

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION,

Plaintiff,

-v-

SOLARWINDS CORP. & TIMOTHY G. BROWN,

Defendants.

23 Civ. 9518 (PAE)

OPINION & ORDER

PAUL A. ENGELMAYER, District Judge:

In this enforcement action, the Securities and Exchange Commission (“SEC”) brings claims against a public company and the head of its information security group arising from the company’s disclosures about its cybersecurity practices.

The SEC contends that SolarWinds Corp. (“SolarWinds” or the “company”), a company that sells high-end and purportedly secure software to governmental and private entities, and Timothy G. Brown, a vice president in charge of the company’s information security, were responsible for two categories of deficient disclosures.

First, the SEC alleges, SolarWinds misleadingly touted its cybersecurity practices and products, including its flagship “Orion” software platform, and understated its cybersecurity risks. SolarWinds did so, the SEC contends, in a “Security Statement” on its website, and in a range of other public statements, including filings required under the securities laws. In fact, the SEC contends, SolarWinds hid the fact that its products and practices had porous cybersecurity. The SEC contends that the company’s hype misled the investing public to believe that SolarWinds’ central software product had minimal vulnerability to cyberattacks.

Second, the SEC alleges, SolarWinds misled the investing public about a series of cyberattacks. These attacks culminated in the revelation, in December 2020, that the company and its customers had been victims of a large-scale cyberattack, known as SUNBURST, which was (and is) believed to have been conducted by state-sponsored hackers in Russia. Because SUNBURST had targeted the Orion software platform for months, customers had unknowingly purchased a corrupted product from SolarWinds that was susceptible to exploitation by the hackers. The SEC contends that, in SUNBURST's immediate aftermath, SolarWinds minimized the scope and severity of the attack, including by omitting that customers had previously reported similarly malicious activity involving the Orion product.

Based on these two sets of disclosures—which the Court terms the “pre-SUNBURST” and “post-SUNBURST” disclosures—the SEC brings claims against SolarWinds and Brown.

Some claims are based on statutory and regulatory grounds familiar to SEC enforcement actions. These claims are brought pursuant to Section 10(b) of the Securities Exchange Act of 1934 (“Exchange Act”), 15 U.S.C. § 78j(b), and its implementing rule, Rule 10b-5(b); Section 13(a) of the Exchange Act, 15 U.S.C. § 78m(a), and its implementing rules, Rules 12b-20, 13a-1, 13a-11, and 13a-13; and Section 17(a) of the Securities Act of 1933 (“Securities Act”), 15 U.S.C. § 77q(a). These claims are based on alleged material misrepresentations and omissions by SolarWinds, including in—depending on the claim—the Security Statement; the cybersecurity risk disclosure in the company's SEC filings, including its Form S-1 registration; press releases, podcasts, and blog posts; and the Form 8-Ks it filed immediately after revelation of the SUNBURST cyberattack, on December 14 and 17, 2020.

Other claims fault SolarWinds for ineffective internal controls and procedures. In one claim, brought under Section 13(b)(2)(B) of the Exchange Act, the SEC alleges, based on the

company's deficient cybersecurity, that SolarWinds failed to "devise and maintain a system of internal accounting controls." 15 U.S.C. § 78m(b)(2)(B). As the SEC acknowledges, this case is the first in which it has brought an accounting control claim based on an issuer's cybersecurity failings.<sup>1</sup> In another claim, brought under Exchange Act Rule 13a-15(a), the SEC contends that SolarWinds had ineffective "disclosure controls and procedures." 17 C.F.R. § 240.13a-15(1).

Defendants now move to dismiss all claims in the SEC's Amended Complaint ("AC") for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6). Defendants' motion has drawn support from numerous industry and public policy amici. The SEC opposes the motion.

For the reasons that follow, the Court denies in part, but grants in large part, the motion to dismiss.

As to pre-SUNBURST disclosures, the Court sustains the SEC's claims of securities fraud based on the company's Security Statement. That statement is viably pled as materially false and misleading in numerous respects. The Court, however, dismisses the claims of securities fraud and false filings based on other statements and filings.

As to post-SUNBURST disclosures, the Court dismisses all claims. These do not plausibly plead actionable deficiencies in the company's reporting of the cybersecurity hack. They impermissibly rely on hindsight and speculation.

Finally, the Court dismisses as ill-pled the SEC's claims relating to SolarWinds' internal accounting and disclosure controls and procedures.

---

<sup>1</sup> In July 2023, the SEC adopted new cybersecurity rules. These require the disclosure of material cybersecurity incidents and annual disclosure of cybersecurity risk management, strategy, and governance. *See* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896 (Aug. 4, 2023) (codified at 17 C.F.R. §§ 229.106, 232, 239, 240, 249). These new rules are not implicated in this case, which involves conduct predating the new rules' effective date.

## I. Factual Background<sup>2</sup>

### A. Nature of SolarWinds' Business

SolarWinds is a publicly traded company incorporated under Delaware law and headquartered in Austin, Texas. Dkt. 85 (“AC”) ¶ 21. It designs and sells software used by companies, and federal, state, and foreign governments, to manage their computer systems. *Id.* ¶ 43. Between October 2018 and January 12, 2021 (the “Relevant Period”), *id.* ¶ 1, SolarWinds had more than 300,000 customers, including 499 companies within the Fortune 500. *Id.* ¶ 43. SolarWinds’ products provide information technology professionals with the ability to “detect, diagnose, and resolve network performance issues.” *Id.* Its flagship product, “Orion,” is an information technology infrastructure and management platform. *Id.* ¶ 44. Orion accounted for 45% of SolarWinds’ revenue during the first nine months of 2020. It was considered one of the company’s “crown jewels.” *Id.*

### B. July 2017: Brown Joins SolarWinds

In July 2017, SolarWinds hired Brown as vice president of security and architecture and the head of its information security group (“infosec”). *Id.* ¶¶ 5, 22. He reported directly to the chief information officer (“CIO”). *Id.* ¶ 243. On joining the company, Brown learned of

---

<sup>2</sup> These facts are drawn primarily from the AC. For the purpose of resolving the motion to dismiss, the Court assumes all well-pled facts to be true and draws all reasonable inferences in favor of plaintiffs. *See Koch v. Christie’s Int’l PLC*, 699 F.3d 141, 145 (2d Cir. 2012). The Court also considers documents incorporated into the AC by reference, documents publicly filed with the SEC, *see ATSI Commc’ns, Inc. v. Shaar Fund, Ltd.*, 493 F.3d 87, 98 (2d Cir. 2007), and other “matters of which a Court may take judicial notice,” *In re Pfizer, Inc. Sec. Litig.*, 538 F. Supp. 2d 621, 627 (S.D.N.Y. 2008). Because all documents attached to defendants’ declaration in support of dismissal and the SEC’s declaration in opposition fall into at least one of these categories, the Court considers them in resolving this motion. *See* Dkts. 91–92 (“Turner Decl.”); Dkt. 103 (“Ney Decl.”); Dkt. 109 (“Second Turner Decl.”).

SolarWinds' poor cybersecurity practices. *Id.* ¶ 45. Shortly after, he gave two internal presentations that highlighted the company's weak security.

In August 2017, one month into his tenure, Brown presented a "Security State of the Union" at the monthly information technology leadership meeting. *Id.*<sup>3</sup> In the presentation, Brown flagged that the "[c]urrent state of security leaves us in a very vulnerable state for our critical assets. A compromise in these assets would damage our reputation and [us] financially." *Id.* He stated that SolarWinds needed to "reduce the number of security incidents by implementing industry standard best practices." *Id.* "Appropriate security policies, procedures, training, [and] PEN testing," he stated, "are required by our commercial customers and asked for in qualifying questionnaires." *Id.* ¶ 47. Brown warned that "[w]ithout appropriate answers we will lose business," noting that the company had recently lost a renewal because it used "free code scanning tools that did not find all vulnerabilities." *Id.*

On September 7, 2017, Brown circulated a similar presentation to other SolarWinds employees. *Id.* ¶ 48. He described the presentation as capturing the "[c]urrent state of security and proposed move to a proactive security model." *Id.* The presentation contained multiple slides assessing cybersecurity measures in SolarWinds' three business segments—Core IT, MSP, and Cloud.<sup>4</sup> *Id.* ¶ 49. The slides used bright green, yellow, gray, and red color-coding. Red boxes reflected areas that needed "more work" or related to a security measure that was "not yet deployed." *Id.* Among the areas coded in red were "Security Training [E]mployee," "Data

---

<sup>3</sup> The AC does not definitively plead that Brown delivered this section of the presentation. Because the start of the presentation prominently featured a picture of Brown, the Court infers that Brown was the presenter. *Id.* ¶ 45.

<sup>4</sup> The MSP, or "Managed Service Provider," unit focused on providing services and products to SolarWinds' customers who are managed service providers—companies that used SolarWinds' products to provide network management services to end users. *Id.* ¶ 125.

Classification,” and “P[enetration] [T]esting.” *Id.* With respect to “Identity Management,” the presentation noted “many gaps” in all three business lines, as well as “inconsistent management” in the CoreIT business line. *Id.* ¶ 53. The presentation warned that a “[l]ack of legally approved security questions/answers [is] costing us time and customers.” *Id.* ¶ 51. Brown also stated that there was a need to “[l]ock down our critical assets that could cause a major event,” including an exigency to “[l]ock down administrative access and improve identity management processes and procedures.” *Id.* ¶ 53.

### C. Pre-SUNBURST Disclosures

#### 1. Late 2017: The Security Statement is First Posted

In late 2017, without fixing its known cybersecurity problems, SolarWinds decided to post a “Security Statement” on the “Trust Center” section of its website.<sup>5</sup> *Id.* ¶¶ 56, 58. Brown was primarily responsible for creating and approving the Security Statement. *Id.* ¶ 58 (in internal documents, Brown was identified as the “owner” or “approver” of the Security Statement). The Security Statement aimed to provide SolarWinds’ customers with “more information about [its] security infrastructure and practices.” Turner Decl., Ex. 5 (“Sec. Statement”) at 2. Brown and others disseminated the Statement to customers, representing that it recounted how SolarWinds mitigated the risk of cyberattacks. AC ¶¶ 57–58.

SolarWinds’ cybersecurity practices were central to its ability to obtain and retain business. *Id.* ¶ 46. Many customers required their software vendors, like SolarWinds, to respond to detailed security questionnaires before buying new products or renewing contracts for existing products. *Id.* ¶ 47. In his “Security State of the Union,” Brown had identified

---

<sup>5</sup> The AC does not specify when the Security Statement first appeared on the website, stating only that it was in “late 2017,” after Brown’s July 2017 start date and before a December 4, 2017 presentation. *See id.* ¶¶ 58, 62.

SolarWinds' inability to answer such questionnaires as a potential reason for losing business. *Id.* SolarWinds used the Security Statement as its official response to customer questionnaires about its cybersecurity practices. *Id.* ¶ 61.

Among its representations about SolarWinds' cybersecurity practices, the Security Statement stated that it (1) complied with the National Institute of Standards and Technology ("NIST") Cybersecurity Framework for evaluating cybersecurity practices; (2) used a secure developmental lifecycle to create its software products; (3) employed network monitoring; (4) had strong password protections; and (5) maintained good access controls. *Id.* ¶ 72. In fact, the AC alleges, in each of these five areas, SolarWinds, as detailed below, was chronically deficient. The AC alleges that the representations in the Security Statement were at odds with SolarWinds' account of its cybersecurity in internal assessments, presentations, and communications. An employee described the Security Statement as "aspirational"—capturing what SolarWinds hoped to achieve in the future. *Id.* ¶ 57. And on December 14, 2017, shortly after the Security Statement was published, Brown emailed a presentation to SolarWinds' CIO, stating that the company was falling short on cybersecurity measures including penetration testing, security training, and data classification. *See id.* ¶ 62 (categories highlighted red). The presentation repeated warnings from the August and September 2017 presentations, including that the "[c]urrent state of security leaves us in a very vulnerable state for our critical assets." *Id.* ¶ 63. In January 2018, managers complained that "we don't do some of the things that are indicated in" the Security Statement. *Id.* ¶ 65.

## 2. Statements Made in Connection with the October 2018 IPO<sup>6</sup>

On October 2018, SolarWinds became a publicly traded company through an Initial

---

<sup>6</sup> SolarWinds' Security Statement was posted on its website and was virtually unchanged at all relevant times, including after the IPO. *Id.* ¶ 71.

Public Offering (“IPO”), and registered as such by filing a Form S-1 registration statement. *Id.*

¶ 1.<sup>7</sup> This registration statement contained the following lengthy cybersecurity risk disclosure.

**If we sustain system failures, cyberattacks against our systems or against our products, or other data security incidents or breaches, we could suffer a loss of revenue and increased costs, exposure to significant liability, reputational harm and other serious negative consequences.**

We are heavily dependent on our technology infrastructure to sell our products and operate our business, and our customers rely on our technology to help manage their own IT infrastructure. Our systems and those of our third-party service providers are vulnerable to damage or interruption from natural disasters, fire, power loss, telecommunication failures, 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 the number, intensity and sophistication of attempted attacks, and intrusions from around the world have increased. In addition, sophisticated hardware and operating system software and applications that we procure from third parties may contain defects in design or manufacture, including “bugs” and other problems that could unexpectedly interfere with the operation of our systems.

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, we may be unable to anticipate these techniques or 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, 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. Our remediation efforts may not be successful and could result in interruptions, delays or cessation of service and loss of existing or potential customers that may impede

---

<sup>7</sup> SolarWinds had conducted an IPO in 2009 and was a public company until February 2016, when it was acquired by private equity firms and taken private. *Id.* ¶ 21. SolarWinds has remained public since its second IPO in October 2018. *Id.* ¶¶ 21, 239.

sales of our products or other critical functions. We could lose existing or potential customers in connection with any actual or perceived security vulnerabilities in our websites or our products.

During the purchasing process and in connection with evaluations of our software, either we or third-party providers collect and use customer information, including personally identifiable information, such as credit card numbers, email addresses, phone numbers and IP addresses. We have legal and contractual obligations to protect the confidentiality and appropriate use of customer data. 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. We have incurred and expect to incur significant expenses to prevent security breaches, including deploying additional personnel and protection technologies, training employees, and engaging third-party experts and consultants. Our errors and omissions insurance coverage covering certain security and privacy damages and claim expenses may not be sufficient to compensate for all liabilities we incur.

Turner Decl., Ex. 1 (“Form S-1”) at 3–4.

SolarWinds thereafter repeated (or incorporated by reference) the same risk disclosure in the following public filings during the Relevant Period: (1) Form 10-Q Quarterly Report (filed Nov. 27, 2018); (2) Form 10-K Annual Report (Feb. 25, 2019); (3) Form S-8 Registration Statement (Apr. 11, 2019); (4) Form 10-Q (May 10, 2019); (5) Form S-1 Registration Statement (May 20, 2019); (6) Form 10-Q (Aug. 12, 2019); (7) Form 10-Q (Nov. 7, 2019); (8) Form S-8 (Dec. 11, 2019); (9) Form 10-K (Feb. 24, 2020); (10) Form S-8 (Feb. 24, 2020); (11) Form 10-Q (May 8, 2020); (12) Form 10-Q (Aug. 10, 2020); (13) Form 10-Q (Nov. 5, 2020). AC ¶ 251.<sup>8</sup>

---

<sup>8</sup> A Form 10-Q is a quarterly report that “provides a continuing view of the company’s financial position during the year and generally includes unaudited financial statements.” *In re Lottery.com, Inc. Sec. Litig.*, No. 22 Civ. 07111 (JLR), 2024 WL 454298, at \*4 n.2 (S.D.N.Y. Feb. 6, 2024) (citation omitted). A Form 10-K is an annual report “intended to detail the financial condition and performance of a particular company for an annual period in a comprehensive manner.” *Id.*

Brown was among the people responsible for the technical content and accuracy of the risk disclosure. *Id.* ¶ 242. During the SEC’s investigation, Brown testified that, although he did not review the precise disclosure language SolarWinds used in its SEC filings, he was asked factual questions, reviewed documentation, and provided information that he understood would be used to create SolarWinds’ risk disclosure in these filings. *Id.*

**3. 2018–2020: Statements Made in Company Press Releases, Blog Posts, Podcasts, and Presentations**

SolarWinds and Brown highlighted the company’s purportedly robust cybersecurity practices in presentations, podcasts, blog posts, and press releases between 2018 and 2020. *Id.* ¶ 219.

In September 2018, Brown delivered a presentation to SolarWinds’ MSP customers, titled, “Embrace Partnerships to Provide Effective Security.” *Id.* ¶ 220. It stated:

- The “majority of breaches still result from bad cyberhygiene.”
- Companies need to “[m]anage identities and know who has access.”
- “We protect our customers and their customers.”
- Companies need to evaluate risk and plan accordingly.

*Id.* The presentation displayed a screenshot of the company’s Security Resource Center, the part of its website where the Security Statement was maintained. *Id.* In a March 2018 podcast episode discussing cybersecurity practices, Brown stated that the company was “focused on . . . heavy-duty hygiene.” *Id.* ¶ 221. In a 2020 blogpost, Brown represented that the company “places a premium on the security of its products and makes sure everything is backed by sound security processes, procedures, and standards.” *Id.* ¶ 222. The blogpost included a hyperlink to the Trust Center of SolarWinds’ website containing the Security Statement. *Id.*

SolarWinds also issued official press releases touting its commitment to cybersecurity. An October 7, 2019 press release, for example, stated that the company “equips technology professionals with tools to help monitor, manage, and secure today’s complex IT environments.” *Id.* ¶ 223. The press release included a statement from Brown that “SolarWinds is committed to helping IT and security teams by equipping them with powerful, affordable solutions that are easy to implement and manage. Good security should be within the reach of all organizations.” *Id.* A December 12, 2019 press release touted “SolarWinds’ commitment to high security standards, which its partners rely on to help keep the systems they manage secure and compliant.” *Id.* ¶ 224. It included statements by Brown that SolarWinds and its employees “are always striving to give our partners a leading edge while also fostering a community built on a bedrock of trust,” and that meeting security standards “demonstrate[s] a vendor’s commitment to privacy and security—something we always strive to improve upon in all we do.” *Id.*

#### **D. The SEC’s Evidence of SolarWinds’ Cybersecurity Deficiencies**

In contrast to the company’s public statements, the AC alleges that SolarWinds and Brown knew, between 2017 and 2020, that its cybersecurity apparatus was deeply flawed. It recounts evidence gleaned by the SEC—including from internal assessments, presentations, and employee communications—that it contends document these deficiencies and contradict the company’s public statements.

##### **1. Evidence Contradicting the Security Statement**

###### *a. NIST Cybersecurity Framework*

The Security Statement represented that SolarWinds “follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect and respond to security incidents.” Sec. Statement at 2. The NIST Cybersecurity Framework is “a set of tools that an organization can use as one part of its assessment of its cybersecurity posture.” AC ¶ 74.

Companies using the framework measure themselves on a scale of “0” to “5” in five areas: “Identify, Detect, Protect, Respond, and Recover.” *Id.* ¶ 75.<sup>9</sup> Companies can also measure themselves on sub-areas within each of the five core areas. *Id.* When compiled, these ratings are sometimes referred to as the “NIST Scorecard.” *Id.* SolarWinds applied the NIST Framework to assess its three main business units: CoreIT; MSP; and Monitoring Cloud. *Id.* ¶ 79. The AC alleges that, as reflected in its annual NIST scorecards, SolarWinds scored poorly on these internal assessments.

i. 2017 NIST assessment

The 2017 NIST Cybersecurity Framework, predating SolarWinds’ IPO, assessed several subareas within the five core areas of Identify, Detect, Protect, Respond, and Recover, with each of SolarWinds’ three business components receiving a separate score.

Several subareas were rated as “0”—meaning either that there was no evidence the company was meeting the security control objective or that the security control objective was unassessed. *Id.* ¶ 80. These included:

- Identify–Business Environment (all three components)
- Protect–Awareness and Training (Monitoring Cloud)
- Detect–Security Continuous Monitoring (Monitoring Cloud).

