certain aspects of SolarWinds' "Security Statement" posted on its website (Compl. ¶¶ 201–215); (2) a website page entitled "Security at SolarWinds" (*id.* ¶¶ 216–17); (3) a website page entitled "SolarWinds Trust Center" (*id.* ¶¶ 218–219); (4) Brown's statement in a March 14, 2019 interview (*id.* ¶¶ 220–221); and (5) Brown's statement in an April 30, 2019 interview (*id.* ¶¶ 222–223). None of these statements is pled to have been false or misleading.

A. The challenged statements are immaterial because SolarWinds disclosed the risks of a cyberattack in its SEC filings.

Plaintiff's allegations that SolarWinds made false or misleading statements about its cybersecurity are not actionable because SolarWinds extensively disclosed the risk that a cyberattack could occur despite all of its security measures to try to prevent such an attack. Risk factor disclosures, which the SEC instructs companies to include in their public filings, are prospective "discussion[s] of the most significant factors that make an investment in the [specific company] risky." 7 C.F.R. § 229.105 (Reg. S-K, Item 105). In compliance with this instruction, SolarWinds repeatedly disclosed a security breach could occur and such an attack could harm its business. *See, e.g.*, Biles Decl. Ex. 7, 10/18/18 Prospectus at 25–26.

Plaintiff attempts to sue Defendants claiming their statements about SolarWinds' security protocols were false and misleading, but each of the challenged statements must be read in conjunction with SolarWinds' SEC filings and accompanying risk disclosures, which stated that SolarWinds "could suffer a loss of revenue and increased costs, exposure to significant liability, reputational harm and other serious negative consequences" if it experiences "cyberattacks against [its[systems or against [its] products, or other data security incidents or breaches." Ex. 13, 2/25/19 10-K at 15. Courts have recognized that such risk disclosures "make clear that [a company] was not claiming that its security system was invulnerable." *Heartland*, 2009 WL 4798148, at *5; *see also In re Qudian Inc. Sec. Litig.*, No. 17-CV-9741 (JMF), 2019 WL 4735376, at *8 (S.D.N.Y. Sept. 27, 2019), *reconsideration denied*, No. 17-CV-9741 (JMF), 2020 WL 3893294 (S.D.N.Y. July 10, 2020) (holding that plaintiffs could not plausibly identify a material misrepresentation about the defendant's data security protocols because the company also disclosed the risks of a cybersecurity breach). SolarWinds repeatedly warned investors of the risk of a cybersecurity breach such as the Cyberattack. The eventual occurrence of that event does not constitute securities fraud.

B. The Complaint fails to allege facts to show that the "Security Statement" was materially false or misleading.

The Complaint focuses almost exclusively on the "Security Statement," which was posted several levels deep on SolarWinds' website, not in any SEC filing or investor-directed communication.[34] Plaintiff challenges six statements as false and misleading: (1) SolarWinds had a security team; (2) SolarWinds had an information security policy; (3) SolarWinds provided security training to its employees; (4) SolarWinds had a password policy; (5) SolarWinds had Role Based Access controls and network segmentation; and (6) SolarWinds followed the NIST Cybersecurity Framework. Compl. ¶¶ 201–215.

But Plaintiff's own allegations establish that these challenged statements were neither false nor misleading. For example, Plaintiff asserts that SolarWinds did not have a security team and that "[s]ecurity was not even discussed within the Company" (*id.* ¶¶ 202–203), yet Plaintiff also alleges that Brown was SolarWinds' Vice President of Security (*id.* ¶ 16), quote a statement from Brown discussing his security "team" (*id.* ¶ 220), and allege that Brown "spoke frequently about the Company's supposed cybersecurity" (*id.* ¶ 4). Thus, the Complaint's *own allegations* contradict Plaintiff's conclusory assertions that SolarWinds did not have a security team and did not discuss cybersecurity.