*Id.* Several subareas were rated as “1”—meaning the company had “an ad-hoc, inconsistent, or reactive approach to meeting the security control objectives.” *Id.* ¶ 81. These included:

---

<sup>9</sup> A score of “0” means “[t]here is no evidence of the organization meeting the security control objectives or [it] is unassessed.” *Id.* ¶ 80. A score of “1” means “[t]he organization has an ad-hoc, inconsistent, or reactive approach to meeting the security control objectives.” *Id.* ¶ 81. A score of “2” means the organization “has a consistent overall approach to meeting the security control objectives, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.” *Id.* ¶ 128. The AC does not allege what a score of “4” or “5” means.

- Identify–Risk Assessment (CoreIT and MSP)
- Protect–Awareness and Training (CoreIT and MSP)
- Protect–Data Security (all three components)
- Protect–Information Protection Processes and Procedures (MPS and Monitoring Cloud)

*Id.*

ii. 2018 NIST assessment

On October 1, 2018, weeks before the IPO, a senior infosec manager (“Manager E”) sent an email to several SolarWinds’ employees, including Brown, with an updated NIST Cybersecurity Framework assessment. *Id.* ¶ 83.<sup>10</sup> Several subareas were again rated as “0”: Protect–Maintenance (Cloud); Detect–Security Continuous Monitoring (Cloud); Detect–Detection Processes (Cloud). *Id.* ¶ 84. Within these sub-areas, 100 specific controls were rated. *Id.* ¶ 85. More than 25 specific controls were scored as “0.” *Id.* These included:

- “Threat and vulnerability information is received from information sharing forums and sources” (Cloud)
- “The development and testing environment(s) are separate from the production environment” (Cloud)
- “Malicious code is detected” (Cloud)

*Id.* The subareas rated as “1” included: Identify–Risk Assessment (Cloud); Protect–Awareness and Training (all three components); Detect–Anomalies and Events (Cloud). *Id.* ¶ 86. More than 50 specific controls were scored as “1.” These included:

- “Asset vulnerabilities are identified and documented” (Cloud)

---

<sup>10</sup> Manager E “was one of two SolarWinds employees who reported directly to Brown during the Relevant Period.” *Id.* ¶ 27.

- “Access permissions are managed, incorporating the principles of least privilege and separation of duties” (all three components)
- “All users are informed and trained” (all three components)
- “Senior executives understand roles [and] responsibilities” (all three components)

*Id.* ¶ 87.

iii. 2019 NIST Assessment

The 2019 NIST Cybersecurity Framework presented to senior executives contained significantly less detail than the 2017 and 2018 NIST scorecards. *Id.* ¶ 90. SolarWinds received a score of “1” for the “Authentication, Authorization and Identity Management” subcategory. *Id.* It received a score of “2” for the “Recover” category and for the “Secure Software Development Lifecycle” subcategory. *Id.*

iv. NIST 800-53 Assessment

In 2019, SolarWinds also used a more specialized NIST assessment—the NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information System and Organization (“NIST 800-53”). *Id.* ¶ 93. It used the NIST 800-53 to “evaluate whether certain of its products could be certified as compliant with the Federal Risk and Authorization Management Program” (“FedRAMP”). *Id.* ¶ 97.

This assessment “revealed multiple programmatic failures at an organizational level that directly contradict the Security Statement and placed SolarWinds at materially increased risk of a cybersecurity incident.” *Id.* ¶ 98. Of the 325 controls tested, SolarWinds identified only 21 (6%) as having a “program/practice in place” and 198 (61%) as having “[n]o program/practice in place.” *Id.* ¶ 99. The remaining 106 controls (33%) fell into the category of “[p]rogram/[p]ractice *may* be in place but requires detailed review.” *Id.*

b. *Secure Development Lifecycle*

The Security Statement also touted that SolarWinds followed a “Secure Development Lifecycle” (“SDL”). Sec. Statement at 4. SDL is a “software production methodology . . . that standardizes industry best practices with the goal of creating secure software products. To follow an SDL, a company would need to employ “numerous practices and controls, including training, threat modeling, penetration testing, and security testing.” *Id.* ¶ 110. The AC alleges that SolarWinds consistently failed to follow key aspects of an SDL during the Relevant Period, as it “was still working to determine how to incorporate aspects of an SDL into its product development.” *Id.* ¶ 115.

For example, in January 2018, an engineering manager (“Manager H”) wrote an email to multiple senior managers regarding the Security Statement’s claim that SolarWinds followed an SDL. *Id.* ¶ 117.<sup>11</sup> He wrote: “I’ve gotten feedback that we don’t do some of the things that are indicated in the [Security Statement SDL Section]. I want to make sure that you all have an answer to this. The simple response is: There is improvement needed to be able to meet the security expectations of a Secure Development Lifecycle. We will be working with teams throughout 2018 to begin incorporating the SDL into their development lifecycle.” *Id.* The email then described a plan that “begins with general SDL training,” deploying SDL “pilots,” and working to “roll out the SDL to additional teams each quarter.” *Id.* In May 2018, Manager H sent an email to Brown and SolarWinds’ CIO about deploying SDL: “[Threat Modeling] is a process. It’s part of the SDL and we are just barely beginning to understand how teams are going to be doing this activity.” *Id.* ¶ 119.

---

<sup>11</sup> During the relevant period, Manager H reported to SolarWinds’ chief technology officer (“CTO”). *Id.* ¶ 30.

During the Relevant Period, SolarWinds executives admitted they were not conducting certain SDL component tests that the Security Statement touted—such as penetration testing and security testing. One presentation stated that penetration testing was unfunded in 2018. *Id.*

¶ 121. A December 2018 presentation stated that there was “[n]o formalized testing” for “Product Presentation Testing.” *Id.* A July 2020 internal presentation prepared by Brown, and reviewed by the CIO and CTO, stated that there was “[i]nconsistent internal security testing as part of product final security reviews,” noting that the company did not “always include web application testing before release.” *Id.* ¶ 122. In 2018 and 2019, SolarWinds failed to implement training or threat modelling for important segments of its business. *Id.* ¶ 123.

An August 16, 2019 presentation scored “Secure Software [D]evelopment Lifecycle”—with an objective of “[e]mployees are aware of [and] utilize a security software development lifecycle in their day to day activities”—as a “2” on the NIST Cybersecurity Framework scale. *Id.* ¶ 128. That score meant this was an area where the company “ha[d] a consistent overall approach to meeting the security control objectives, but it [was] still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.” *Id.*

In June 2020, a SolarWinds engineer questioned whether the Orion Improvement Program (“OIP”), a component of the Orion platform, had been developed in a manner consistent with an SDL process. *Id.* ¶ 131. The engineer emailed: “Do we have SDL process enforced for Orion Improvement Program server? If SDL is not enforced for OIP, we should do it ASAP and consider additional actions to make sure that OIP is very well protected.” *Id.* The engineer explained that he was asking this question because he had determined OIP was using a library of software code that he described as “vulnerable.” *Id.* ¶ 132. The code was listed in the U.S. Department of Commerce National Institute of Standards and Technology’s National

Vulnerability Database. *Id.* ¶ 132. In the email, the engineer provided a weblink to the database with an entry identifying the code’s known vulnerability. *Id.* Another engineer responded: “I don’t believe we cover OIP today with the SDL, but we should.” *Id.* The email was forwarded to Brown and the CIO. *Id.* ¶ 131.

*c. Network Monitoring*

The Security Statement made several representations about SolarWinds’ network monitoring, a practice which the AC alleges is vital to overall cybersecurity. Among other things, “it can help prevent or detect threat actors seeking to move laterally within a computer network or exfiltrate files from a network.” *Id.* ¶ 155. The Security Statement stated:

**Change Management**

SolarWinds maintains a change management process to ensure that all changes made to the production environment are applied in a deliberate manner. Changes to information systems, network devices, and other system components, and physical and environment changes are monitored and controlled through a formal change control process. Changes are reviewed, approved, tested and monitored post-implementation to ensure that the expected changes are operating as intended.

...

**Auditing and Logging**

... Network components, workstations, applications and any monitoring tools are enabled to monitor user activity.

...

**Network Security**

Our infrastructure servers reside behind high-availability firewalls and are monitored for the detection and prevention of various network security threats. . . . Next generation firewalls deployed within the data center as well as remote office sites monitor outbound communications for unusual or unauthorized activities, which may be an indicator of the presence of malware (e.g., malicious code, spyware, adware).

Sec. Statement at 3.

In fact, the AC alleges, SolarWinds internally documented numerous network monitoring deficiencies, as reflected by its NIST Cybersecurity Framework assessments.

In 2017 and 2018, SolarWinds gave itself a score of “0” for the Cloud business segment’s “Security Continuous Monitoring” control. AC ¶¶ 149, 150. In 2018, the company gave itself a score of “0” for the Cloud’s “Detection Processes” control—a downgrade from its score of “3” the previous year. *Id.* ¶ 150. In 2018, among the specific controls rated as a “0” for the Cloud included:

- “The network is monitored to detect potential cybersecurity events”
- “Personnel activity is monitored to detect potential cybersecurity events”
- “Malicious code is detected”
- “Unauthorized mobile code is detected”
- “External service provider activity is monitored to detect potential cybersecurity events”

*Id.* ¶ 151.

The 2019 NIST 800-53 assessment documented similar monitoring control failures. It assessed whether “[t]he organization . . . [m]onitors information systems for . . . atypical use . . . and [r]eports atypical usage of information system accounts.” *Id.* ¶ 153. It stated: “GAP. Currently there is no program for this across [SolarWinds].” *Id.* For the control “[t]he organization develops a continuous monitoring strategy and implements a continuous monitoring program,” the assessment stated: “We have no continuous monitoring in place.” *Id.*

Brown sent a September 2018 presentation to the CTO on “Information Security” that used red font to flag that “[a]ctive monitoring and true SOC services” were “[l]imited or non existent.” *Id.* ¶ 152.

*d. Password Policy*

The Security Statement represented that SolarWinds enforced a strong password policy:

We require that authorized users be provisioned with unique account IDs. Our password policy covers all applicable information systems, applications, and databases. Our password best practices enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords. Passwords are individually salted and hashed.<sup>12</sup>

Sec. Statement at 4. During the Relevant Period, SolarWinds' password policy required passwords to (1) be changed every 90 days, (2) have a minimum length of eight characters, and (3) include three of the four following characteristics: uppercase letter, lowercase letter, digit (0–9), and non-alphanumeric character. AC ¶ 160. However, the AC alleges, SolarWinds did not enforce strong password requirements and repeatedly failed to abide by its own password policy. Despite employees'—including Brown's—knowledge of these lapses, they persisted for years, including throughout the Relevant Period. *Id.* ¶ 163.

The AC describes specific instances in which passwords for SolarWinds' products and systems did not comply with the company's internal policy.

In April 2017, an employee emailed the CIO, expressing concern that issues “like ‘default passwords’ are [still] plaguing us when the product has been in the market [for this long].” *Id.* ¶ 164. He described the many “vulnerabilities” as “amateur.” *Id.* ¶ 164. The employee singled out, as an example, that one product had the default password “password.” *Id.*

In September 2019, a compliance employee sent an email to the CIO about security risks embedded in the Cloud product line's main source of authentication. *Id.* ¶ 169. The employee observed: “[p]asswords have no specific parameters, as stated in the IT guidelines”; and “[p]asswords are able to be reused and are not changed at a set number of days.” *Id.* This posed

---

<sup>12</sup> For a password to be “individually salted and hashed,” it must be maintained in an encrypted state. *Id.* ¶ 161.

problems for customers using Cloud products and for SolarWinds' own internal security, as company employees used Cloud-based products for internal authentication. *Id.*

In November 2019, an outside security researcher notified the company that the password to the company's "Akamai" server, used to distribute software updates to customers, was publicly available. *Id.* ¶ 172. The leaked password to the server, "solarwinds123," was formulated in a blatant violation of the company's password policy. *Id.* The researcher warned that a threat actor could use the public password to infect SolarWinds' software updates. He stated: "I have found a public Github repo which is leaking ftp credential belong[ing] to SolarWinds [sic]. . . . Via this any hacker could upload malicious [executable code] and update it with release [of] SolarWinds product." *Id.* Manager E confirmed the security researcher's account. *Id.*

Results from internal audits and NIST Cybersecurity Framework assessments also documented persistent password problems at SolarWinds.

An April 2018 audit identified multiple critical systems that breached the company's password policy. *Id.* ¶ 165. The audit found systems where "shared SQL [structured query language] legacy account login credentials [were] used" in manners contradicting the Security Statement's representation that SolarWinds had unique account IDs for authorized users. *Id.* The audit also revealed database passwords "not encrypted within the configuration file," login credentials "stored in plain text in configuration files," and passwords "stored in plain text on the public web server in the web configuration file and in the system registry of the machine." *Id.* ¶ 166.

Sarbanes-Oxley ("SOX") audits from 2019 and 2020 documented additional instances in which "[p]assword requirements" were not met. *Id.* ¶ 167. Of the 100 controls tested under

SOX, 27 controls relating to information technology were found deficient—many of which were access and password controls. *Id.*

The 2019 NIST 800-53 assessment concluded that for the subcategory “Identification and Authentication”: zero controls were rated “in place”; seven were rated as “may be in place”; and 20 were rated as having “[n]o program/practice in place.” *Id.* ¶ 170.

*e. Access Control*

The Security Statement represented that SolarWinds implemented strong “access controls.” Sec. Statement at 4. The company used the terms “access controls” and “access management” interchangeably. AC ¶ 178. It described access management as “the management of individual identities, their authentication, authorization, roles and privileges within the enterprise in order to minimize security risks associated [with] the use of privileged and non-privileged access.” *Id.*

The Security Statement made several representations about SolarWinds’ access controls.

These included:

**Access Controls**

Role based access controls are implemented for access to information systems. Processes and procedures are in place to address employees who are voluntarily or involuntarily terminated. Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis. Access control lists define the behavior of any user within our information systems, and security policies limit them to authorized behaviors.

...

SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet. Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as defined by our security guidelines. Approvals are managed by workflow tools that maintain audit records of changes.

Sec. Statement at 4.

The AC alleges that SolarWinds' access controls were chronically deficient. Between 2017 and 2020, senior management knew SolarWinds routinely and pervasively granted employees unnecessary "admin" rights, which gave them access to more systems than needed to accomplish their job functions, and thus violated the concept of "least privilege" touted in the Security Statement. AC ¶ 182. The AC alleges that "there is evidence that most employees had 'admin' rights at times during the Relevant Period." *Id.* ¶ 182.

These problems were identified as early as mid-2017, before Brown had joined SolarWinds and before the Security Statement was posted on SolarWinds' website. A June 2017 presentation, prepared by the director of information technology ("Director of IT") and shared with the CIO, described an "unnecessary level of risk" as a result of "too many accounts having admin level access." *Id.* ¶ 184. After Brown joined SolarWinds, he and others presented about insecure access controls and excessive "admin" rights. Brown's August 2017 Security State of the Union warned of the need to "[l]ock down administrative access." *Id.* ¶ 185. A January 2018 presentation—circulated after the Security Statement issued—prepared by a project manager, and shared with Brown, the CIO, the Director of IT, and others, warned: "Currently there is a collection of people who have access to many systems and many people [are] involved in provisioning access." *Id.* ¶ 186. It stated that the "lack of standardized user access management processes . . . create[s] a loss risk of organizational assets and personal data." *Id.* Brown helped prepare a March 2018 presentation, where he warned that the "[c]oncept of least privilege [is] not followed as a best practice" and cautioned against the "[u]se of shared accounts throughout internal and external applications." *Id.* ¶ 187. A month before the IPO, Brown sent the CTO a September 2018 presentation on "Information Security" which flagged "Identity Management–Role and Privilege [M]anagement" as "[l]imited or non existent." *Id.* ¶ 189.

The access control problems persisted after the IPO. A December 2018 presentation, prepared by Manager E, listed as an information security gap that the company had yet to “[d]efine standards and best practices for Role Based Access Controls and Least Privilege,” “[a]ddress the use of local administrator access to non-privileged users,” and “[m]anage, audit, and apply security controls around privileged access.” *Id.* ¶ 191. Brown helped draft Quarterly Risk Review presentations in March and October 2020, which identified as a “key risk” the “[s]ignificant deficiencies in user access management.” *Id.* ¶ 198.<sup>13</sup>

Internal assessments also identified access controls as an area needing improvement. An August 16, 2019 Security and Compliance Program Quarterly Review prepared by Brown, reviewed by the CIO, and received by the CEO, highlighted: “Access and privilege to critical systems/data is inappropriate.” *Id.* ¶¶ 128, 192. It noted that for the control objective “[u]ser identity, authentication and authorization are in place and activity monitored across the company,” SolarWinds had received a NIST score of “1”, meaning it had an ad-hoc, inconsistent, or reactive approach to meeting that cybersecurity control objective. *Id.*<sup>14</sup> The 2019 NIST 800-53 security controls assessments assessed the subcategory of “[a]ccess controls.” *Id.* ¶ 193. Of the 43 specific access controls evaluated, only two were rated as “in place,” 18 were rated as “may be in place,” and 23 rated as “[n]o program/practice in place.” *Id.* Some controls that SolarWinds assessed as not in place included:

---

<sup>13</sup> Although not noted by the SEC, those same March and October 2020 Quarterly Risk Review presentations also noted that SolarWinds was “[o]n track for overall improvement in 2020” and that its scores for the relevant category had improved—receiving scores of “1.5” in 2017, “3.0” in 2018, and “3.2” in 2019. Turner Decl., Exs. 8–9.

<sup>14</sup> The August 2019 presentation recited NIST scores for 25 controls. Only “Authentication, Authorization and Identity Management” received a score of “1”; every other control evaluated received a score of “2” or higher. Turner Decl., Ex. 7.

Control Evaluated:	Finding:
<p>“The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on . . . organization-defined information flow control policies.”</p>	<p>“Agree with [Product Manager]. This is a gap.”</p>
<p>“The organization explicitly authorizes access to . . . organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information. . . . Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges).”</p>	<p>“We have no explicit authorization policy, nor is this documented that I am aware of for the company or individual products.”</p>
<p>“The organization restricts privileged accounts on the information system to . . . organization-defined personnel or roles.”</p>	<p>“We have no explicit restriction policy, nor is this documented that I am aware of for the company or individual products.”</p>
<p>“The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.”</p>	<p>“This has not been tested/audited, nor is a policy documented.”</p>
<p>“The organization: (a) Limits privileges to change information system components and system-related information within a production or operational environment.”</p>	<p>“No known [privileges] limitations.”</p>

*Id.* ¶ 194.

## 2. VPN Security Weaknesses

In June 2018, an engineer (“Engineer D”) identified a “security gap” in SolarWinds’ virtual private network (“VPN”) that allowed a user with credentials to log on to SolarWinds’ VPN network from a device that was not owned or managed by SolarWinds’ information

technology department. *Id.* ¶ 201.<sup>15</sup> On June 4, 2018, Engineer D emailed multiple employees, including Manager E, describing the current configuration as “not very secure for resources currently accessible via VPN and data stored there,” and making recommendations to address the issue. *Id.* ¶¶ 201–03.<sup>16</sup>

On August 24, 2018, after receiving pushback on his recommendation and seeing no remedial action taken, Engineer D sent a more urgent message to Manager E and the Director of IT. *Id.* ¶ 204. He warned that the security gap “can compromise [the] entire network by spreading malware (spyware, viruses, trojans, ransomware), because we cannot ensure that such device[s] will be fully compliant in terms of [operating system] updates, antivirus [protection], software installed etc.” *Id.* Engineer D stated that the VPN security gap was exacerbated by the fact that many SolarWinds employees had admin rights. He recommended SolarWinds consider “implementing/deploying new systems without full admin rights.” *Id.* ¶ 205.

On August 28, 2018, Engineer D also gave a “VPN Security Gap Presentation.” *Id.* ¶ 206. The presentation stated that an attacker could access SolarWinds’ VPN and upload code without detection, which could serve as a backdoor for future attacks. *Id.* On August 31, 2018, Manager E forwarded Engineer D’s June 4 and August 24, 2018 emails and August 2018 presentation to Brown. *Id.* ¶ 209. Brown did not elevate the matter or alert senior executives to the VPN security issue. *Id.* ¶¶ 209, 211. In January 2020, Manager E again sent Brown the “VPN Security Gap” presentation, noting that the recommendation “did not get any traction” when it was raised in 2018. *Id.* ¶ 210. Despite these warnings, Brown and others aware of the

---

<sup>15</sup> Engineer D is a former SolarWinds employee. *Id.* ¶ 27.

<sup>16</sup> The AC does not allege that Engineer D directly alerted Brown to the VPN security gap.

VPN issue “did not take sufficient steps to ensure that this security gap was either fixed or disclosed.” *Id.* ¶ 211.

### 3. Employee Recognition of Systemic Cybersecurity Deficiencies

SolarWinds employees, including Brown, knew the issues highlighted above “were part of a systemic cybersecurity problem.” *Id.* ¶ 226.

In October 2018, the same month as SolarWinds’ IPO, Brown sent a presentation to SolarWinds’ CIO that warned:

- SolarWinds needed to “[l]ock down [its] critical assets that could cause a major event.”
- The “[c]urrent state of security leaves us in a very vulnerable state for our critical assets.”
- “A compromise of these assets would damage our reputation and [us] financially.”
- “Lack of cyberhygiene leaves us open to being a target of opportunity.”

*Id.* ¶ 227.

On April 15, 2020, a security and compliance manager (“Manager L”) sent Brown an email stating that even the group that directly reported to the CIO was not incorporating cybersecurity practices into its work. She warned: “we have a *systemic issue* around lack of awareness for Security/Compliance requirements with most if not all [of the information technology group’s] projects.” *Id.* ¶ 228. She explained that because cybersecurity “requirements [are] not thought of or ingested upfront, the result is a complete scramble and process piecemeal either right before or after a system is live.” *Id.*

Manager E sent an instant message on November 2020 highlighting his disapproval of the company’s cybersecurity posture: “[W]e’re so far from being a security minded company.

[E]very time I hear about our head geeks talking about security I want to throw up.” *Id.* ¶ 229.

The AC does not allege to whom that message was sent. *Id.*

## **E. Cyber-Attacks Directed to SolarWinds’ Orion Product**

### **1. January 2019: Threat Actors Access SolarWinds’ Network Environment**

In January 2019, unbeknownst at the time to SolarWinds or its employees, threat actors later responsible for the SUNBURST cyberattack accessed SolarWinds’ corporate VPN. They did so by using unmanaged third-party devices and stolen credentials, exploiting the VPN cybersecurity weakness that Engineer D had identified six months earlier. *Id.* ¶ 254. Between January 2019 and November 2020, threat actors repeatedly accessed SolarWinds’ network through a VPN. They “conducted reconnaissance, exfiltration, and data collection; identified product and network vulnerabilities; harvested credentials of SolarWinds employees and customers; and planned additional attacks against SolarWinds’ products.” *Id.* ¶ 255.

By exploiting the VPN connection, these threat actors were able to access SolarWinds’ “entire network.” *Id.* ¶ 256. They were able to “elevate privileges, disable antivirus software, and access and exfiltrate data, including computer code and customer information, without triggering alerts from SolarWinds’ data loss prevention software.” *Id.* They used multiple accounts with administrative privileges to access and monitor emails of SolarWinds’ key personnel without detection. *Id.* Between December 2019 and December 2020, the threat actors “exfiltrat[ed] approximately 7 million emails from more than 70 SolarWinds employees.” *Id.*

In November 2019, threat actors used information gained from their unauthorized access of SolarWinds’ networks to undertake a trial run of the SUNBURST attack. *Id.* ¶ 257. They first inserted non-malicious test code into SolarWinds’ Orion software builds. *Id.* In February 2020, seeing that the test code had gone undetected, they began inserting malicious code. *Id.*

¶ 258. Over the next several months, threat actors inserted malicious code into three different Orion software builds used by approximately 18,000 customers. *Id.* The impacted customers included many federal and state government agencies, and more than 1,500 publicly traded U.S. companies, banks, broker-dealers, accounting firms, and other SEC-regulated entities. *Id.* The malicious code gave threat actors a “backdoor into the network environments of SolarWinds’ customers who downloaded and installed the infected versions of the software to systems that were connected to the internet.” *Id.*<sup>17</sup>

## 2. January to June 2020: Managed Service Provider Product Threats

In early 2020, SolarWinds and Brown learned of an increase in threats to its products and customers. *Id.* ¶ 260. One business unit affected was SolarWinds’ MSP unit, which provides services and products to customers who are themselves managed service providers, and who in turn provide their own network management services to end users, often small or medium-sized companies. *Id.* ¶ 125. In early 2020, at least nine SolarWinds customers who were MSPs suffered attacks through SolarWinds’ MSP products. *Id.* ¶ 261. In all nine attacks, threat actors used accurate credentials on their first attempt to gain access, suggesting that they had obtained customer credentials. The attacks led SolarWinds to investigate whether its database of customer credentials had been compromised. *Id.* SolarWinds was unable to resolve this concern through the investigation. *Id.*

Later that year, in March 2020, SolarWinds learned that threat actors had attacked SolarWinds’ MSP customers using a list of 19,000 single sign-on customers. *Id.* ¶ 262. This suggested that threat actors had information to distinguish between customers who had enabled multi-factor authentication and those who only had single-factor authentication. *Id.* SolarWinds

---

<sup>17</sup> The AC does not allege that SolarWinds knew of these developments at the time.

again was unable to determine how the threat actors had obtained customer credentials and identified the company's single sign-on customers. *Id.* Some employees, including Manager E, theorized that threat actors might have accessed this information through a breach of SolarWinds' systems. *Id.* ¶ 263.

In June 2020, Brown acknowledged to company executives the ongoing problems with SolarWinds' MSP products, including that threat actors had exhibited a high degree of familiarity with these products. *Id.* ¶ 264. Brown gave SolarWinds' CIO and CTO updates on aspects of these ongoing issues. *Id.* In a July 2020 presentation to product managers in the MSP business unit, Brown stated that "SolarWinds [was] no longer under the radar." *Id.* ¶ 291. He stated that threat actors "know N-Central [an MSP product]" and "[k]now how to deploy software, shut off backup etc." *Id.* Brown's presentation described "[distributed denial of service] attacks against marketing sites," "targeted attacks against products," and "sophisticated phishing attacks increasing." *Id.*

SolarWinds considered its MSP products, like its Orion products, "among the Company's 'crown jewels.'" *Id.* ¶ 266. To this end, in a September 2019 interview, Brown had stated:

So, as part of our crown jewels, our MSP business is absolutely, 100-percent at the top of my risk level. They are my risk level, because I realize what access we grant to them. So if you look across my assets at SolarWinds, that is absolutely one of the major crown jewels I watch very closely. Our board watches very closely. That's what we get questions about from our risk committee and others, is "Do we have enough protection around the MSP environment."

*Id.*

### **3. June 2020: Cyberattack on the U.S. Trustee Program**

In May 2020, the U.S. Department of Justice's U.S. Trustee Program ("USTP") installed and evaluated SolarWinds' Orion software on a trial basis before deciding to purchase it. *Id.*

¶ 268.<sup>18</sup> In June 2020, USTP notified SolarWinds about malicious activity the agency had noticed by the Orion software after installation. *Id.* ¶ 269. USTP told SolarWinds that, during the trial installation, the Orion software “reached out to contact websites with an unknown purpose.” *Id.* By June 2020, Brown had become aware of the attack on USTP. *Id.* ¶ 270. In testimony to the SEC, he described the attack as a “unique” and “concerning” incident, because the malicious activity implicated the OIP server, which was a component of the Orion platform. *Id.* ¶¶ 270, 275. The OIP was an internally hosted server—“something inside [the company’s] environment.” *Id.* ¶ 275. Brown reported being concerned that the “traffic going to that [internal] environment looked like a piece of . . . additional software that was installed on the machine that was targeting SolarWinds.” *Id.* Brown explained that the activity reported by USTP “was very unique to that environment because we had never seen anything like this before.” *Id.* The novelty of the activity and the fact that it implicated an internal system concerned Brown.

After investigating the incident, SolarWinds determined that the “BusinessLayer” portion of the Orion software was causing the software “to reach out” and “attempt[] to provide information to the website about the network on which it was located.” *Id.* ¶ 269. SolarWinds also uncovered “evidence that the threat actors who were attacking [USTP] had conducted reconnaissance on the Orion platform since at least mid-2019 and were mimicking SolarWinds’ communication protocols to obfuscate the malicious activity.” *Id.* SolarWinds’ internal investigation, however, “failed to uncover the root cause” of the malicious activity. This prevented SolarWinds from “remediat[ing] the vulnerability.” *Id.* ¶ 270.

---

<sup>18</sup> The AC identifies USTP as “Government Agency A.” The Court refers to the agency by name.

On June 18, 2020, several employees—including an infosec employee (“Employee F”)—engaged in an instant message conversation, in which they discussed the possibility that the USTP attack could reflect an ongoing attack against multiple customers.<sup>19</sup>

Employee: [A]re you aware of any other incident like this where it seems that Orion was used for attack? My biggest concern is that we have [an] exploit somewhere and there are other cases like this but unnoticed.

Infosec Employee F: No. . . . That’s my concern too.

*Id.* ¶ 271.

On July 1, 2020, a member of the engineering team sent Brown an email reporting feeling “spooked” by Orion’s activity at USTP. *Id.* ¶ 272. Brown determined that there were only two possible scenarios: “(1) the attacker was already present on the customer’s system or (2) the attackers were looking closely at Orion ‘for methods to utilize it in larger attacks.’” *Id.* Brown described the incident as “very concerning,” because SolarWinds’ “backends are not that resilient.” *Id.*

The USTP attack was recorded internally under SolarWinds’ Incident Response Plan (“IRP”). *Id.* ¶ 273. As reflected in the chart below, the IRP classified incidents on a scale from “0” (minimal) to “3” (high), with incidents scored as “2” or higher requiring notification of SolarWinds’ CEO and CTO. *Id.*

---

<sup>19</sup> Infosec Employee F is a SolarWinds employee who, at all relevant times, reported directly to Manager E and indirectly to Brown. *Id.* ¶ 28.

IMPACT / RISK LEVEL	CLASSIFICATION LEVEL	DESCRIPTION	IRT REQUIRED
HIGH	3	Affects a significant segment of the SWI customer, disrupts a large segment of IT services, involves the compromise of confidential data, and/or whose impact could have a severe adverse effect on SolarWinds' reputation, revenue, customer(s), partner(s) or the public.	YES
MODERATE	2	Affects multiple SWI customers, involves SWI accounts with elevated privileges, involves a compromise to personal data (under GDPR) or data that should be protected from general access, and/or whose impact could have an adverse effect on SolarWinds' reputation, revenue, customer, partner or the public.	YES
LOW	1	Affects a small SWI customer segment, services of a customer or group of individuals with no sensitive data involved, involves a compromised account with access to non-sensitive data, and/or whose impact could have limited adverse effect on SolarWinds' reputation, revenue, customer(s), partner(s) or the public.	ADVISED
MINIMAL	0	Involves a compromise to public data and/or occurrences of very minor or undetermined security activities or events for which there is no practical follow up.	NO

Turner Decl., Ex. 17 at 3. Under the IRP's internal criteria, an incident was to be scored "2" or higher when it affected multiple customers "whose impact could have an adverse effect on SolarWinds' reputation, revenue, customer, partner or the public." *Id.* This "[i]ncludes a report of compromise for which other customers are susceptible." AC ¶ 273.<sup>20</sup> The USTP attack was scored "0"—a "minimal" incident. Brown thus did not need to notify the CEO or the CTO about the attack, and did not do so.<sup>21</sup>

In the immediate aftermath of the USTP attack report, Brown and others at SolarWinds noted the heightened risks to company products, especially Orion. After an internal investigation of the attack revealed "numerous" vulnerabilities, several employees complained to Brown and other infosec employees that they were inadequately staffed to address the large number of vulnerabilities being identified in June and July 2020. *Id.* ¶ 276. They complained that fixing all

<sup>20</sup> The AC does not specify the origin of this quoted language. It does not appear in the "Security Incident Response Plan Overview," attached as an exhibit to the Turner Declaration.

<sup>21</sup> The AC alleges that the CTO nonetheless learned of the USTP attack, presumably through a different channel. AC ¶ 328.

of the issues identified, even with adequate staffing, would take years. *Id.* During this period, SolarWinds used Risk Acceptance Forms to document instances where cybersecurity-related risks fell outside SolarWinds’ “standard guidelines.” *Id.* ¶ 277. Brown was one of a “small group of people” authorized by SolarWinds to accept and approve such risks. *Id.* In September 2020, a manager from SolarWinds’ engineering team submitted for approval a “Risk Acceptance Form” related to Orion. *Id.* The form requested that SolarWinds “accept[] the risk of legacy issues in the Orion Platform” because “[t]he volume of security issues being identified over the last month have outstripped the capacity of the Engineering teams to resolve [them].” *Id.*

On July 1, 2020, Brown sent an email to the engineering team, describing the increased “activity” that the company was experiencing. He wrote:

We have been getting hit by a lot of activity in the last couple of months. Targeted DDOS attacks against our Websites, Bot nets flooding us with failed login attempts first to Take Control UI and then to Take Control API, multiple account takeovers for MSP admins of N-Central. We are definitely not flying under the radar, because of this I’m thinking that some threat groups may also be looking at Orion.

*Id.* ¶ 292 (emphasis omitted).

#### 4. October 2020: Palo Alto Networks Cyber Intrusion

In October 2020, a second SolarWinds customer, Palo Alto Networks (“PAN”), notified SolarWinds about malicious activity by the Orion software implicating Orion’s BusinessLayer. *Id.* ¶ 279.<sup>22</sup> PAN reported to SolarWinds that it had discovered this activity during an internal “red-team exercise.” Tr. 61.<sup>23</sup> It reported that the Orion software was “reaching out to a website

---

<sup>22</sup> The AC refers to PAN as “Cybersecurity Firm B.”

<sup>23</sup> A red-team exercise is a simulation of an attack, conducted by authorized cybersecurity professionals for testing purposes. *See* NIST, *Computer Security Resource Center Glossary*, [https://csrc.nist.gov/glossary/term/red\\_team](https://csrc.nist.gov/glossary/term/red_team). The AC did not state that PAN had reported to SolarWinds that the malicious activity had been detected during a “red-team exercise.” However, that fact is undisputed, and the SEC, on questioning by the Court, acknowledged it as argument in May 2024. *See* Tr. 61 (“[PAN] reported it to SolarWinds as being part of what they

and downloading a malicious file,” AC ¶ 279. At the time the incident was reported, employees at SolarWinds “recognized and discussed internally that the activity was similar to the activity” reported by USTP. *Id.* Employees on the infosec team “recognized the unique nature of the intrusion and noted that both attacks utilized SolarWinds’ BusinessLayer to reach out to external websites that it should not have been contacting in the ordinary course of operations.” *Id.*

In October 2020, Brown was informed of the PAN incident and the similarities between it and the May 2020 USTP incident. *Id.* ¶ 280. On October 16, 2020, he was forwarded an earlier email (sent October 14, 2020), which stated: “[PAN] in touch with customer support and it seems they had a breach similar to [USTP]. This does not appear to be OIP (that we know of yet) related, but the business layer was used in the attack chain according to them. In this case however it was to do [BusinessLayer] running some malicious download.” *Id.*

On November 5, 2020, more than a dozen employees, not including Brown, engaged in a group instant message conversation. *Id.* ¶¶ 280–81. In it, several employees noted similarities between the two attacks.

---

called a red-team exercise.”). At argument, the SEC revealed that PAN’s November 5, 2020 representation to SolarWinds that it had learned of the malicious activity through a red-team exercise had been untruthful. *See id.*; *see also* Dkt. 124 at 1. PAN, the SEC revealed, had told SolarWinds this falsehood so as not to reveal PAN’s own “cybersecurity problems.” Tr. at 61–62. In a post-argument letter, SolarWinds faulted the SEC for drafting the AC to obfuscate the fact of PAN’s falsehood to SolarWinds. It argued that the SEC’s clarification contradicts the AC’s characterization of the PAN incident as an “attack.” Dkt. 116 at 1–2. In response, the SEC noted that PAN, in reporting the incident to SolarWinds, had advised SolarWinds to treat the situation as if it had involved “an external attacker” and that SolarWinds had internally characterized the incident as a “breach” and as an “attack.” Dkt. 122 at 1–2.

The clarification that PAN had dissembled to SolarWinds as to how it learned of the malicious activity was important. Nevertheless, the fact PAN reported to SolarWinds—that the Orion product, after installation by PAN, had engaged in malicious activity of this nature—was plainly salient information for SolarWinds, regardless of its having been misled as to how it had come to light within PAN.

- “[S]eems similar to [USTP] where BusinessLayer was also used to attack.”
- “We had similar case with [USTP]. BL [Business Layer] was used during an attack.”
- “[Infosec Employee F] was driving the [USTP response], can we g[e]t him on this one as well?”
- “I’m curio[us] what happened on [USTP] and this could be a way to find out.”

*Id.* ¶ 281.

In that same group instant message, an employee raised whether to alert PAN that there had been a prior attack through the BusinessLayer. *Id.* ¶ 282. Infosec Employee F responded: “[I’d] prefer nobody says on the call that we have seen something like this in the past.” *Id.* Infosec Employee F then separately messaged Manager E, who agreed that SolarWinds should not disclose to PAN the previous USTP attack. *Id.* Later that day, on a phone call between SolarWinds and PAN, employees at PAN asked if SolarWinds had ever seen Orion act in this manner before. Infosec Employee F responded that they had not previously seen similar activity from the Orion platform. *Id.* ¶ 283. In contemporaneous instant messages sent during the call, Infosec Employee F messaged his colleague: “Well I just lied.” *Id.* (emphasis omitted).

After the call, PAN strongly encouraged SolarWinds to handle the incident as reflecting “an external attacker.” *Id.* ¶ 284. SolarWinds classified the PAN incident as “0”—a minimal incident—under the IRP, notwithstanding the assessment by some employees that the incident could be related to the USTP attack. *Id.* ¶ 287. Accordingly, the PAN incident was not reported to the CEO or CTO. *Id.* ¶ 328. SolarWinds again failed to uncover the root cause of the malicious activity, preventing it from remedying the vulnerability in the Orion software, which was then being used by thousands of customers worldwide. *Id.* ¶ 287.

Around the time of PAN’s report, Brown and others at SolarWinds again identified heightened risks to SolarWinds’ products. An October 2020 presentation that Brown helped

prepare noted that “SolarWinds was no longer under the radar, that threat actors had specifically targeted SolarWinds’ products, and that threat actors had been conducting reconnaissance against SolarWinds’ products since mid-2019.” *Id.* ¶ 293. An October 2020 Quarterly Risk Review presentation, sent to Brown and others, highlighted that: “Events show that [SolarWinds’] products have [been] explicitly targeted” and that “[t]hreat actors have invested time and have done research and modeling of our products prior to executing attacks.” *Id.* ¶ 295.

In October and November 2020, SolarWinds was informed through the company’s “Zero Day Initiative [program] of at least eight other high-risk vulnerabilities affecting the Orion platform.”<sup>24</sup> *Id.* ¶ 294. In November 2020, an infosec employee sent an instant message to Manager E with a link to a list of more than a dozen high risk vulnerabilities in the Orion platform. *Id.* ¶ 296. He stated: “The products are riddled and obviously have been for many years.” *Id.* The next month, a SolarWinds network engineer complained in an internal message: “We filed more vulnerabilities than we fixed. And by fixed, it often means just a temporary fix . . . but the problem is still there and it’s huge. I have no idea what we can do about it. Even if we started to hire like crazy, which we will most likely not, it will still take years. Can’t really figure out how to unf\*\*k this situation.” *Id.* The AC does not allege to whom that message was sent.

## 5. December 2020: The SUNBURST Attack

In December 2020, a third SolarWinds customer, Mandiant, notified SolarWinds of an attack against its Orion platform. *Id.* ¶ 305.<sup>25</sup> Mandiant identified the Orion platform as the likely means of the attack. Mandiant then reverse-engineered SolarWinds’ Orion software code

---

<sup>24</sup> As part of this initiative, SolarWinds rewarded security researchers who privately reported vulnerabilities. *Id.* ¶ 294.