Plaintiff's attempt to leverage media reports to impugn SolarWinds' security procedures reflect blatant cherry-picking and ignore widespread public evidence to the contrary. Post-Cyberattack public statements, including Congressional testimony, demonstrate that SolarWinds' statement that it had a security team was true. In contrast to Plaintiff's conclusory assertions, SolarWinds invested in security at "a level meaningfully higher than the industry average" and hired very experienced professionals to

[34] To be actionable under Section 10(b), a statement must have been made "in a manner reasonably calculated to influence the investing public[,]" such that it can be considered to have been made in connection with the purchase or sale of a security. *SEC v. Tex. Gulf Sulphur Co.*, 401 F.2d 833, 862 (2d Cir. 1968). The Security Statement buried on SolarWinds' website was not such a statement.

strengthen its security team in 2016 and 2017, including Joseph Kim as Chief Technology Officer, Rani Johnson as Chief Information Officer, and Tim Brown as Vice President of Security.[35]

None of the FEs' statements refute the Security Statement's descriptions of precautions SolarWinds took to have a strong infrastructure security. Notably, none of the FEs were in positions to know anything about the Cyberattack or SolarWinds' cybersecurity infrastructure. None of them worked on the Orion Software Platform—which was the only product that was affected in the Cyberattack—or worked on SolarWinds' internal cybersecurity. Instead, the FEs worked on non-Orion products, in sales, in recruitment, or in human resources.[36] Courts have held that former employee's opinions that a company may not have done everything it could have done in the security realm does not render statements about the security in place false. *See, e.g.*, *Heartland*, 2009 WL 4798148, at *5 ("[O]ne former employee's opinion that Heartland did not do everything it could have done to address the security breach does not render the statement 'We place significant emphasis on maintaining a high level of security' false."). This is particularly true when the company also warns "of the possibility of a breach and the consequences of such a breach" in SEC filings. *Id.* The FE statements do not demonstrate that the Security Statement was materially false or misleading.

Similarly, Thornton-Trump's presentation and his alleged knowledge of the security culture at SolarWinds is a red herring. First, the presentation does not identify *any* of the alleged security deficiencies that Plaintiff challenges in the Security Statement—instead, the presentation identifies "four functional areas of security" and states that "[p]arts of these four functional areas exist [at SolarWinds] today." Biles Decl. Ex. 24, Thornton-Trump PowerPoint at PDF p. 11. There is nothing

[35] Biles Decl. Ex. 8, Mr. Thompson, 2/26/21 Congressional Hearing at 12–13; 53; Decl. Ex. 9, 4/25/17 SolarWinds press release.

[36] FE 1 did not work on Orion-based products. Comp. ¶ 84 n.21. FEs 2, 3, 4, 7, 8, 9, and 10 worked in sales. *Id.* ¶¶ 91–93 n.22–24, 98–101 n.27–31. And FEs 5 and 6 worked in recruitment and Human Resources. *Id.* ¶¶ 94–97 n.25–26.

in the presentation that conflicts with any of the challenged statements. Further, Thornton-Trump (who was at SolarWinds for only a few months) quit in May 2017, when he was not promoted, which was approximately 17 months *before* the putative Class Period began. While his soundbites may have appeal for the media covering the Cyberattack, Thornton-Trump's statements do not and cannot render any of the challenged statements in the Security Statement false or misleading during the Class Period because he has no knowledge of the cybersecurity controls in place at SolarWinds many months after he left the Company.

Even if SolarWinds' security was lacking in some areas, or if SolarWinds did not perfectly enforce the security protocols detailed in its Security Statement, SolarWinds' statements are still not materially false or misleading because there is no link between any challenged statement and the Cyberattack. Plaintiff offers only rank speculation to connect the Cyberattack with the challenged statements in the Security Statement, and none of the FEs statements are connected to the Cyberattack.[37] As discussed at length in Congressional hearings and other public forums since the Cyberattack was announced, the Cyberattack was the "largest and most sophisticated operation" that the world has ever seen, and even the best cyber hygiene could not have prevented it. *See supra* Factual Background, Sec. C (discussing the sophisticated nature of the attack). Even Plaintiff's key witness, Thornton-Trump, admitted that data breaches were "inevitable"[38] and that the hackers that carried out the Cyberattack were "so sophisticated it would have been hard for anyone to defend against them." Biles Decl. Ex. 25, 4/16/21 NPR Article at 19. Because Plaintiff has failed to adequately