<sup>25</sup> The AC refers to Mandiant as “Cybersecurity Firm C.”

and identified the root cause of the malicious activity. *Id.* On December 12, 2020, Mandiant contacted SolarWinds' CEO, and reported that SolarWinds had a vulnerability in its Orion product as a result of malicious code that a threat actor had inserted into the Orion software code. *Id.* ¶ 306. That same day, Mandiant shared the decompiled code with Brown and others. *Id.*

On or around December 13, 2020, after reviewing the decompiled code supplied by Mandiant, Brown immediately linked the Mandiant attack to the earlier May 2020 attack against USTP and the October 2020 cyber-incident involving PAN. *Id.* ¶ 307. During the SEC's investigation, Brown testified:

Q: Was there additional analysis that was done to determine that happened in the [PAN] incident and it happened in the [USTP] incident?

A: It wasn't necessary, right? The code that he saw that was dropped that was supplied by [Mandiant], decompiled code gave us a full path. And there is plenty of investigation to show that, okay, business layer host was involved. This was a stream of data—this is what—oh, this matched what [USTP] had seen. So it wasn't trying to attack us, it had a different purpose. So it became very, very apparent extremely quickly that that's what the cases were.

*Id.*

#### **F. Post-SUNBURST Disclosures**

Immediately after confirming Mandiant's report that malicious code had been inserted into the Orion platform, Brown and other executives worked to prepare a Form 8-K publicly reporting this event. *Id.* ¶ 308.<sup>26</sup> Brown participated in drafting the Form 8-K and was responsible for confirming its technical accuracy. *Id.*

---

<sup>26</sup> A Form 8-K is a filing with the SEC announcing, "material corporate events that should be known by the shareholders." *Wyche v. Advanced Drainage Sys., Inc.*, No. 15 Civ. 05955 (KPF), 2017 WL 971805, at \*1 n.1 (S.D.N.Y. Mar. 10, 2017), *aff'd*, 710 F. App'x 471 (2d Cir. 2017) (summary order).

On December 14, 2020, SolarWinds filed a Form 8-K with the SEC that publicly disclosed the SUNBURST attack. The Form 8-K, in relevant part, stated:

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

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 (the “Relevant Period”), 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. SolarWinds has taken steps to remediate the compromise of the Orion software build system and is investigating what additional steps, if any, should be taken. SolarWinds is not currently aware that this vulnerability exists in any of its other products.

SolarWinds currently believes that:

- Orion products downloaded, implemented or updated during the Relevant Period contained the vulnerability;
- Orion products downloaded and implemented before the Relevant Period and not updated during the Relevant Period did not contain the vulnerability;
- Orion products downloaded and implemented after the Relevant Period did not contain the vulnerability; and
- Previously affected versions of the Orion products that were updated with a build released after the Relevant Period no longer contained the vulnerability; however, the server on which the affected Orion products ran may have been compromised during the period in which the vulnerability existed.

. . . On December 13, 2020, SolarWinds delivered a communication to approximately 33,000 Orion product customers that were active maintenance customers during and after the Relevant Period. SolarWinds currently believes the actual number of customers that may have had an installation of the Orion products

that contained this vulnerability to be fewer than 18,000. The communication to these customers contained mitigation steps, including making available a hotfix update to address this vulnerability in part and additional measures that customers could take to help secure their environments. SolarWinds is also preparing a second hotfix update to further address the vulnerability, which SolarWinds currently expects to release on or prior to December 15, 2020. For the nine months ended September 30, 2020, total revenue from the Orion products across all customers, including those who may have had an installation of the Orion products that contained this vulnerability, was approximately \$343 million, or approximately 45% of total revenue.

There has been significant media coverage of attacks on U.S. governmental agencies and other companies, with many of those reports attributing those attacks to a vulnerability in the Orion products. SolarWinds is still investigating whether, and to what extent, a vulnerability in the Orion products was successfully exploited in any of the reported attacks.

. . .

SolarWinds' investigations into these matters are preliminary and on-going, and SolarWinds is still discerning the implications of these security incidents. During the course of these investigations, SolarWinds may become aware of new or different information. At this time, SolarWinds is unable to predict any potential financial, legal or reputational consequences to the Company resulting from this incident, including costs related thereto. So as not to compromise the integrity of any investigations, SolarWinds is unable to share additional information at this time.

Turner Decl., Ex. 2 ("12/14/2020 Form 8-K") at 4–5.

On December 17, 2020, SolarWinds filed a second Form 8-K with the SEC with an update on the SUNBURST attack. This update, in relevant part, stated:

On Saturday, December 12, our CEO was advised by an executive at FireEye of a security vulnerability in our Orion Software Platform which was the result of a very sophisticated cyberattack on SolarWinds. We soon discovered that we had been the victim of a malicious cyberattack that impacted our Orion Platform products as well as our internal systems. While security professionals and other experts have attributed the attack to an outside nation-state, we have not independently verified the identity of the attacker.

Immediately after this call, we mobilized our incident response team and quickly shifted significant internal resources to investigate and remediate the vulnerability. Know that each of our 3,200 team members is united in our efforts to meet this challenge. We remain focused on addressing the needs of our customers, our partners and the broader technology industry.

To accomplish that, we swiftly released hotfix updates to impacted customers that we believe will close the code vulnerability when implemented. These updates were made available to all customers we believe to have been impacted, regardless of their current maintenance status. We have reached out and spoken to thousands of customers and partners in the past few days, and we will continue to be in constant communication with our customers and partners to provide timely information, answer questions and assist with upgrades.

We are solely focused on our customers and the industry we serve. Our top priority has been to take all steps necessary to ensure that our and our customers' environments are secure. We are taking extraordinary measures to accomplish this goal. We shared all of our proprietary code libraries that we believed to have been affected by SUNBURST to give security professionals the information they needed to do their research. We also have had numerous conversations with security professionals to further assist them in their research. We were very pleased and proud to hear that colleagues in the industry discovered a "killswitch" that will prevent the malicious code from being used to create a compromise.

Here are a few important things to know:

- This was a highly sophisticated cyberattack on our systems that inserted a vulnerability within our Orion® Platform products. This particular intrusion is so targeted and complex that experts are referring to it as the SUNBURST attack. The vulnerability has only been identified in updates to the Orion Platform products delivered between March and June 2020, but our investigations are still ongoing. Also, while we are still investigating our non-Orion products, to date we have not seen evidence that they are impacted by SUNBURST.
- The vulnerability was not evident in the Orion Platform products' source code but appears to have been inserted during the Orion software build process.
- We swiftly released hotfix updates to impacted customers, regardless of their maintenance status, that we believe will close the vulnerability when implemented.
- After our release of Orion 2020.2.1 HF2 on Tuesday night, we believe the Orion Platform now meets the US Federal and state agencies' requirements. We are providing direct support to these customers and will help them complete their upgrades quickly.
- We are continuing to take measures to ensure our internal systems are secure, including deploying the Falcon Endpoint Protection Platform across the endpoints on our systems.

- We have retained industry-leading third-party cybersecurity experts to assist us with this work and are actively collaborating with our partners, vendors, law enforcement and intelligence agencies around the world.

Turner Decl., Ex. 3 at 3 (“12/17/2020 Form 8-K”).

Finally, on January 11, 2021, SolarWinds filed a third Form 8-K, reporting additional information and findings from its investigation of the SUNBURST attack. It stated:

**New Findings from our Investigation of SUNBURST**

Since the cyberattack on our customers and SolarWinds, we have been working around the clock to support our customers. As we shared in our recent update, we are partnering with multiple industry-leading cybersecurity experts to strengthen our systems, further enhance our product development processes and adapt the ways that we deliver powerful, affordable AND secure solutions to our customers.

We are working with our counsel, DLA Piper, CrowdStrike, KPMG and other industry experts to perform our root cause analysis of the attack. As part of that analysis, we are examining how the SUNBURST malicious code was inserted into our Orion Software Platform and once inserted, how the code operated and remained undetected.

Today we are providing an update on the investigation thus far and an important development that we believe brings us closer to understanding how this serious attack was carried out. We believe we have found a highly sophisticated and novel malicious code injection source that the perpetrators used to insert the Sunburst malicious code into builds of our Orion Software Platform.

...

**Highly sophisticated and complex malware designed to circumvent threat detection**

As we and industry experts have noted previously, the SUNBURST attack appears to be one of the most complex and sophisticated cyberattacks in history. The US government and many private-sector experts have stated the belief that a foreign nation-state conducted this intrusive operation as part of a widespread attack against America’s cyber infrastructure. To date, our investigations have not independently verified the identity of the perpetrators.

Analysis suggests that by managing the intrusion through multiple servers based in the United States and mimicking legitimate network traffic, the attackers were able to circumvent threat detection techniques employed by both SolarWinds, other private companies and the federal government. The SUNBURST malicious code

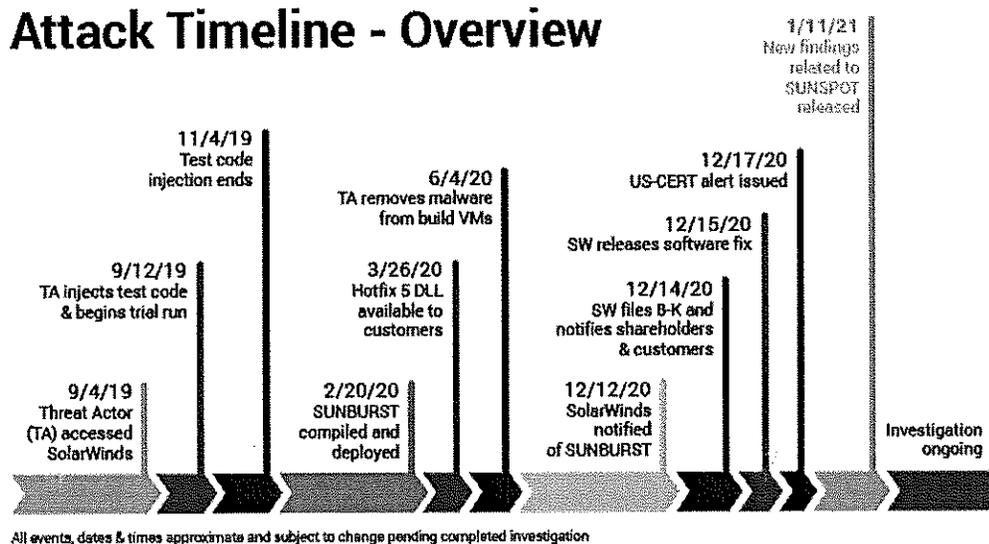
itself appears to have been designed to provide the perpetrators a way to enter a customer’s IT environment. If exploited, the perpetrators then had to avoid firewalls and other security controls within the customer’s environment.

KPMG and CrowdStrike, working together with the SolarWinds team, have been able to locate the malicious code injection source. We have reverse-engineered the code responsible for the attack, enabling us to learn more about the tool that was developed and deployed into the build environment.

This highly sophisticated and novel code was designed to inject the SUNBURST malicious code into the SolarWinds Orion platform without arousing the suspicion of our software development and build teams. We encourage everyone to visit this blog post, authored by the CrowdStrike team, which provides additional details into these findings and other technical aspects of this attack and contains valuable information intended to help the industry better understand attacks of this nature.

**Our investigations to date**

We are actively working with law enforcement, the intelligence community, governments and industry colleagues in our and their investigations. As we recently disclosed, we even shared all of our proprietary code libraries that we believed to have been affected by SUNBURST to give security professionals the information they needed in their research.



- Our current timeline for this incident begins in September 2019 which is the earliest suspicious activity on our internal systems identified by our forensic teams in the course of their current investigations.

- The subsequent October 2019 version of the Orion Platform release appears to have contained modifications designed to test the perpetrators' ability to insert code into our builds undetected.
- An updated version of the malicious code injection source that inserted the SUNBURST malicious code into Orion Platform releases starting on February 20, 2020.
- The perpetrators remained undetected and removed the SUNBURST malicious code from our environment in June 2020. During that time, through to today, SolarWinds investigated various vulnerabilities in its Orion platform. It remediated or initiated the process of remediating vulnerabilities, a regular process that continues today. However, until December 2020, the company did not identify any vulnerabilities as what we now know as SUNBURST.
- On December 12, 2020, we were informed of the cyberattack and moved swiftly to notify and protect our customers and to investigate the attack in collaboration law enforcement, intelligence and governments.

As part of our ongoing efforts to protect our customers and investigate the SUNBURST attack, we are reviewing historical and current customer inquiries that might contribute to a better understanding of the attack. To date, we have identified two previous customer support incidents that, with the benefit of hindsight, we believe may be related to SUNBURST. The first incident concerns a pilot development system installation that we investigated in conjunction with our customer and two third-party security companies. At that time, we did not determine the root cause of the suspicious activity or identify the presence of the SUNBURST malicious code within our Orion Software Platform. The presence of an affected version of the Orion Software Platform in the customer's environment was only identified recently after we were notified of the attack in December. The second incident occurred in November, and similarly, we did not identify the presence of the SUNBURST malicious code. We are still investigating these incidents and are sharing information related to them with law enforcement to support investigation efforts.

Turner Decl., Ex. 4 ("1/11/2021 Form 8-K") at 4–6. The AC alleges that the information revealed in the January 11 Form 8-K was known to Brown at the time the December 14 Form 8-K was filed. *Id.* ¶ 319.

## II. Procedural History of This Litigation

On October 30, 2023, after investigative discovery, the SEC filed its original Complaint. Dkt. 1. On December 14, 2023, the Court held an initial conference. Dkt. 30. On December 27, 2023, the Court approved a briefing schedule for defendants' anticipated motion to dismiss. Dkt. 38.

On January 26, 2024, SolarWinds and Brown filed a joint motion to dismiss, Dkt. 44, a memorandum of law, Dkt. 46, and declaration in support, Dkt. 49. On February 16, 2024, the SEC filed the AC, the operative complaint. Dkt. 85. On March 22, 2024, defendants filed the pending motion to dismiss the AC, Dkt. 88, and, in support, a memorandum of law, Dkt. 88 ("Def. Mem."), and a declaration, Dkts. 91–92 ("Turner Decl."). On April 19, 2024, the SEC filed its opposition, Dkt. 102 ("SEC Opp."), and a declaration in support, Dkt. 103 ("Ney Decl."). On May 3, 2024, defendants filed a reply, Dkt. 108 ("Def. Reply"), and a declaration in support, Dkt. 109 ("Second Turner Decl."). The Court has received amicus briefs from four groups in support of dismissal.<sup>27</sup> On May 15, 2024, the Court heard argument. Dkt. 120 ("Tr.").<sup>28</sup>

---

<sup>27</sup> See Dkt. 67 (brief from Software Alliance); Dkts. 68–69 (brief from Business Roundtable and Chambers of Commerce); Dkt. 70 (brief from chief information security officers and cybersecurity organizations); Dkt. 73 (brief from former government officials).

<sup>28</sup> On May 17, 2024, after argument, defendants filed a letter addressing what they termed an important factual clarification by the SEC during argument, relating to the means by which PAN had become aware of suspicious activity by its Orion software. See Dkt. 117; see also note 23, *supra*. On May 24, 2024, the SEC filed a letter in response. Dkt. 122. On May 28, 2024, defendants filed a reply. Dkt. 123. On May 31, 2024, the SEC filed a sur-reply. Dkt. 124.

### **III. Applicable Legal Standards**

#### **A. Motion to Dismiss Under Rule 12(b)(6)**

To survive a motion to dismiss under Rule 12(b)(6), a complaint must plead “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is facially plausible “when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A complaint is properly dismissed where, as a matter of law, “the allegations in a complaint, however true, could not raise a claim of entitlement to relief.” *Twombly*, 550 U.S. at 558. When resolving a motion to dismiss, the Court must assume all well-pled facts to be true, “drawing all reasonable inferences in favor of the plaintiff.” *Koch*, 699 F.3d at 145. That tenet, however, does not apply to legal conclusions. *See Iqbal*, 556 U.S. at 678. Pleadings that offer only “labels and conclusions” or “a formulaic recitation of the elements of a cause of action will not do.” *Twombly*, 550 U.S. at 555.

#### **B. Standards Applicable to Fraud Claims**

Federal Rule of Civil Procedure 9(b) imposes “a heightened pleading standard on complaints alleging securities fraud.” *SEC v. Wey*, 246 F. Supp. 3d 894, 909 (S.D.N.Y. 2017) (citing *Novak v. Kasaks*, 216 F.3d 300, 306 (2d Cir. 2000)). Under Rule 9(b), parties alleging fraud must “state with particularity the circumstances constituting fraud.” To satisfy Rule 9(b), a plaintiff alleging fraudulent statements must: (1) specify the fraudulent statements; (2) identify the speaker; (3) state where and when the statements were made; and (4) explain why the statements were fraudulent. *Novak*, 216 F.3d at 306. However, “[m]alice, intent, knowledge,

and other conditions of a person’s mind may be alleged generally.” Fed. R. Civ. P. 9(b).<sup>29</sup> “This pleading constraint serves to provide a defendant with fair notice of a plaintiff’s claim, safeguard his reputation from improvident charges of wrongdoing, and protect him against strike suits.”

*ATSI Commc’ns, Inc. v. Shaar Fund, Ltd.*, 493 F.3d 87, 99 (2d Cir. 2007) (citation omitted).

#### **IV. Securities Fraud and False Filing Claims<sup>30</sup>**

The SEC brings securities fraud and false filing claims against SolarWinds and Brown based on pre- and post-SUNBURST disclosures. The fraud claims are brought under (1) Section 10(b) of the Exchange Act and Rule 10b-5; and (2) Section 17(a) of the Securities Act. They are based on alleged material omissions and misstatements in the Security Statement, podcasts, press releases, and blog posts, the cybersecurity risk disclosure in the Form S-1, and the SUNBURST disclosures in the Form 8-Ks. The false filing claims are brought under Section 13(a) of the Exchange Act and Rules 12b-20, 13a-1, 13a-11, and 13a-13. They are based on statements in filings SolarWinds made to the SEC—the cybersecurity risk disclosure in the Form S-1 filed in

---

<sup>29</sup> Unlike a private plaintiff, however, the SEC need not satisfy the heightened pleading requirements imposed by the Private Securities Litigation Reform Act (“PSLRA”). *SEC v. China Ne. Petroleum Holdings Ltd.*, 27 F. Supp. 3d 379, 387 (S.D.N.Y. 2014); *see also SEC v. Dunn*, 587 F. Supp. 2d 486, 501 (S.D.N.Y. 2008) (“Any argument that Congress intended to apply the provisions of the PSLRA to SEC enforcement actions ignores the statute’s plain language.”).

<sup>30</sup> The claims analyzed under this section include the AC’s first four claims of securities fraud: (1) its first claim of violations of Section 17(a) of the Securities Act against SolarWinds and Brown, AC ¶¶ 332–34; (2) its second claim of aiding and abetting liability under Section 17(a) against Brown, *id.* ¶¶ 335–38; (3) its third claim of violations of Section 10(b) under the Exchange Act and Rule 10b-5 against SolarWinds and Brown, *id.* ¶¶ 339–41; and (4) its fourth claim of aiding and abetting liability under these provisions against Brown, *id.* ¶¶ 342–45. They also include the AC’s false filing claims: (5) its fifth claim of violations of Section 13(a) of the Exchange Act and Rules 12b-20, 13a-1, 13a-11, and 13a-13 against SolarWinds, *id.* ¶¶ 346–48; and (6) its sixth claim of aiding and abetting liability under these provisions against Brown.

October 2018, and incorporated by reference in later filings, and the disclosures relating to SUNBURST in the Form 8-Ks filed in December 2020.

**A. Applicable Statutory Provisions and Legal Standards**

**1. Securities Fraud**

*Misrepresentation Liability.* Section 10(b) of the Exchange Act makes it unlawful for any person “[t]o use or employ, in connection with the purchase or sale of any security . . . any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the [SEC] may prescribe.” 15 U.S.C. § 78j(b). Section 10(b) “is designed to protect investors by serving as a ‘catchall provision’ which creates a cause of action for manipulative practices by defendants acting in bad faith.” *In re Openwave Sys. Sec. Litig.*, 528 F. Supp. 2d 236, 249 (S.D.N.Y. 2007) (citation omitted). Rule 10b-5 implements Section 10(b) by making it unlawful for

any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange,

- (a) To employ any device, scheme, or artifice to defraud,
- (b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or
- (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security.

17 C.F.R. § 240.10b-5.

Similarly, Section 17(a) of the Securities Act makes it unlawful, in the offer or sale of securities, by the use of any means of interstate commerce or by use of the mails,

- (1) to employ any device, scheme, or artifice to defraud, or
- (2) to obtain money or property by means of any untrue statement of a material fact or any omission to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or

(3) to engage in any transaction, practice, or course of business which operates or would operate as a fraud or deceit upon the purchaser.

17 U.S.C. § 77q(a).

“[T]o establish primary liability under § 10(b) and Rule 10b-5, a plaintiff is required to prove that in connection with the purchase or sale of a security the defendant, acting with scienter, made a material misrepresentation (or a material omission if the defendant had a duty to speak) or used a fraudulent device.” *SEC v. First Jersey Sec., Inc.*, 101 F.3d 1450, 1467 (2d Cir. 1996) (citations omitted). “The elements of a claim under § 17(a) of the Securities Act, and under § 10(b) of the Exchange Act and SEC Rule 10b-5 are essentially the same, and many courts—including the Second Circuit—analyze claims under both statutes together.” *SEC v. Constantin*, 939 F. Supp. 2d 288, 302 (S.D.N.Y. 2013) (cleaned up). “The only meaningful analytical distinction in this context is that the SEC need not plead scienter for a claim under subsections (2) and (3) of § 17(a).” *China Ne. Petroleum Holdings*, 27 F. Supp. 3d at 388 (citations omitted).

*Scheme Liability.* To state a claim for scheme liability under Rule 10b-5 and Securities Act Section 17(a)(1), a complaint must allege “that the defendant (1) committed a manipulative or deceptive act (2) in furtherance of the alleged scheme to defraud, (3) [with] scienter.” *Wey*, 246 F. Supp. 3d at 905–16. As with misrepresentation claims, scienter can be shown by facts that give rise to a “strong inference of fraudulent intent.” *Id.* at 916. A scheme liability claim under Securities Act Section 17(a)(3) does not require showing scienter but is instead “satisfied by allegations that the defendant acted negligently.” *Id.* at 917. For a scheme liability claim to be viable, the “manipulative or deceptive act” must be “something *beyond* misstatements and omissions, such as dissemination.” *SEC v. Rio Tinto plc*, 41 F.4th 47, 49 (2d Cir. 2022).

## 2. False Filing

False filing claims are based in Section 13(a) of the Exchange Act and its implementing rules. Section 13(a) provides:

- (a) Every issuer of a security registered pursuant to section 78l of this title shall file with the Commission, in accordance with such rules and regulations as the Commission may prescribe as necessary or appropriate for the proper protection of investors and to insure fair dealing in the security—
  - (1) such information and documents (and such copies thereof) as the Commission shall require to keep reasonably current the information and documents required to be included in or filed with an application or registration statement filed pursuant to section 78l of this title, except that the Commission may not require the filing of any material contract wholly executed before July 1, 1962.
  - (2) such annual reports (and such copies thereof), certified if required by the rules and regulations of the Commission by independent public accountants, and such quarterly reports (and such copies thereof), as the Commission may prescribe.

15 U.S.C. § 78m(a). Section 13(a) and Rules 13a-1, 13a-11, and 13a-13 require issuers of registered securities to file with the SEC annual reports on Form 10-K, current reports on Form 8-K, and quarterly reports on Form 10-Q. *SEC v. Espuelas*, 698 F. Supp. 2d 415, 434 n.22 (S.D.N.Y. 2010). Rule 12b-20 requires issuers to disclose any material information necessary to ensure that the reports are not misleading. It provides:

In addition to the information expressly required to be included in a statement or report, there shall be added such further material information, if any, as may be necessary to make the required statements, in the light of the circumstances under which they are made not misleading.

17 C.F.R. § 240.12b-20. The Exchange Act’s reporting requirements are only satisfied by the “filing of complete, accurate, and timely reports.” *SEC v. Savoy Indus., Inc.*, 587 F.2d 1149, 1165 (D.C. Cir. 1978).

## B. Pre-SUNBURST Disclosures

### 1. Security Statement

The SEC pursues securities fraud claims against the defendants—under theories of both misrepresentation and scheme liability—on the ground that the Security Statement made material misrepresentations as to the state of the company’s cybersecurity. It contends that the defendants shaped, disseminated, and promoted the Statement; that the Statement was materially misleading; and that Brown, and, through him, SolarWinds, acted with scienter. The Court sustains both theories of fraud liability with respect to the Statement.

#### a. Securities Fraud: Misrepresentation Liability

The AC pleads securities fraud based on misrepresentations in the Security Statement with the required particularity.

#### i. False or Misleading Statements or Omissions

First published in 2017 and on SolarWinds’ website throughout the Relevant Period, the Security Statement made broad representations about SolarWinds’ cybersecurity practices. The SEC argues that the Statement contained five sets of misrepresentations regarding SolarWinds’ (1) access controls; (2) password protections; (3) compliance with the NIST Cybersecurity Framework; (4) network monitoring; and (5) compliance with the secure development lifecycle. AC ¶¶ 70–73. It argues that the Statement was “misleading as to a material fact,” *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 38 (2011) (emphasis omitted), meaning “a reasonable investor would have considered [it] significant in making investment decisions,” *Ganino v. Citizens Utils. Co.*, 228 F.3d 154, 161 (2d Cir. 2000). See *Basic Inc. v. Levinson*, 485 U.S. 224, 231–32 (1988) (to establish materiality, “there must be a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the ‘total mix’ of information made available.”).

At the threshold, the Court addresses—and dispatches—two arguments defendants make with respect to the Security Statement as a whole.

First, defendants suggest that the Security Statement cannot be actionable because it was directed to *customers*, not investors. That is wrong. It is well established that false statements on public websites can sustain securities fraud liability. *See, e.g., SEC v. Enters. Sols., Inc.*, 142 F. Supp. 2d 561, 577–78 (S.D.N.Y. 2001) (finding liability for securities fraud violation based in part on misleading statements on company’s website); *SEC v. Riel*, 282 F. Supp. 3d 499, 519–21 (N.D.N.Y. 2017) (same); *SEC v. Terry’s Tips, Inc.*, 409 F. Supp. 2d 526, 534 (D. Vt. 2006) (SEC adequately pled that defendant “intentionally or recklessly allowed false and misleading performance figures to be published and to remain on [defendant’s] website.”). Notwithstanding that the Security Statement was aimed at persuading customers to buy SolarWinds’ ostensibly cybersecure products—making its misleading claims potentially part of a fraud on customers, too—the Statement was on SolarWinds’ public website and accessible to all, including investors. It was, unavoidably, part of the “total mix of information” that SolarWinds furnished the investing public. *Basic*, 485 U.S. at 232 (cleaned up).

Second, defendants urge that the representations in the Statement be evaluated in isolation. *See* Tr. 38. They contend that if any representation, individually, is not found materially misleading, it should be put aside in the Court’s motion to dismiss analysis and off limits in post-motion discovery. That is also methodologically wrong. Of course, of necessity, each of the five challenged sets of representations must be considered distinctly for purposes of evaluating whether it is plausibly pled as misleading. But as to materiality, the well-pled misrepresentations in the Statement must be viewed together as collectively bearing on the Statement’s central thesis: that the cybersecurity practices of SolarWinds, a software vendor

whose public and private customers expected its products to be reliably airtight against cybersecurity intrusions, were strong. A holistic assessment follows from the precept that the investing public evaluates the information available to it, including that provided by the issuer, “as a whole,” not in pointillistic fashion. *Olkey v. Hyperion 1999 Term Tr., Inc.*, 98 F.3d 2, 5 (2d Cir. 1996); *see, e.g., id.* (“It is undisputed that prospectuses must be read ‘as a whole.’”); *McMahan & Co. v. Warehouse Ent., Inc.*, 900 F.2d 576, 579 (2d Cir. 1990) (rejecting district court’s “atomistic consideration of the presentation” and analyzing it “as a whole”); *See SEC v. Farmer*, No. 14 Civ. 2345 (KPE), 2015 WL 5838867, at \*7 n.8 (S.D. Tex. Oct. 7, 2015) (“[E]ven a single misstatement or omission is sufficient for liability.” (cleaned up)).

For the reasons that follow, the Court finds that the AC pleads that the Security Statement contained misrepresentations as to at least two of the five cybersecurity practices. These concern SolarWinds’ (1) access controls and (2) password protection policies. As to each, the company’s representations, as pled, were materially misleading by a wide margin. And the Security Statement’s overall portrait of SolarWinds’ cybersecurity was all the more materially misleading considering the two sets of misrepresentations together.<sup>31</sup>

#### A. Representations regarding access controls

The AC pleads, citing ample evidentiary support, that the Security Statement misleadingly touted SolarWinds’ access controls as strong.

On this subject, the Security Statement represented:

##### **Access Controls**

##### **Role Based Access**

---

<sup>31</sup> In light of this determination—and the determination, *post*, that these misrepresentations were made with scienter—it is unnecessary to resolve on the pleadings whether the representations in the Security Statement as to the other three cybersecurity practices were also misleading.

Role based access controls are implemented for access to information systems. Processes and procedures are in place to address employees who are voluntarily or involuntarily terminated. Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know/least privilege<sup>32</sup> necessary basis. Access control lists define the behavior of any user within our information systems, and security policies limit them to authorized behaviors.

### **Authentication and Authorization**

. . . . Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as defined by our security guidelines. Approvals are managed by workflow tools that maintain audit records of changes.

Sec. Statement at 4.

In fact, the AC alleges, between 2017 and 2020, SolarWinds was routinely promiscuous in freely granting administrative rights to employees and conferring access rights way beyond those necessary for employees' specific job functions. AC ¶¶ 181–82. It alleges “that most employees had ‘admin’ rights at times during the Relevant Period.” *Id.* ¶ 182. It alleges that SolarWinds’ “significant deficiencies” in access controls—which resulted in widespread grant of “admin rights” among employees—were well-documented and widely acknowledged within the company. *Id.* ¶¶ 199–200. The largely indiscriminate provision of administrative access to employees blatantly contradicts the Security Statement’s representations to the public that: (1) “[e]mployees are granted access to certain additional resources based on their specific job function”; and (2) the company provided access to sensitive data on a “need-to-know/least privilege necessary basis.” Sec. Statement at 4.

---

<sup>32</sup> “[L]east privilege” is an “industry-standard concept that persons should be granted the minimum system resources and authorizations needed to perform their job functions.” *Id.* ¶ 181.

Reinforcing this point, the AC pleads that SolarWinds’ deficiencies in access controls were not only glaring—they were long-standing, well-recognized within the company, and unrectified over time. AC ¶¶ 181–83. These had been identified in mid-2017, before SolarWinds became public and before the Security Statement was posted on the company website. Internal presentations frequently warned that “too many accounts [had] admin level access.” *Id.* ¶ 184 (June 2017 presentation prepared by Director of IT and shared with CIO). Brown himself recognized these problems as important to correct upon joining the company. *See id.* ¶ 185 (citing Brown’s August 2017 Security State of the Union warning of the need to “[l]ock down administrative access.”). Despite internally acknowledging these deficiencies, Brown approved the Security Statement, which portrayed a diametrically opposite representation for public consumption. And, after the Statement was posted, Brown and others continued to internally acknowledge porous access control. In January 2018, Brown, along with the CIO and Director of IT, received a presentation which warned: “Currently there is a collection of people who have access to many systems and many people involved in provisioning access.” *Id.* ¶ 186. And in a March 2018 presentation, Brown admitted that the “[c]oncept of least privilege [is] not followed as a best practice” and that “shared accounts” were used “throughout internal and external applications,” *id.* ¶ 187. As pled, these internal accounts contradicted the Security Statement’s representation that “[a]ccess controls to sensitive data in our databases, systems, and environments are set on a need-to-know/least privilege necessary basis” and that “[r]ole based access controls are implemented for access to information systems.” *Sec. Statement* at 4. These problems continued to be documented leading up to the IPO. In September 2018, a month before the IPO, Brown sent the CTO a presentation on “Information Security” which described

“Identity Management–Role and Privilege Management” as “[l]imited or non-existent.” AC ¶ 189.

Critically, the AC pleads that, after SolarWinds went public, it did not resolve its access controls problems, or withdraw, repudiate, or modify the Security Statement’s bogus claims on this point. Internal presentations continued to document these deficiencies, impeaching the Security Statement’s claims of robust access controls. A December 2018 presentation listed, as an information security gap, that SolarWinds had yet to “[d]efine standards and best practices for Role Based Access Controls and Least Privilege,” “[a]ddress the use of local administrator access to non-privileged users,” and “[m]anage, audit, and apply security controls around privileged access.” *Id.* ¶ 191. Presentations in March and October 2020, which Brown helped draft, identified “[s]ignificant deficiencies in user access management” as a key risk to the company. *Id.* ¶ 198.

Post-IPO internal evaluations reinforce the SEC’s claim that the Security Statement prevaricated as to access control practices. In 2019, for example, the company assessed 43 types of “[a]ccess controls” required by the NIST 800-53 cybersecurity framework. It found that, of the 43 controls, only two were “in place”; 18 “may be in place,” and 23 had “[n]o program/practice in place.” *Id.* ¶ 193. This assessment found that SolarWinds lacked an “explicit restriction policy” by which it “restrict[ed] privileged accounts on the information system to . . . organization-defined personnel or roles.” *Id.* ¶ 194. It found that SolarWinds had neither “tested” nor “audited” whether its “information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.” *Id.* And it found that SolarWinds had “no explicit authorization policy” that restricted “access to . . . organization-defined security functions

(deployed in hardware, software, and firmware) and security-relevant information.” *Id.* (also finding “a gap” in how SolarWinds “enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on . . . organization-defined information flow control policies”). That same year, applying the more general NIST Cybersecurity Framework, SolarWinds assigned itself a score of “1” in meeting the control objective: “User identity, authentication and authorization are in place and actively monitored across the company.” *Id.* ¶ 192. A score of “1” meant that SolarWinds had “an ad-hoc, inconsistent, or reactive approach to meeting that cybersecurity control objective.” *Id.* ¶ 192.

In light of these detailed pleadings, which chronicle diverse findings contradicting SolarWinds’ public representations, the AC plausibly alleges that Solar Winds and Brown made sustained public misrepresentations, indeed many amounting to flat falsehoods, in the Security Statement about the adequacy of its access controls. Given the centrality of cybersecurity to SolarWinds’ business model as a company pitching sophisticated software products to customers for whom computer security was paramount, these misrepresentations were undeniably material.

#### B. Representations regarding password policy

The AC also adequately alleges that the Security Statement materially misrepresented to the public that SolarWinds enforced a strong password policy. The Statement stated:

We require that authorized users be provisioned with unique account IDs. Our password policy<sup>33</sup> covers all applicable information systems, applications, and databases. Our password best practices enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords. Passwords are individually salted and hashed.

---

<sup>33</sup> During the Relevant Period, SolarWinds’ password policy required passwords to (1) be changed every 90 days, (2) have a minimum length of eight characters, and (3) include three of the four following characteristics: uppercase letter, lowercase letter, digit (0–9), and non-alphanumeric character. *Id.* ¶ 160.

Sec. Statement at 4.

In fact, the AC alleges, the company's stated password policy was generally not enforced. Company employees, it alleges, routinely used simple, unencrypted passwords with respect to products and internal systems, compounding SolarWinds' vulnerability to intrusion by threat actors. The AC alleges that Brown and others failed to correct these known problems, allowing them to fester for years. AC ¶ 163.

To this end, the AC sets out evidence, from pre- and post-IPO, that top executives were alerted to ongoing password practices that breached SolarWinds' ostensible password policy. In April 2017, an employee emailed the CIO, reporting that "'default passwords' are [still] plaguing us when the product has been in the market [for this long]." *Id.* ¶ 164. For example, a company product still used "password" as the default password. *Id.* In September 2019, a compliance employee emailed the CIO, reporting security risks affecting SolarWinds' Cloud product lines' main source of authentication. *Id.* ¶ 169. The employee reported that passwords "have no specific parameters, as stated in the IT guidelines," and "are able to be reused and are not changed at a set number of days." *Id.* In November 2019, an outside security researcher notified the company that the password to its "Akamai" server, used to distribute software updates to customers, was publicly available. *Id.* ¶ 172. The leaked password was "solarwinds123," a blatantly inadequate password for a company specializing in selling cybersecure software.

The AC further alleges that SolarWinds' failure to maintain the sound password practices that it touted was documented repeatedly in audits and internal assessments. An April 2018 audit revealed database passwords "not encrypted within the configuration file," login credentials "stored in plain text in configuration files," and passwords "stored in plain text on the public web server in the web configuration file and in the system registry of the machine." *Id.* ¶ 166. These

practices were incompatible with the Security Statement's claim that SolarWinds' passwords were "individually salted and hashed" (*i.e.*, encrypted). SolarWinds' 2019 and 2020 SOX audits also revealed failures to meet "[p]assword requirements." *Id.* ¶ 167; *see id.* ¶ 168 (March 2020 Quarterly Risk Review presentation, drafted with Brown's input and shared with CIO and CTO, describing SOX audit findings.). And as with access controls, the company's 2019 NIST 800-53 assessment witheringly graded its password security. It rated 27 controls related to "Identification and Authentication." *Id.* ¶ 170. Out of the 27, 20 were rated as having "no program/practice in place"; seven were rated as "program/practice may be in place but required detailed review"; and none were rated as having a "program/practice in place." *Id.*

In light of these detailed pleadings, the Security Statement's statements about the muscularity of the company's password practices are well pled as misleading if not outright false. These misrepresentations, too, are well pled as material, especially given the nature of the company's products and customer base.

In sum, even without considering the three other cybersecurity subjects as to which the SEC challenges the Security Statement's claims, the Statement is aptly pled as materially misleading and false. In essence, the Statement held out SolarWinds as having sophisticated cybersecurity controls in place and as heeding industry best practices. In reality, based on the pleadings, the company fell way short of even basic requirements of corporate cyber health. Its passwords—including for key products—were demonstrably weak and the company gave far too many employees unfettered administrative access and privileges, leaving the door wide open to hackers and threat actors. *See In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189, 1219–20 (N.D. Ga. 2019) ("Given the dangerously deficient state of [defendant's] cybersecurity, the Court concludes it was false, or at least misleading, for [defendant] to tout its advanced cybersecurity

protections. . . . Plaintiff has pleaded a variety of facts showing that [defendant's] cybersecurity systems were outdated, below industry standards, and vulnerable to cyberattack, and that [it] did not prioritize data security efforts.”).

A reasonable person contemplating investing in SolarWinds would have viewed the alleged gap between SolarWinds' words and on-the-ground reality as highly consequential—as “significant in making investment decisions.” *Ganino*, 228 F.3d at 161. Indeed, the business risks presented by such penetrable cybersecurity might well have been material for a company that sold old-fashioned products (*e.g.*, furniture or cars). But the specific risks were magnified for SolarWinds, whose products (software) had cybersecurity as a key attribute and whose key clients (government agencies and Fortune 500 companies) expected the software they purchased to be and remain uncompromised. SolarWinds' cybersecurity practices thus “play[ed] a significant role in [its] operations [and] profitability.” *Freudenberg v. E\*Trade Fin. Corp.*, 712 F. Supp. 2d 171, 181 (S.D.N.Y. 2010); *see, e.g., id.* at 184 (misleading statement “with regards to the important segment of [defendants'] business” material, as “reasonable investors would have taken [statements] into account when making investment decision[s]”); *Babaev v. Grossman*, No. 03 Civ. 5076 (DLI), 2007 WL 633990, at \*4 (E.D.N.Y. Feb. 26, 2007) (omission material because it concerned contracts that constituted a “large portion” of defendant's business and “any potential termination of these exclusive agreements would affect the probable future of the company”); *In re Henry Schein, Inc. Sec. Litig.*, No. 18 Civ. 01428 (MKB), 2019 WL 8638851, at \*11 (E.D.N.Y. Sept. 27, 2019) (“Because [defendant's] dental distribution business accounts for approximately half of its total net sales, the omitted information was therefore likely to affect the future of [its] profitability.”). On a motion to dismiss, “a complaint may not properly be dismissed . . . on the ground that the alleged misstatements or omissions are not material unless

they are so obviously unimportant to a reasonable investor that reasonable minds could not differ on the question of their importance.” *Ganino*, 228 F. 3d at 162 (quoting *Goldman v. Belden*, 754 F.2d 1059, 1067 (2d Cir. 1985)). The AC clears this hurdle by a wide margin.