[37] *See Izadjoo v. Helix Energy Sols. Grp., Inc.*, 237 F. Supp. 3d 492, 511 (S.D. Tex. 2017) (finding that the statements made by confidential witnesses were not "sufficient by itself or taken with the other to allege the material falsity" of the defendant's statements); *In re BP p.l.c. Sec. Litig.*, 852 F. Supp. 2d 767, 795 (S.D. Tex. 2012) (dismissing complaint finding that while plaintiff's theory could "theoretically" be accurate, "Plaintiffs here attempt to draw a connection between temporally disparate events").
[38] Biles Decl. Ex. 24, Thornton-Trump PowerPoint at PDF p. 4.

allege that any of the challenged statements in the Security Statement was connected to the Cyberattack, the challenged statements cannot be materially misleading.

C. Vague statements of corporate optimism are immaterial as a matter of law.

Plaintiff alleges that Brown's statements that SolarWinds had "good basic hygiene" and focused on "heavy-duty hygiene" were false and misleading. Compl. ¶¶ 220–223. But these vague statements are classic corporate puffery that are immaterial as a matter of law. Similarly, the aspirational statements—that SolarWinds "is committed to taking [its] customers security and privacy concerns seriously and makes it a priority" and that it "strive[s] to implement and maintain security processes" on its website (Compl. ¶¶ 216–219)—are merely corporate optimism that cannot be considered materially misleading. As the Fifth Circuit recently reiterated:

> Allegations that amount to little more than corporate 'cheerleading' are puffery . . . and are not actionable under federal securities law because no reasonable investor would consider such statements material and because investors and analysts are too sophisticated to rely on vague expressions of optimism rather than specific facts.

Police & Fire Ret. Sys. of City of Detroit v. Plains All Am. Pipeline, L.P., 777 F. App'x 726, 730 (5th Cir. 2019) (internal quotation marks and citations omitted). For this reason, courts routinely hold that such statements are immaterial as a matter of law. *See In re Intel Corp. Sec. Litig.*, No. 18-cv-00507-YGR, 2019 WL 1427660, at *9 (N.D. Cal. Mar. 29, 2019) (collecting cases holding "vague positive statements which are immaterial as a matter of law").

Further, optimistic statements of opinion like these cannot be false unless (1) the speaker does not "actually hold[] the stated belief," (2) the statements "contain embedded statements of untrue facts," or (3) there are omitted facts that "conflict with what a reasonable investor . . . would take from the statement itself." *Omnicare Inc. v. Laborers Dist. Council Constr. Indus. Pension Fund*, 575 U.S. 175, 176 (2015). "[A] sincere statement of pure opinion is not an 'untrue statement of material fact,' regardless whether an investor can ultimately prove the belief wrong." *Id.* at 186. The Complaint

does not plead falsity under this standard because it is devoid of allegations that Brown did not believe that SolarWinds had good cyber hygiene when he made the challenged statements.

Finally, SolarWinds' general commitments to take security seriously are immaterial as a matter of law. *See, e.g., In re Extreme Networks, Inc. Sec. Litig.*, No. 15-cv-04883-BLF, 2018 WL 1411129, at *23 (N.D. Cal. Mar. 21, 2018) (finding "'commitment' statements are inactionable puffery."); *In re Alphabet, Inc. Sec. Litig.*, No. 18-cv-06245-JSW, 2020 WL 2564635, at *4 (N.D. Cal. Feb. 5, 2020) (finding "generalized statements" about a "general commitment to . . . protect[] [user] data . . . inactionable puffery"), *aff'd In re Alphabet, Inc. Sec. Litig.*, No. 20-15638, 2021 WL 2448223 (9th Cir. June 16, 2021). In other words, no investor "would take such statements seriously in assessing a potential investment, for the simple fact that almost every [similar company] makes these statements." *In re Constellation Energy Grp., Inc. Sec. Litig.*, No. CCB-08-02854, 2012 WL 1067651, at *12 (D. Md. Mar. 28, 2012).