The above assessment aligns with the decision denying a motion to dismiss a private securities fraud lawsuit brought in the Western District of Texas against Solar Winds, Brown, and others. The claims there, to the extent based on the Security Statement, largely parallel those here. See *In re SolarWinds Corp. Sec. Litig.*, 595 F. Supp. 3d 573 (W.D. Tex. March 30, 2022), *opinion clarified*, No. 21 Civ. 138 (RP), 2022 WL 3699429 (W.D. Tex. Aug. 19, 2022) (“*In re SolarWinds*”).<sup>34</sup> The lead plaintiff there, the New York City District Council of Carpenters Pension Fund, brought suit in February 2021 on behalf of a putative class of investors who had purchased SolarWinds securities between October 18, 2018, and December 17, 2020, and lost money as a result of the stock-price drop upon revelation of the SUNBURST cybersecurity breach. *Id.* at 579. Relevant here, the district court (Pitman, J.) denied a motion by SolarWinds and Brown to dismiss the claims brought against them under Section 10(b) of the Exchange Act and Rule 10b-5, which alleged that they had falsely and misleadingly touted as robust the company’s cybersecurity system and its adherence to specific cybersecurity practices as set forth in the Security Statement. The complaint, the court held, viably pled that the Security Statement made materially misleading statements on these subjects. Although the decision there does not bind this Court, its thoughtful analysis of substantially similar claims, subject to the heightened pleading standards of both Rule 9(b) and the PSLRA, is persuasive authority.<sup>35</sup>

---

<sup>34</sup> That lawsuit also named as defendants chief executive officer Kevin B. Thompson, chief financial officer and treasurer J. Barton Kalsu, and two private equity firms that each owned approximately 40% of SolarWinds’ securities during the class period.

<sup>35</sup> On November 3, 2022, seven months after the district court denied the motion to dismiss, the parties filed a notice of a class-wide settlement, No. 21 Civ. 138, Dkt. 95, which settled all

## ii. Scierter

The SEC alleges that SolarWinds and Brown acted with scierter in keeping the Security Statement on the company website in the face of known cybersecurity deficiencies that made the Statement false and misleading. In moving to dismiss, defendants argue that the AC does not adequately allege that they sought to deceive investors through the Statement. The AC amply alleges scierter.

As used in connection with the securities fraud statutes, scierter means “intent to deceive, manipulate, or defraud; or at least knowing conduct.” *SEC v. First Jersey Sec., Inc.*, 101 F.3d 1450, 1467 (2d Cir. 1996) (internal citations omitted). “The requisite scierter can be established by alleging facts to show either (1) that defendants had the motive and opportunity to commit fraud, or (2) strong circumstantial evidence of conscious misbehavior or recklessness.” *ECA, Loc. 134 IBEW Joint Pension Tr. of Chi. v. JP Morgan Chase Co.*, 553 F.3d 187, 198 (2d Cir. 2009). Where, as here, a plaintiff does not allege motive and opportunity, it “must produce a stronger inference of recklessness” under “the conscious misbehavior or recklessness” theory. *Kalnit v. Eichler*, 264 F.3d 131, 143 (2d Cir. 2001).

“[C]onscious recklessness” is a “state of mind *approximating actual intent*, and *not merely a heightened form of negligence*.” *S. Cherry St., LLC v. Hennessie Group LLC*, 573 F.3d 98, 109 (2d Cir. 2009). To meet this standard, the AC must allege “reckless conduct” by defendants. Such can entail conduct that is “highly unreasonable and which represents an extreme departure from the standards of ordinary care to the extent that the danger was either known to the defendant or so obvious that the defendant must have been aware of it”; or a

---

claims there for \$26 million, *id.*, Dkt. 97 at 7. On June 28, 2023, the district court approved the settlement. *Id.*, Dkt. 112.

“fail[ure] to review or check *information that they had a duty to monitor*, or ignored *obvious signs of fraud*,” such that defendants “should have known that they were misrepresenting material facts.” *Id.* The SEC can also plead recklessness based on facts showing that “defendants knew facts or had access to non-public information contradicting their public statements” and therefore “knew or should have known they were misrepresenting material facts.” *In re Scholastic Corp. Sec. Litig.*, 252 F.3d 63, 76 (2d Cir. 2001) (citing *Novak*, 216 F.3d at 308). In other words, the SEC must adequately allege that “defendants understood that their public statements were inaccurate, or were ‘highly unreasonable’ in failing to appreciate this possibility.” *In re Sanofi Sec. Litig.*, 87 F. Supp. 3d 510, 534 (S.D.N.Y. 2015), *aff’d sub nom*, *Tongue v. Sanofi*, 816 F.3d 199 (2d Cir. 2016).

The Court’s analysis begins with Brown, whom the AC claims actually knew (and at a minimum should have known) that the Security Statement was false or misleading. AC ¶¶ 10, 56, 58, 64. The AC easily pleads Brown’s scienter. It pleads that he approved the Security Statement and, as set out above, was privy to internal information contradicting the Statement’s representations both as to the company’s access controls and compliance with the password policy. And logically so—as vice president of security and architecture, Brown was responsible for SolarWinds’ cybersecurity protocols and the cybersecurity architecture of its products. Along these lines, the AC pleads that, immediately after joining in 2017, Brown learned of the company’s cybersecurity deficiencies. Thereafter, he gave presentations about the need for improvement, was privy (before and after the IPO) to the internal assessments and presentations that spotlighted SolarWinds’ ongoing shortcomings, and presented on these points himself. *See, e.g., id.* ¶ 189 (September 2018 presentation by Brown to CTO flagging that “Identity Management–Role and Privilege management” was “[l]imited or nonexistent.”); *id.* ¶ 192

(August 2019 preparation by Brown of Security and Compliance Program Quarter Review, that stated that: “Access and privilege to critical systems/data is inappropriate.”); *id.* ¶ 168 (March 2020 Quarterly Risk Review presentation, drafted with Brown’s input, which described SOX audit’s finding that “[p]assword requirements [were] not met.”).

The above is alone enough to plead Brown’s knowledge of, and alternatively his recklessness as to, the misstatements on SolarWinds’ website. The AC, however, goes beyond that. It pleads that Brown knew of actual cybersecurity incidents, tending to undermine the Security Statement’s top-line message that SolarWinds had strong cybersecurity practices. In August 2018 and again in January 2020, Brown received a presentation describing a major security vulnerability with SolarWinds’ VPN network, which allowed a user with credentials to log on to the company’s network from an unmanaged device. The presentation warned—presciently, as it turned out—that an attacker could access SolarWinds’ VPN and upload code without detection, which could serve as a backdoor for future attacks. *Id.* ¶ 206. Despite Engineer D’s repeated warnings about this issue and recommendations on how to address it, the company did not do so. As to the other security lapses chronicled in the AC, the AC does not recite direct evidence of Brown’s being alerted to them. But given his position as vice president of security and architecture, his duty to monitor SolarWinds’ cybersecurity, and his role as the company’s cybersecurity spokesperson, the only rational inference is that he knew of them. In November 2019, a third-party security researcher alerted SolarWinds that the password to one of its servers was publicly available, and a ripe target for exploitation by a threat actor. *Id.* ¶ 172. That the leaked password was “solarwinds123” also contradicted the company’s public claim to use “password best practices,” including mandating “the use of complex passwords that include both alpha and numeric characters.” Sec. Statement at 4.

The AC thus amply pleads, with particularity, that Brown knew of the substantial body of data that impeached the Security Statement's content as false and misleading.<sup>36</sup> His conduct in allowing the Statement to issue publicly, and to remain in place for years, in the face of company practices inconsistent with it, is plausibly pled as "highly unreasonable or extreme misconduct." *In re Livent, Inc. Noteholders Sec. Litig.*, 151 F. Supp. 2d 371, 422 (S.D.N.Y. 2001).

Brown's scienter is also properly imputed to SolarWinds. For scienter to be imputed to a corporate entity, a plaintiff must show "that an agent of the corporation committed a culpable act with the requisite scienter." *Teamsters Loc. 445 Freight v. Dynex Cap. Inc.*, 531 F.3d 190, 195 (2d Cir. 2008); *see also SEC v. Treadway*, 430 F. Supp. 2d 293, 337 (S.D.N.Y. 2006) ("It is settled that the scienter of executives can be imputed to corporate entities.") As the Second Circuit has recognized, consistent with the doctrine of *respondeat superior*, the scienter of a corporate defendant is generally inferred based on the scienter of a defendant executive. *Dynex*, 531 F.3d at 195. Here, given Brown's having (on the facts pled) acted with the required scienter in publishing the Security Statement and maintaining it on SolarWinds' public-facing website, and given Brown's lead role on cybersecurity matters at the company, his state of mind (like his actions) is properly imputed to SolarWinds. *See, e.g., SEC v. N. Am. Rsch. & Dev. Corp.*, 424 F.2d 63, 79 (2d Cir. 1970); *SEC v. Ballesteros Franco*, 253 F. Supp. 2d 720, 728–29 (S.D.N.Y. 2003) (attributing executive's knowledge to corporation in connection with that executive's actions, noting "that a corporation can act only through the actions of natural persons and that the actions of its agents, acting within the scope of their agency, are attributed to the corporation").

---

<sup>36</sup> In denying the motion to dismiss, the district court in *In re SolarWinds* similarly held that, on the facts pled, Brown had acted with at least severe recklessness in touting SolarWinds' security measures while knowing "that the cybersecurity measures at the company were not as they were portrayed." 595 F. Supp. 3d at 588. The court noted that, alerted to the "solarwinds123" password leak, Brown should have realized "something was dangerously amiss." *Id.* at 584.

The AC thus adequately pleads, against both defendants, all elements of its securities fraud claim based on misrepresentations. The Court denies the motion to dismiss as to that claim.

*b. Securities Fraud: Scheme Liability*

The AC separately alleges scheme liability under Rule 10b-5(a) and (c) and Securities Act Section 17(a)(1) and (3). It alleges that Brown is subject to scheme liability because he helped disseminate the Security Statement.

Misstatements and omissions alone are generally not “sufficient to constitute a scheme.” *Rio Tinto*, 41 F.4th at 54. “[A]n actionable scheme liability claim also requires something *beyond* misstatement and omissions, such as dissemination.” *Id.* at 49. The AC pleads that. It alleges that Brown disseminated the Security Statement to customers. *See* AC ¶ 57 (“Brown and SolarWinds misleadingly posted the Security Statement on the Company’s website and *affirmatively sent it to customers* claiming it described the practices SolarWinds followed at the time.” (emphasis added)); *id.* ¶ 58 (“Brown (or others acting at his direction) disseminated the Security Statement, or a link to the Security Statement, to customers seeking more information about SolarWinds’ security practices, and he provided a link to the Trust Center in Company-approved blog posts that he authored and that were posted on a SolarWinds’ website.”); *id.* ¶ 61 (“The Security Statement was then used as part of SolarWinds’ official response to customer questionnaires regarding its cybersecurity practices. In other words, it was the missing document that Brown said in August and September 2017 that SolarWinds needed to obtain and retain customers.”). And it alleges that Brown promoted the Statement in blogposts, podcasts, and press releases touting SolarWinds’ strong cybersecurity measures. *See, e.g.*, AC ¶ 222 (Brown

made a 2020 blog post that “included a hyperlink . . . to the Trust Center of SolarWinds’ website containing the Security Statement”).

These allegations, to the effect that Brown promoted and actively disseminated the misleading and false Security Statement, adequately plead scheme liability. *See, e.g., United States v. Kwok*, No 23. Cr. 118 (AT), 2024 WL 1407057, at \*8 (S.D.N.Y. Apr. 2, 2024) (scheme liability well-pled where indictment “adequately alleges that [defendant] participated in the dissemination of the misstatements by posting videos to his large following on social media.”); *Sec. & Exch. Comm’n v. City of Rochester*, No. 22 Civ. 06273, 2024 WL 909475, at \*10 (W.D.N.Y. Mar. 4, 2024) (scheme liability well-pled because SEC “adequately pleaded dissemination by alleging . . . the City Defendants disseminated the false statements in the offering documents sent to investors”); *Rio Tinto*, 41 F. 4th at 53 (recognizing that “transmission of emails, or dissemination, c[an] sustain a claim under the scheme subsections” (internal quotation marks omitted)).

And for the reasons reviewed above in connection with the misrepresentation claim, the AC plausibly alleges scienter with respect to Brown’s dissemination and promotion of the Security Statement. The required scienter is “intent to defraud or recklessness for each of the scheme liability provisions except Section 17(a)(3), for which a showing of negligence is sufficient.” *SEC v. Terraform Labs Pte. Ltd.*, No. 23 Civ. 1346 (JSR), 2023 WL 8944860, at \*18 (S.D.N.Y. Dec. 28, 2023) (citations and internal quotation marks omitted). As alleged, Brown approved, disseminated, and promoted the Security Statement despite knowing of the ample evidence contradicting the Statement’s rosy account of SolarWinds’ cybersecurity practices. Thus, his dissemination and promotion of the Security Statement as an accurate depiction of

SolarWinds' cybersecurity practice was reckless and an extreme departure from standards of ordinary care.

The AC thus plausibly pleads scheme liability against Brown based on his dissemination and promotion of the Security Statement. Because Brown's conduct and scienter with respect to the Statement is attributable to SolarWinds, as reviewed above, the AC also ably pleads scheme liability against SolarWinds.

## 2. Press Releases, Blog Posts, and Podcasts

The AC separately brings securities fraud claims against SolarWinds and Brown based on other public statements by Brown, including in company-approved press releases, blog posts, and podcasts. AC ¶¶ 219–25. The SEC argues that these misleadingly touted SolarWinds' cybersecurity practices. The challenged statements include:

- In a July 2018 blogpost, Brown wrote: “People often think of security as an insurance policy—something you have to have, like locks on your doors, fire and flood insurance, and business insurance. While these are all true, there are opportunities to think of security as a business enabler, something that can help you open additional doors for your business and stand out from your competition.” *Id.* ¶ 54.
- In a March 2019 podcast, Brown stated that SolarWinds was “focused on . . . heavy-duty hygiene.” *Id.* ¶ 221.
- In a 2020 blog post, Brown stated that SolarWinds “places a premium on the security of its products and makes sure everything is backed by sound security processes, procedures, and standards.” *Id.* ¶ 222.
- In an October 7, 2019 press release, SolarWinds stated that it “equips technology professionals with tools to help monitor, manage, and secure today’s complex IT environments.” The press release included Brown’s statement that “SolarWinds is committed to helping IT and security teams by equipping them with powerful, affordable solutions that are easy to implement and manage. Good security should be within the reach of all organizations.” *Id.* ¶ 223.
- In a December 12, 2019 press release posted on its website, SolarWinds stated that it was committed “to high security standards, which its partners rely on to help keep the systems they manage secure and compliant.” *Id.* ¶ 224. That press release included Brown’s

statement that SolarWinds and its employees “are always striving to give our partners a leading edge while also fostering a community built on a bedrock of trust,” and that meeting security standards “demonstrate[s] a vendor’s commitment to privacy and security—something we always strive to improve upon in all we do.” *Id.*

The Court dismisses the AC’s claims based on these statements, because each qualifies as non-actionable corporate puffery, “too general to cause a reasonable investor to rely upon them.” *ECA*, 553 F.3d at 206. None of these challenged materials purport to describe SolarWinds’ cybersecurity practices or general business practices at the level of detail at which a reasonable investor would have relied on them in making investment decisions. The statements are “too generic to express any objective fact.” *In re Synchrony Fin. Sec. Litig.*, 988 F.3d 157, 173 (2d Cir. 2021); *see, e.g., In re JP Morgan Chase Sec. Litig.*, 363 F. Supp. 2d 595, 632–33 (S.D.N.Y. 2005) (corporate defendant’s representations of “itself as an institution of integrity with sound risk-management procedures . . . amount[ed] to no more than puffery”); *Lasker v. N.Y. State Elec. & Gas Corp.*, 85 F.3d 55, 58–59 (2d Cir. 1996) (corporate statements that company refused to “compromise its financial integrity,” and had a “commitment to create earnings opportunities,” and that these “business strategies [would] lead to continued prosperity” were puffery); *In re Gentiva Sec. Litig.*, 932 F. Supp. 2d 352, 370 (E.D.N.Y. 2013) (“The Court finds that the descriptions at issue here—that the compliance programs was ‘robust’ or ‘best-of-class’ and that the company’s financial reporting was ‘very conservative’—fall into the category of commonplace statements too general to cause reliance by a reasonable investor.” (internal quotation marks omitted)).

### 3. Form S-1 Cybersecurity Risk Disclosure

The SEC also brings fraud charges against the defendants—again under theories of misrepresentation and scheme liability—based on SolarWinds’ cybersecurity risk disclosure, originally made in its 2018 Form S-1 registration and incorporated by reference in its ensuing

periodic Form 10-K, 10-Q, and S-8 filings. Based on the same disclosures, the SEC brings a false filing claim against SolarWinds. The Court dismisses all claims based on the risk disclosure.

*a. Securities Fraud: Misrepresentation Liability*

*i. False or Misleading Statements or Omissions*

The AC alleges that the cybersecurity risk disclosure was false and misleading, because it concealed the gravity of the cybersecurity risks that SolarWinds faced.

Decisions sustaining fraud claims based on the text of a cautionary risk disclosure are relatively uncommon. “Though ubiquitous in securities filings, cautionary statements of potential risk have only rarely been found to be actionable by themselves.” *In re FBR Inc. Sec. Litig.*, 544 F. Supp. 2d 346, 360 (S.D.N.Y. 2008) (internal citation omitted). Issuers instead commonly include cautionary language of a risk disclosure as a shield, with the goal of “insulat[ing] a defendant from liability under the ‘bespeaks caution’ doctrine.” *Id.* at 361.

In *In re Van der Moolen Holding N.V. Sec. Litig.*, 405 F. Supp. 2d 388 (S.D.N.Y. 2005), the late Judge Sweet first held that “under certain circumstances, cautionary statements can give rise to [securities fraud] liability.” *Id.* at 400 (noting split in authority whether cautionary statements can themselves be actionable). Ensuing cases that have held risk disclosures actionable have done so in the narrow circumstance where it was well pled that the disclosure “warn[ed] of a risk that has already occurred.” *Marcu v. Cheetah Mobile Inc.*, No. 18 Civ. 11184 (JMF), 2020 WL 4016645, at \*6 n.19 (S.D.N.Y. July 16, 2020) (citing *Gregory v. ProNAi Therapeutics Inc.*, 297 F. Supp. 3d 372, 406 n.19 (S.D.N.Y. 2017), *aff’d*, 757 F. App’x 35 (2d Cir. 2018)); *see, e.g., In re Facebook, Inc. IPO Sec. & Derivative Litig.*, 986 F. Supp. 2d 487, 516 (S.D.N.Y. 2013) (risk warning actionable where it “misleadingly represented that this

revenue cut was merely possible when, in fact, it had already materialized.”); *Dodona I, LLC v. Goldman, Sachs & Co.*, 847 F. Supp. 2d 624, 647 (S.D.N.Y. 2012) (boilerplate disclosure actionably misleading because it inaccurately represented defendants’ assessment of risk in the subprime mortgage market); *Chapman v. Mueller Water Prod., Inc.*, 466 F. Supp. 3d 382, 405 (S.D.N.Y. 2020) (“[C]ourts in this Circuit have held that a risk disclosure can itself constitute a material misrepresentation when it presents as a risk an event that has already transpired.”).<sup>37</sup>

In evaluating the risk disclosure here, the Court nonetheless assumes *arguendo* that such a risk disclosure can be actionable if it could have misled a reasonable investor, in any manner, “about the nature of the risk when he invested.” *In re Mylan N.V. Sec. Litig.*, 16 Civ. 7926 (JPO) 2018 WL 1595985, at \*9 (S.D.N.Y. 2018). The SEC, however, has not so pled. On the contrary, SolarWinds’ cybersecurity risk disclosure, reproduced in full above, enumerated in stark and dire terms the risks the company faced were its cybersecurity measures to fail. Although a reasonable investor could easily have been led astray by the Security Statement, such an investor could not have been misled by the risk disclosure.