D. The Complaint fails to allege facts showing the Individual Defendants "made" any of the challenged statements.

As noted above, the challenged statements come from five different sources—three website pages and two interviews with Brown. To be held liable for a misstatement or omission under Section 10(b) and Rule 10b-5, the defendant must be the "maker" of the statement, *i.e.*, "the person or entity with ultimate authority over the statement, including its content and whether and how to communicate it." *First Derivative Traders*, 564 U.S. at 142. Notably, company executives are not responsible for every minor statement made in corporate communication. *See Magruder v. Halliburton Co.*, 359 F. Supp. 3d 452, 462–63 (N.D. Tex. 2018) (holding that representations made in press releases and teleconferences must be tied to specific individuals and "[a]llegations that an individual furnished the information for the statement or approved the statement or its making or issuance are sufficient").

Here, the Complaint is devoid of allegations that the Individual Defendants were the "maker" of any of the statements published on SolarWinds' website, and, therefore, they cannot be held liable for the alleged misstatements.

III. Plaintiff fails to adequately plead loss causation.

The Court should dismiss the Complaint because it fails to adequately plead that SolarWinds' stock declined *because of a corrective* disclosure that revealed the *truth* about any of the five challenged statements. *See Dura Pharms.,* 544 U.S. at 342 (requiring plaintiffs to allege facts sufficient to show "a causal connection between the *material* misrepresentation and the loss") (emphasis added); 15 U.S.C. § 78u–4(b)(4). It is not enough for Plaintiff to show that he bought SolarWinds' stock at inflated prices and that the stock price declined after negative news was reported. *See Archdiocese of Milwaukee Supporting Fund, Inc. v. Halliburton Co.*, 597 F.3d 330, 340–41 (5th Cir. 2010).

A. December 14, 2020 Disclosure

Plaintiff alleges the truth of the five challenged statements was "revealed" to the market on three occasions, the first of which was Monday, December 14, 2020,[39] when SolarWinds disclosed it had been the victim of the Cyberattack. *See* Compl. ¶¶ 226–27; Biles Decl. Ex. 15, 12/14/20 8-K. SolarWinds explained that:

> a cyberattack [had] inserted a vulnerability within its Orion monitoring products[,] which … 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 … SolarWinds is cooperating with the Federal Bureau of Investigation, the U.S. intelligence community, and other government agencies in investigations related to this incident.
>
> Based on its investigation to date, SolarWinds has evidence that the vulnerability was inserted within the Orion products and existed in updates released between March and June 2020 … was introduced as a result of a compromise of the Orion software build system and was not present in the source code repository of the Orion products. …

[39] Plaintiff also identifies two disclosures on Sunday, December 13, 2020: (1) a *Reuters* article, and (2) a Cybersecurity and Infrastructure Security Agency ("CISA") emergency directive. Compl. ¶ 225. Although both disclosures suggested that a SolarWinds' product was the source of hack into federal government servers, they provide far less detail than SolarWinds' 8-K released the next day when the markets were open.

> SolarWinds' investigations into these matters are preliminary and on-going, and SolarWinds is still discerning the implications of these security incidents.