---

<sup>37</sup> To the extent *Van der Moolen* suggests that risk disclosures may be actionable on other grounds—for example, for not warning in stronger terms about an as-yet non-materialized risk—ensuing decisions have not embraced that view. See, e.g., *Marcu*, 2020 WL 4016645, at \*5 n.2 (“*Van der Moolen* could be read to endorse a broader proposition: that a defendant can be held liable based on little or nothing more than an allegedly inadequate warning of risk. Once again, there is good reason to avoid—or decline to follow—that reading.”); *In re FBR Inc. Sec. Litig.*, 544 F. Supp. 2d at 360 (“[T]he Court declines to find that boilerplate risk factors can *never* provide a basis for liability. However, in the case *sub judice*, the Court finds that defendants’ boilerplate description of its regulatory risks could not have been misleading to a reasonable investor as the description ‘said nothing company-specific, and no reasonable investor would infer anything about the state of [the company’s regulatory] compliance.’” (quoting *Anderson v. Abbott Labs.*, 140 F. Supp. 2d 894, 905 (N.D. Ill. 2001)); *In re Noah Educ. Holdings, Ltd. Sec. Litig.*, No. 08 Civ. 9203 (RJS), 2010 WL 1372709, at \*7 (S.D.N.Y. Mar. 31, 2010) (“The Court acknowledges the tension between *In re FBR Inc. Securities Litigation* and *In re Van der Moolen Holding N.V. Securities Litigation*. . . . [T]he Court finds the reasoning of *In re FBR* persuasive, and concludes that its analysis better fits the facts of this case.” (citation omitted)).

The SEC first faults the cybersecurity risk disclosure as unacceptably boilerplate and generic. AC ¶¶ 239, 298. It argues that a generic disclosure of potential vulnerability was inadequate given the company's internal recognition that its security systems were faulty. This argument, and the SEC's portrait of the risk disclosure as opaque, is incorrect.

The disclosure set out in some detail the unique risks in this area that SolarWinds, as a cybersecurity company, faced. It began by setting out risks that are fairly termed generic: "If we sustain system failures, cyberattacks against our systems or against our products, or other data security incidents or breaches, we could suffer a loss of revenue and increased costs, exposure to significant liability, reputational harm and other serious negative consequences." Form S-1 at 3. But it then went further to list specific risks SolarWinds faced given its business model, as a company "heavily dependent on [its] technology infrastructure." *Id.* These included that SolarWinds was "vulnerable to damage or interruption" from "traditional computer 'hackers,'" "malicious code (such as viruses and worms)," "denial-of-service attacks" and "sophisticated nation-state and nation-state-supported actors (including advanced persistent threat intrusions)." *Id.* The disclosure added that "[t]he 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 the number, intensity and sophistication of attempted attacks." *Id.* It also warned that SolarWinds might prove unable to anticipate, prevent, or detect such attacks.

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, we may be unable to anticipate these techniques or 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.

*Id.* at 3–4. Finally, the risk disclosure alerted investors to the potential for a security breach to have very damaging consequences to the company.

The foregoing security problems could result in, 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. Our remediation efforts may not be successful and could result in interruptions, delays or cessation of service and loss of existing or potential customers that may impede sales of our products or other critical functions. We could lose existing or potential customers in connection with any actual or perceived security vulnerabilities in our websites or our products.

*Id.* at 4.

Viewed in totality, this risk disclosure was sufficient to alert the investing public of the types and nature of the cybersecurity risks SolarWinds faced and the grave consequences these could present for the company's financial health and future. *See, e.g., Rombach v. Chang*, 355 F. 3d 164, 176 (2d Cir. 2004) (“While some of these cautionary statements were formulaic, we conclude that as a whole they provided a sobering picture of [the company's] financial condition and future plans.”). In breadth, specificity, and clarity, SolarWinds' disclosure comfortably aligned with risk disclosures—of various types—that courts have upheld as adequate. *See, e.g., Garnett v. RLX Tech. Inc.*, 632 F. Supp. 3d 574, 602 (S.D.N.Y. 2022), *aff'd sub nom. Tseng v. De Vries*, No. 22-2787, 2023 WL 8073087 (2d Cir. Nov. 21, 2023) (statements warning investors “to the existing regulatory strictures in China governing e-cigarettes” and “the prospect that heightened regulation of these products would be undertaken” “were sufficient to pick up the regulatory risk that later materialized: that China would decide to calibrate regulation of e-cigarettes to track its regulation of tobacco products”); *In re Heartland Payment Sys., Inc. Sec. Litig.*, No. 09 Civ. 1043 (AET), 2009 WL 4798148, at \*5–6 (D.N.J. Dec. 7, 2009) (March 2008 Form 10-K statement that represented that company “place[d] significant emphasis on

maintaining a high level of security” while warning that “computer systems could be penetrated by hackers” was not made materially misleading by non-disclosure of a December 2007 attack by hackers against company’s computer network, as “the 10-K did not make any statements to the effect that the company’s network was immune from security breaches or that no security breach had ever occurred.”).

To the extent the SEC, in terming the disclosure generic, means to fault SolarWinds for not spelling out these risks in greater detail, the case law does not require more, for example, that the company set out in substantially more specific terms scenarios under which its cybersecurity measures could prove inadequate. As decisions in this District have recognized, the anti-fraud laws do not require cautions to be articulated with maximum specificity. Indeed, these decisions have recognized policy reasons not to require as a matter of law that disclosures be made at the level of specificity known to the issuer. Spelling out a risk with maximal specificity may backfire in various ways, including by arming malevolent actors with information to exploit, or by misleading investors based on the formulation of the disclosure or the disclosure of other risks at a lesser level of specificity. *See, e.g., In re Mylan N.V. Sec. Litig.*, 2018 WL 1595985, at \*1 (“[T]he more specific the caution, the more likely it is to mislead a reasonable investor. For example, a caution that ‘input prices may rise next quarter’ would not cause a reasonable investor to conclude that the prices of all inputs had remained flat or declined in the previous quarter. But a caution that ‘the price of our primary input may rise above \$5 next quarter’ could certainly cause a reasonable investor to conclude that the price was, at present, \$4.99 or less.” (internal citations omitted)); *Chapman*, 466 F. Supp. 3d at 405–06 (disclosure of the “risk that new products *may* have quality or other defects or deficiencies” was not materially false or misleading because when “read in context, [the] risk disclosure[] cannot be understood as a

guarantee that none of ‘new products and systems’ that [the company] shipped or expected to ship would have defects or deficiencies that would require repair or replacement”); *In re Coty Inc. Sec. Litig.*, No. 14 Civ. 919 (RJS), 2016 WL 1271065, at \*11 (S.D.N.Y. Mar. 29, 2016) (“[E]ven if it could be demonstrated that some of these events had occurred prior to June 12, 2013, [the company’s] highly vague and generic discussion of potential market risks ‘could not have been misleading to a reasonable investor as the description said nothing company-specific, and no reasonable investor would infer anything about the state of’ the company”).

The SEC next argues that the risk disclosure was materially misleading because SolarWinds did not update it to take account of two cybersecurity incidents it learned of from customers in the period leading up to the SUNBURST attack. These were the incidents reported to it by USTP and PAN. The SEC argues SolarWinds’ failure to update its disclosure to report these incidents was a material misrepresentation, in that it caused the disclosure to present “as a risk an event that ha[d] already transpired.” *Chapman*, 466 F. Supp. 3d at 405; *see also Meyer v. Jinkosolar Holdings Co.*, 761 F.3d 245, 250 (2d Cir. 2014) (“A generic warning of a risk will not suffice when undisclosed facts on the ground would substantially affect a reasonable investor’s calculations of probability.”).

As the body of cases reviewed above reflects, the SEC’s liability theory is conceptually sound: a risk’s materialization may require modifying a disclosure that had cast the risk as latent (*i.e.*, unrealized). Those decisions apply, in the context of risk disclosures, familiar principles in securities fraud case law, to wit, that “once a company speaks on an issue or topic, there is a duty to tell the whole truth.” *Id.* And: “when an offering participant makes a disclosure about a particular topic, whether voluntary or required, the representation must be complete and accurate.” *In re Morgan Stanley Info. Fund Sec. Litig.*, 592 F.3d 347, 366 (2d Cir. 2010)

(internal quotation marks omitted); *see also Meyer*, 761 F.3d at 247 (“failure to disclose ongoing, serious pollution problems rendered misleading statements in a prospectus describing prophylactic measures taken to comply with Chinese environmental regulations”); *Menaldi v. Och-Ziff Cap. Mgmt. Grp. LLC*, 164 F. Supp. 3d 568, 584 (S.D.N.Y. 2016) (complaint plausibly alleged “actionable misstatements about the existence and risks of regulatory proceedings” where company suggested it “was not facing an investigation that could have a material impact on its business, when, in fact, it was facing such an investigation”).

Here, however, on the facts pled, SolarWinds did not have an obligation to update its cybersecurity risk disclosure in light of the USTP and PAN incidents. The cybersecurity risk disclosure already warned investors, in sobering terms, that “[o]ur systems . . . are vulnerable to damage or interruption” from a variety of cyberattacks. Form S-1 at 3. It noted that “[t]he risk of a security breach . . . through cyberattacks or cyber intrusion . . . has generally increased the number, intensity and sophistication of attempted attacks.” *Id.* And it noted that the company “may be unable to anticipate these techniques or to implement adequate preventative measures.” *Id.* This language warned investors about the serious threat of cyberattacks and cyber intrusions that the company faced. And it warned them that SolarWinds was not positioned to, and could not be expected to, anticipate or prevent all such intrusions. In light of this fulsome disclosure, SolarWinds did not have a duty to disclose the fact of individual cyber intrusions or attacks. It had already disclosed the likelihood of these as, regrettably, a fact of life. *Cf. In re Bank of Am. AIG Disclosure Sec. Litig.*, 980 F. Supp. 2d 564, 579 (S.D.N.Y. 2013), *aff’d*, 566 F. App’x 93 (2d Cir. 2014) (“[W]here there is disclosure that is broad enough to cover a specific risk, the disclosure is not misleading simply because it fails to discuss the specific risk.”).

With the perspective of hindsight, particularly with the benefit of knowledge of the later-occurring SUNBURST attack, the USTP and PAN incidents are easily depicted as far more than quotidian—as the proverbial canaries in the coal mine. The SUNBURST attack made apparent to SolarWinds that it had been victimized by a sweeping intrusion affecting many customers, in which malicious actors inserted malicious code in the Orion software that, once received by customers and installed, was apt to reach out to external websites. In hindsight, the USTP and PAN incidents present as prefiguring SUNBURST.

But the adequacy of SolarWinds' pre-SUNBURST risk disclosure must be evaluated based on the information the company had in real time and the conclusions it reasonably drew from that information. And the AC does not plausibly plead that, before SUNBURST, SolarWinds had concluded that it had been victim to a systematic intrusion apt to materially damage the company, its Orion product, and its customers, or that SolarWinds' failure to so conclude reflected either a deliberate or reckless ignorance to that reality.

On the contrary, on the facts pled, SolarWinds did not have enough information about these incidents to reliably draw that conclusion. There was, to be sure, a similarity to the USTP and PAN incidents. In each, the customer reported that the BusinessLayer portion of the Orion software was reaching out to external websites, for unknown purposes. But there were also differences. As to USTP, Orion was attempting to provide information about the network on which it was located. As to PAN, Orion was reaching out to a website and downloading a malicious file. And insofar as SolarWinds understood, these behaviors had been uncovered by different means. USTP reported the suspicious activity after the agency had installed the software on a trial basis. AC ¶ 269. PAN reported to SolarWinds that it learned of Orion's

outreach not as a result of a live attack, but during a red-team exercise—a controlled simulation of an attack. Dkt. 117 at 1–2.

Critically, as pled, SolarWinds, after investigating, was unable to determine the “root cause” of either set of intrusions. *See* AC ¶ 270 (“SolarWinds’ internal investigation [of the USTP attack] failed to uncover the root cause for the malicious activity”); *id.* ¶ 284 (as to PAN, “SolarWinds again failed to . . . uncover the root cause for the malicious activity”). The AC, in fact, alleges that, after the USTP attack, Brown determined that there were two scenarios that could explain the incident. In one, the attackers might be gaining access via the customer’s system. Alternatively, the attacker might be targeting the Orion product ““for methods to utilize it in larger attacks.”” *Id.* ¶ 272. The AC does not allege facts that made it unreasonable for Brown or SolarWinds to entertain the first scenario, in which the source of the vulnerability was the customer’s system, not SolarWinds’ product. Nor does the AC allege that SolarWinds had definitively determined that the two incidents were linked.<sup>38</sup>

On the facts pled, SolarWinds was undeniably on notice from two customers of unusual and concerning activity involving its Orion product. It was aware of the possibility that the two incidents were related. But—even with the benefit of investigative documents and deposition

---

<sup>38</sup> The AC also alleges that certain low-level employees at SolarWinds recognized the potential similarities between the USTP and PAN incidents. Although employees informally commented on these similarities in group instant message conversation, on the facts pled, no employee had definitively concluded they were linked. *See, e.g.*, AC ¶ 281. In October 2020, Brown was also informed about the similarities. On October 16, 2020, he was forwarded an email that stated in part: “[PAN] in touch with customer support and it seems they had a breach similar to [USTP]. This does not appear to be OIP (that we know of yet) related, but the business layer was used in the attack chain according to them. In this case however it was to do [BusinessLayer] running some malicious download.” *Id.* ¶ 280. The email, however, also noted differences. The PAN incident, unlike the USTP attack, did not appear to implicate the OIP server. And the malicious activity observed by PAN involved the BusinessLayer running a malicious download, which was not the case for USTP.

discovery—the SEC has not pled more. It has not pled facts known to the company that then demonstrated a singular cyberattack, let alone a serious or pervasive one. It has not pled facts that the company had reached any such internal conclusion. It has not pled facts that the company internally had concluded it was presented with a serious threat to its financial well-being or business prospects. In these circumstances, with the significance and nature of the two incidents as more unknown than known, the securities laws did not impose on SolarWinds an obligation to update its cybersecurity risk disclosure. Its existing disclosure drove home that the company’s “systems are vulnerable” to cyberattack. Form S-1 at 3. An updated disclosure could say little more than that the company was investigating but had not reached a conclusion as to two customer-reported incidents involving Orion. The SEC has not cited authority supporting a legal duty to update its risk disclosure in the face of this level of knowledge.

The SEC relies on decisions finding risk disclosures inadequate where the risk had already transpired. *See Chapman*, 466 F. Supp. 3d at 405 (“[C]ourts in this Circuit have held that a risk disclosure can itself constitute a material misrepresentation when it presents as a risk an event that has already transpired.”). But, given the uncertain character, source, and relatedness of the two incidents, SolarWinds had not determined that the material risks of which it had warned had in fact transpired. The cybersecurity disclosure warned of the company’s vulnerability to “traditional computer ‘hackers,’” “malicious code (such as viruses and worms),” “employee theft or misuse,” “denial-of-service attacks” and “sophisticated nation-state and national-state supported actors (including advanced persistent threat intrusions).” Form S-1 at 3. But on the facts pled, SolarWinds did not know enough to reliably sort the USTP or PAN incidents under any of these headers, and it had not done so. It had not yet determined that the incident reflected a vulnerability within SolarWinds’ own systems, as opposed to those of its

customers. This line of authority is thus inapposite. See *In re Heartland Payment Sys., Inc. Sec. Litig.*, No. 09 Civ. 1043, 2009 WL 4798148, at \*6–7 (D.N.J. Dec. 7, 2009) (defendants did not have a “general duty” to disclose a 2007 structured query language (SQL) cyberattack because “the existence of such a breach [did] not make any of Defendants’ statements concerning their security systems misleading”); *Gregory*, 297 F. Supp. 3d at 406 n.19 (“[W]hile the risk of failure [of the PNT2258 drug candidate] was present (and disclosed) at all times, the reality of failure of PNT2258 did not durably come to pass during the Class Period.”); *Chapman*, 466 F. Supp. 3d at 405–06 (rejecting claim that language warning of the “risk that new products *may* have quality or other defects or deficiencies” was false and misleading because it did not reveal that “significant risks, deficiencies and failures associated with new products were already occurring”; read in context, the “risk disclosure[] cannot be understood as a guarantee that none of the ‘new products and systems’ . . . would have defects or deficiencies”); *Noah Educ.*, 2010 WL 1372709, at \*8 (“[T]he lengthy, forward-looking recitation of risks facing [the company] did not imply that none of these risks, at least to some extent, would affect [its] most recent fiscal quarter.”).

Accordingly, the AC does not plausibly plead that the cybersecurity risk disclosure was materially false or misleading.

ii. Scierter

In the interest of completeness, the Court addresses the AC’s claim that Brown acted with scierter in not amending the cybersecurity disclosure in light of the USTP and PAN incidents.

AC ¶ 298.<sup>39</sup> Brown signed cybersecurity sub-certifications and supplied other information to the

---

<sup>39</sup> Brown’s scierter is the primary basis on which the AC contends that SolarWinds acted with scierter with regard to the alleged misleading risk disclosures. SEC Opp. at 40–41. The SEC also briefly argues that even in the absence of Brown’s scierter, SolarWinds could still be found liable on the basis of “collective negligence.” *Id.* at 41. The Court addresses this argument below.

senior executives responsible for certifying the SEC filings containing the disclosure. The SEC argues that Brown intentionally or recklessly disregarded discrepancies between the risks that the disclosure identified and the actual risks of which SolarWinds had become aware as a result of the reports from USTP and PAN.

The AC's allegations do not adequately plead Brown's scienter.<sup>40</sup> It falls far short of pleading with particularity his scienter via conscious misbehavior. And it does not attempt to plead his scienter based on motive and opportunity.

---

<sup>40</sup> To the extent the AC brings claims against Brown as a principal violator under Section 10(b) of the Exchange Act and Rule 10b-5 based on the cybersecurity risk disclosure, Brown has a substantial additional argument against liability, even assuming *arguendo* that the AC had pled a material misrepresentation in these and scienter on his part. Under Section 10(b) and Rule 10b-5, a defendant must have "made" the allegedly material misstatements. *Janus Capital Group Inc. v. First Derivative Traders*, 564 U.S. 135, 141 (2011); *see* 17 C.F.R. § 240.10b-5(b) (Rule 10b-5(b) makes it unlawful "[t]o make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading") (emphasis added). "[T]he maker of a statement is the person or entity with ultimate authority over the statement, including its content and whether and how to communicate it." *Janus*, 564 U.S. at 142. Following *Janus*, "an executive may be held accountable where the executive had ultimate authority over the company's statement; signed the company's statement; ratified and approved the company's statement; or where the statement is attributed to the executive." *In re Fanni Mae 2008 Sec. Litig.*, 891 F. Supp. 2d 458, 473 (S.D.N.Y. 2012), *aff'd*, 525 F. App'x 16 (2d Cir. 2013). There is a substantial argument that the AC does not allege any of the above as to Brown with respect to the risk disclosure. It alleges that he was responsible for the disclosure's technical content and accuracy, and that he was asked factual questions, reviewed documentation, provided relevant information, and signed sub-certifications that were relied on by the senior executives responsible for signing and certifying the filings that contained the risk disclosures. AC ¶¶ 242, 298. On the pleadings, these executives, not Brown, appear to have had "ultimate authority" over the company's risk disclosure. This argument, however, would not bar a claim against Brown for aiding and abetting liability. Nor would it impair the SEC's claim against Brown under Section 17(a) of the Securities Act, because *Janus* does not apply to Section 17(a)(2), which does not require for liability that the defendant have made the actionable statement. *See Rio Tinto*, 41 F.4th at 50 n. 2 (2d Cir. 2022) (citing *SEC v. Knight*, 694 F. App'x 853, 856 n.2 (2d Cir. 2017), *as amended*, (June 7, 2017)); *compare* 15 U.S.C. § 77q(a)(2) (Securities Act Section 17(a)(2)) (in operative language, making it illegal to "obtain money or property by means of any untrue statement of a material fact or any omission to state a material fact") (emphasis added), *with* 17 C.F.R. § 240.10b-5(b) (in operative language, making actionable "any untrue statement of a material

To begin, as noted, the AC does not viably allege that the cybersecurity disclosure was actionable, making its claim of Brown's scienter with respect to a misleading statement therein logically unsustainable. Simply put, given that the risk disclosure was not inaccurate, the AC cannot plausibly allege that Brown actually "understood that [SolarWinds'] public statements were inaccurate." *Sanofi Sec. Litig.*, 87 F. Supp. 3d at 534.