The December 14 disclosure is not a *corrective* disclosure because it does not *correct* any of the statements challenged in the Complaint.[40] *See Greenberg v. Crossroads Sys., Inc.*, 364 F.3d 657, 667 (5th Cir. 2004) (stating that the allegedly corrective disclosure was not sufficiently related to prior allegedly false statements about the speed of new routers because the disclosure made "no reference to increased router speed"); *see also In re Dell Inc., Sec. Litig.*, 591 F. Supp. 2d 877, 907–908 (W.D. Tex. 2008) (finding "a corrective disclosure must 'at a minimum … identify which prior representation is called into question'") (citations omitted); *see also In re Marriott*, 2021 WL 2407518, at *44 (rejecting allegations that announcement of data breach was a corrective disclosure). For example, the December 14 disclosure did not disclose that SolarWinds: lacked a "security team" or an "Information Security Policy" (Compl. ¶¶ 203, 205); failed to offer "cybersecurity training to its employees" (*id.* ¶ 207); "did not have a password policy" (*id.* ¶ 209); failed to "limit user authorization or segment [its] networks" (*id.* ¶ 212); or failed to "adhere to the NIST Cybersecurity Framework" (*id.* ¶ 215). Nor did it disclose that SolarWinds failed to "make security a priority" or to "apply appropriate security controls" (*id.* ¶¶ 217, 219).

B. December 15 and 17, 2020 Disclosures

Plaintiff also alleges the Wall Street Journal, Reuters and Bloomberg issued articles on December 15 and 17 that federal agencies "were among those breached" in the Cyberattack and SolarWinds "was previously warned that the password to access the internal server to the Update

[40] *See, e.g.*, Compl. ¶¶ 202, 204, 206, 208, 210–11, 213 (challenging statements in the "Security Statement"); *id.* ¶¶ 216, 218 (challenging statements on SolarWinds' website); *id.* ¶¶ 216, 218 (challenging statements made during two interviews in March and April 2019).

Server" (*i.e.*, "solarwinds123") was "publicly available on the internet." Compl. ¶¶ 229–31.[41] As previously noted, the allegation that an intern violated SolarWinds' internal policies by publicly disclosing a password to a third-party server that was not compromised in the Cyberattack does not render any of the five challenged statements false or misleading. *Supra* Factual Background Sec. D(3). While these reports may have given an unfavorable impression of SolarWinds' security protocols, they do not reveal the falsity of any challenged statement. Plaintiff also fails to explain how these disclosures corrected any challenged statement, other than stating that it revealed the truth "about the nature and extent of SolarWinds' security deficiencies." *Id.* ¶ 224.

* * *

In short, Plaintiff has failed to meet his burden to plead loss causation because the Complaint is devoid of facts connecting the alleged corrective disclosures with any challenged statement. *See Magruder*, 2009 WL 854656, at *15 (finding loss causation was not sufficiently pled because "[d]espite the myriad of statements identified in the subject Complaint, the Plaintiffs simply fail to connect the alleged misrepresentations with correlative corrective disclosures during the Class Period").

IV. Plaintiff has failed to plead control-person liability against the Individual Defendants.

Plaintiff's control-person liability claim under § 20(a) of the Exchange Act must be dismissed because Plaintiff has not pled a primary § 10(b) violation. *See ABC Arbitrage*, 291 F.3d at 348 n.57.

CONCLUSION

For the foregoing reasons, the Court should dismiss the Complaint with prejudice.

[41] Plaintiff also alleges that Microsoft revealed "more than 40 of its customers were victims of the attack," that large IT companies announced that they were "breached as a result of SolarWinds' products," and that Bloomberg reported that "cybercriminals had also infiltrated" federal agencies and "three state governments." *Id.* ¶¶ 232–33.

/s/ Michael J. Biles
Paul R. Bessette
Texas Bar No. 02263050
Michael J. Biles
Texas Bar No. 24008578
Srimath Saliya Subasinghe
Texas Bar No. 24093226
Jessica England
Texas Bar No. 24105841
KING & SPALDING LLP
500 W. 2nd Street, Suite 1800
Austin, TX 78701
Tel: (512) 457-2050
Fax: (512) 457-2100
pbessette@kslaw.com
mbiles@kslaw.com
ssubasinghe@kslaw.com
jengland@kslaw.com

Counsel for SolarWinds Corp., and Tim Brown

CERTIFICATE OF SERVICE

I certify that on August 2, 2021, all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF Filing System on all parties in this case.

/s/ Michael J. Biles
Michael J. Biles