Beyond that, the AC does not allege that Brown consciously or deliberately withheld information from the persons responsible for creating the risk disclosure. On the contrary, it alleges that Brown was among those responsible for the formidable list of cybersecurity risks that the disclosure enumerated. AC. ¶ 22. And it alleges that he created internal presentations, which he shared with top-level executives, that openly discussed SolarWinds' cybersecurity deficiencies. *See, e.g., id.* ¶¶ 45, 49–51, 62–63. Brown's revelation of these deficiencies is in tension with the AC's theory that he deliberately concealed cybersecurity risks from the senior staff responsible for the risk disclosure. Moreover, assuming the cybersecurity disclosure was faulty for its lack of a reference to the USTP and PAN incidents, the AC does not plead facts that made it unreasonable for Brown to view the broad cautionary language in the disclosure as adequately capturing the risks to the company. With the nature and significance of the two incidents unclear, the AC also does not viably plead that Brown had a duty to disclose the information known about these to officials formulating the disclosure. *See Kalnit v. Eichler*, 264 F.3d at 144 ("Because . . . this case does not present facts indicating *a clear duty to disclose*, plaintiff's scienter allegations do not provide *strong* evidence of conscious misbehavior or recklessness."). In sum, on the facts plead, Brown's conduct with respect to the risk disclosure

---

fact or to omit to state a material fact necessary in order to make the statements *made*, in the light of the circumstances under which they were made, not misleading") (emphasis added).

was not “highly unreasonable” or “an extreme departure from the standards of ordinary care.” *S. Cherry St.*, 573 F.3d at 109.

As an alternative means of pleading SolarWinds’ scienter with respect to the disclosure, the SEC alleges, that, even if Brown lacked the requisite scienter, the disclosed risks so grossly differed from the actual risks that a factfinder could infer that SolarWinds deviated from the standards of ordinary care regarding them. This argument is a non-starter. Although corporate scienter need not be based on that of a named individual defendant, *Plumbers & Pipefitters Loc. Union No. 719 Pension Tr. Fund v. Conseco Inc.*, No. 09 Civ. 6966 (JGK), 2011 WL 1198712, at \*23 (S.D.N.Y. Mar. 30, 2011), to allege corporate scienter, a complaint must plead facts giving rise to a strong inference that (1) “someone whose intent could be imputed to the corporation acted with the requisite scienter,” *Dynex*, 531 F.3d at 195; or (2) the statements “would have been approved by corporate officials sufficiently knowledgeable about the company to know that those were misleading,” *Loreley Fin. (Jersey) No. 3 Ltd. v. Wells Fargo Sec., LLC*, 797 F.3d 160, 177 (2d Cir. 2015) (internal quotation marks omitted).

The AC does not plead either. It does not allege with particularity that the officers who approved the cybersecurity risk disclosure understood it was misleading. Nor, particularly given the holding that the disclosure was not actionable, does it allege a “misrepresentation significant enough” to infer that a “corporate officer whose intent may be imputed to the corporation was aware of the misrepresentation.” *Plumbers & Pipefitters*, 2011 WL 1198712, at \*23. The Second Circuit in *Teamsters* gave an example of a significant enough misrepresentation to support such an inference:

Suppose General Motors announced that it had sold one million SUVs in 2006, and the actual number was zero. There would be a strong inference of corporate scienter, since so dramatic an announcement would have been approved by corporate officials sufficiently knowledgeable about the company to know that the announcement was false.

*Id.* at 195–96; *see also In re MBIA, Inc., SEC. Litig.*, 700 F. Supp.2d 566, 574 (S.D.N.Y. 2010) (non-disclosure of an \$8.1 billion exposure to collateralized debt obligations a sufficient basis on which to infer corporate scienter); *In re NovaGold Res. Inc. Sec. Litig.*, 629 F. Supp. 2d 272, 299–300 (S.D.N.Y. 2009) (misrepresentation of \$4.4 billion in capital costs a sufficient basis on which to infer corporate scienter). The omissions the SEC alleges here do not approach this scale. As canvassed above, because the company had limited information about the USTP and PAN incidents, their significance were highly uncertain. *See, e.g., Plumbers & Pipefitters*, 2011 WL 1198712, at \*22–24 (given company’s “extensive disclosure,” its alleged misstatements did not approach the magnitude necessary to allege corporate scienter); *In re Kandi Techs. Grp., Inc. Sec. Litig.*, No. 17 Civ. 1944 (ER), 2019 WL 4918649, at \*6 (S.D.N.Y. Oct. 4, 2019) (defendant’s “restate[ment] [of] several periods of its financial statements due to GAAP violations does not establish scienter, especially given the lack of effect on reported corporate income for the relevant time periods”).

*b. Securities Fraud: Scheme Liability*

The SEC alternatively alleges scheme liability against Brown, based on the sub-certifications he made that were used to fashion the cybersecurity risk disclosure. These, the SEC contends, were “inherently deceptive acts” that support scheme liability.

That claim fails, too. Scheme liability “hinges on the performance of an inherently deceptive act that is *distinct* from an alleged misstatement.” *SEC v. Kelly*, 817 F. Supp. 2d 340, 34 (S.D.N.Y. 2011); *see also WPP Lux. Gamma Three Sarl v. Spot Runner, Inc.*, 655 F. 3d 1039, 1057 (9th Cir. 2011) (“A defendant may only be liable as part of a fraudulent scheme based upon misrepresentations and omissions under Rules 10b-5(a) and (c) when the scheme also encompasses conduct beyond those misrepresentations or omissions.”). The scheme liability

provisions of Rule 10b-5 and Section 17 of the Securities Act cannot be used as a “back door into liability for those who help others make a false statement or omission” in violation of Rule 10b-5 and Securities Act Section 17. *Kelly*, 817 F. Supp. 2d at 343. Thus, where “the core misconduct alleged is in fact a misstatement, it [is] improper to impose primary liability . . . by designating the alleged fraud a ‘manipulative device’ rather than a ‘misstatement.’” *In re Smith Barney Transfer Agent Litig.*, 884 F. Supp. 2d 152, 161 (S.D.N.Y. 2012). Here, Brown’s sub-certification of allegedly false or misleading statements is the very conduct that the SEC uses to premise its misstatement claims under Rule 10b-5(b) and Securities Act Section 17(a). It thus cannot form the sole basis of its scheme liability claim. For this reason—and because SolarWinds’ filings have not been pled as actionable—the AC fails to adequately plead scheme liability with respect to Brown in connection with any of these SEC filings.

*c. False Filing Claim*

The SEC also brings false filing claims against SolarWinds based on the risk disclosure in its Form S-1 and later SEC filings under Section 13(a) of the Exchange Act and Exchange Act Rules 12b-20, 13a-1, 13a-11, and 13a-13. These provisions require filing “with the Commission accurate periodic and current reports,” *SEC v. Yuen*, No. 03 Civ. 4376 (MRP) (PLAX), 2006 WL 1390828, at \*41 (C.D. Cal. Mar. 16, 2006), and are satisfied “by the filing of complete, accurate, and timely reports,” *SEC v. Savoy Indus., Inc.*, 587 F.2d 1149, 1165 (D.C. Cir. 1978). A company “violates these provisions if it files a report that contains materially false or misleading information.” *Yuen*, 2006 WL 1390828, at \*41.

Insofar as the Court has held that the AC does not plead that the cybersecurity risk disclosure was materially false or misleading, it follows that the AC does not state a claim based on that disclosure under Section 13(a) and its implementing rules. The Court therefore dismisses

this claim. *See, e.g., SEC v. Patel*, 07 Civ. 39 (SM), 2009 WL 3151143, at \*32 (D.N.H. Sept. 30, 2009) (dismissing false filing claim where allegedly false statement in SEC filings was not material as a matter of law”); *Ponce v. SEC*, 345 F.3d 722, 736 (9th Cir. 2003) (upholding dismissal of false filing claim which had same factual basis as dismissed anti-fraud claims).<sup>41</sup>

### **C. Post-SUNBURST Disclosure**

The SEC brings securities fraud and false filing claims based on SolarWinds’ December 14 and 17, 2020 Form 8-Ks, in which it disclosed the SUNBURST attack.

#### **1. False or Misleading Statements or Omissions**

##### *a. December 14 Form 8-K*

The AC alleges that the December 14 Form 8-K was materially misleading because it did not disclose the earlier malicious activity reports from PAN and USTP and—in the SEC’s view—therefore gave the wrong impression that SUNBURST was a purely theoretical problem.

The Form 8-K stated, in relevant part:

- The company “has been made aware of a cyberattack that inserted a vulnerability within its Orion monitoring products which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run.”
- The company “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.”
- The company “has retained third-party cybersecurity experts to assist in an investigation of these matters, including whether a vulnerability in the Orion monitoring products was exploited as a point of any infiltration of any customer systems, and in the development of appropriate mitigation and remediation plans.”
- “SolarWinds is cooperating with the Federal Bureau of Investigation, the U.S. intelligence community, and other government agencies in investigations related to this incident.”

---

<sup>41</sup> In light of this dismissal, the Court also dismisses the aiding and abetting claim against Brown.

- “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 (the ‘Relevant Period’), 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.”
  - “Orion products downloaded, implemented or updated during the Relevant Period contained the vulnerability.”
  - “SolarWinds currently believes the actual number of customers that may have had an installation of the Orion products that contained this vulnerability to be fewer than 18,000.”
- “There has been significant media coverage of attacks on U.S. governmental agencies and other companies, with many of those reports attributing those attacks to a vulnerability in the Orion products. SolarWinds is still investigating whether, and to what extent, a vulnerability in the Orion products was successfully exploited in any of the reported attacks.”

12/14/2020 Form 8-K at 4.

The AC’s critique does not plausibly plead that the Form 8-K was materially misleading. As to this claim, perspective and context are critical. The Form 8-K was filed just two days after Mandiant contacted SolarWinds’ CEO to report discovery of a vulnerability in the Orion product resulting from malicious code inserted by a threat actor. Considered in light of this short turn-around, the Form 8-K disclosed the SUNBURST attack and surrounding events with appropriate gravity and detail. Its disclosure included that up to 18,000 customer-installed Orion products might contain the vulnerability. The disclosure was made at a time when SolarWinds was at an early stage of its investigation, and when its understanding of that attack was evolving.

The AC does not allege that any statement in the December 14 Form 8-K was factually inaccurate. It instead faults SolarWinds for casting SUNBURST’s compromise of the Orion product as purportedly only of theoretical concern, in that the Form 8-K stated that SUNBURST “could potentially allow an attacker to compromise the server on which the Orion products run”; that SolarWinds was considering “whether a vulnerability in the Orion monitoring products was

exploited”; and that the company was “still investigating whether, and to what extent, a vulnerability in the Orion products was successfully exploited.” *Id.* In fact, the SEC alleges, by December 14, 2020, Brown had concluded that the USTP and PAN incidents—in each of which the Orion software had reached out to external websites—were linked to SUNBURST. The omission of the fact that the malicious code inserted into Orion had already activated in these two instances, the SEC argues, made the Form 8-K materially misleading.

That is unpersuasive. Read fairly and in totality, the Form 8-K disclosure did not imply that the “vulnerability” it reported had been inserted into up to 18,000 customer-purchased Orion products, had nowhere yet been activated. The Form 8-K instead described the potential for the vulnerability to activate, and compromise the server, with respect to *all* such products in which the vulnerability had been inserted. Indeed, it recounted widespread news accounts of attacks on governmental agencies and private companies that attributed these attacks to a vulnerability in the Orion server. The SEC relies on the Form 8-K’s statement that SolarWinds was “still investigating whether, and to what extent, a vulnerability in the Orion products was successfully exploited in any of the reported attacks.” *Id.* This locution, it contends, conveyed to reasonable investors that SolarWinds was unaware of any instance in which the malicious software that had been inserted in Orion had reached out to extrinsic servers. But that is an *ipse dixit*. The SEC’s construction of the term “successful[] exploit[ation]” of the software as equating to external outreach by the infected software does not necessarily follow (and the Form 8-K does not anywhere so define “successful exploitation”). A reasonable investor could easily read that term to connote more consequential or damaging events or outcomes. And the AC does not identify any other part of the Form 8-K as purportedly rendered misleading by virtue of the nondisclosure that the USTP and PAN servers had reached out to extrinsic websites.

Importantly, too, although the AC pleads that Brown, on December 13, had mentally linked SUNBURST to the reports from USTP and PAN, it does not allege that Brown (or any other executive) had concluded that threat actors had “successfully exploited” the vulnerability inserted in those entities’ Orion products or that the outreach that had been detected there had “compromise[d] [their] servers.” *Id.* On the contrary, the AC describes the reports to SolarWinds from USTP and PAN in less dire terms. USTP reported that the “Orion software reached out to contact websites with an unknown purpose” and that the “software was *attempting* to provide information to the website about the network on which it was located.” AC ¶ 269 (emphasis added). PAN, for its part, reported that during its “red-team” simulation, Tr. at 61, the Orion software was “reaching out to a website and downloading a malicious file,” *id.* ¶ 279.

In these circumstances, the AC does not plead with particularity that the Form 8-K—which by any measure bluntly reported brutally bad news for SolarWinds—was misleading for not disclosing the USTP and PAN incidents. “Silence, absent a duty to disclose, is not misleading,” *Basic*, 485 U.S. at 239 n.17, and “[d]isclosure of . . . information is not required . . . simply because it may be relevant or of interest to a reasonable investor,” *In re Braskem S.A. Sec. Litig.*, 246 F. Supp. 3d 731, 752 (S.D.N.Y. 2017). The AC’s omission could be actionable only if disclosure of the USTP and PAN incidents was necessary to make the Form 8-K not misleading. *Matrixx Initiatives*, 563 U.S. at 44. The Form 8-K, however, was not misleading.

Mandiant’s report to SolarWinds—which prompted issuance of the Form 8-K—similarly fell short of stating that a threat actor had successfully exploited the vulnerability infecting the Orion product. The AC alleges that Mandiant reported to SolarWinds that upon discovering an “attack against its Orion platform,” AC ¶ 305, it reverse-engineered the Orion software code and identified a “vulnerability in the Orion software as a result of malicious code that had been

inserted into the Orion product by a threat actor,” *id.* at ¶ 306. On the facts pled, however, Mandiant did not represent to SolarWinds that the threat actors had gone farther, so as to compromise its servers and infiltrate its network.

Thus, the three customers had all reported that the Orion product, when installed, had reached out to external websites;<sup>42</sup> USTP had reported that Orion had sent information about the server it was located on; and PAN had reported that Orion had downloaded malicious files during a red-team exercise. Although the potential for grave harm was obvious (as the Form 8-K made clear), the AC does not allege that such harm was known to have befallen these customers, including from the malicious file download that PAN had reported.<sup>43</sup> The heart of the Form 8-K’s disclosure—that a cyberattack had “inserted a vulnerability within [SolarWinds’] Orion monitoring products” and that the vulnerability “if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run”—fairly captured the known facts. 12/14/2020 Form 8-K at 4. It is faithful to the AC’s account of what SolarWinds then knew from its customers.

---

<sup>42</sup> Brown’s testimony about Mandiant’s report to SolarWinds implies that the software had reached out to external websites insofar it emitted a “stream of data.” *See* AC ¶ 307 (“The code that he saw that was dropped that was supplied by [Mandiant], decompiled code gave us a full path. And there is plenty of investigation to show that, okay, business layer host was involved. This was a stream of data—this is what—oh, this matched what [USTP] had seen. So it wasn’t trying to attack us, it had a different purpose. So it became very, very apparent extremely quickly that that’s what the cases were.”).

<sup>43</sup> The AC notes that in internal presentations before SUNBURST, employees used pungent language to describe the USTP incident. For example, on July 10, 2020, an employee termed the incident a “customer compromise” and stated that the “attack [] was successful.” AC ¶ 313. The PAN incident was likewise internally referred to as a “breach.” *Id.* ¶ 315. These snippets do not substantively contradict the Form 8-K or make it materially misleading.

The lengthy Form 8-K disclosure, read as a whole, captured the big picture: the severity of the SUNBURST attack. This made the absence of a reference to the two earlier incidents immaterial. The Form 8-K described the event as a “cyberattack” that was “likely the result of a highly sophisticated, targeted and manual supply chain attack by an outside nation state.” *Id.* It reported that the “vulnerability was inserted within the Orion products and existed in updates released between March and June 2020”; and “Orion products downloaded, implemented or updated during [March to June 2020] contained the vulnerability.” *Id.* It estimated that up to 18,000 customers “may have had an installation of the Orion products that contained this vulnerability.” *Id.* It noted significant media reports “of attacks on U.S. governmental agencies and other companies” that “attribute[ed] those attacks to a vulnerability in the Orion products.” *Id.* It acknowledged its ongoing investigation into “whether, and to what extent, a vulnerability in the Orion products *was successfully exploited* in any of the reported attacks.” *Id.* (emphasis added). And the market got the message. SolarWinds’ share price dropped more than 16% the day of the announcement, and another 8% the next day. AC ¶ 318. The additional disclosure about the USTP and PAN incidents that the SEC contends was obligatory “was not materially different from the information that was already publicly disclosed.” *Bank of Am. AIG Disclosure Sec. Litig.*, 980 F. Supp. 2d at 576.<sup>44</sup>

The AC thus does not adequately plead that the December 14 Form 8-K was materially false or misleading.

---

<sup>44</sup> When SolarWinds eventually reported the USTP and PAN incidents in its Form 8-K of January 11, 2021, its stock price barely moved. *See* Turner Decl., Ex. 6 (chart); *Bank of Am. AIG Disclosure Sec. Litig.*, 980 F. Supp. 2d at 578, *aff’d*, 566 F. App’x 93 (2d Cir. 2014) (absence of market reaction to disclosure of omitted information “underscores that no reasonable investor would have considered such information material when purchasing stock” in company).

*b. December 17 Form 8-K*

On December 17, SolarWinds filed an additional Form 8-K, updating its disclosure, in relevant part, as follows:

- “On Saturday, December 12, our CEO was advised by an executive at FireEye of a security vulnerability in our Orion Software Platform which was the result of a very sophisticated cyberattack on SolarWinds. We soon discovered that we had been the victim of a malicious cyberattack that impacted our Orion Platform products as well as our internal systems. While security professionals and other experts have attributed the attack to an outside nation-state, we have not independently verified the identity of the attacker.”
- “Immediately after this call, we mobilized our incident response team and quickly shifted significant internal resources to investigate and remediate the vulnerability. Know that each of our 3,200 team members is united in our efforts to meet this challenge. We remain focused on addressing the needs of our customers, our partners and the broader technology industry.”
- “[W]e swiftly released hotfix updates to impacted customers that we believe will close the code vulnerability when implemented. These updates were made available to all customers we believe to have been impacted, regardless of their current maintenance status. We have reached out and spoken to thousands of customers and partners in the past few days, and we will continue to be in constant communication with our customers and partners to provide timely information, answer questions and assist with upgrades.”
- “We also have had numerous conversations with security professionals to further assist them in their research. We were very pleased and proud to hear that colleagues in the industry discovered a ‘killswitch’ that will prevent the malicious code from being used to create a compromise.”
- “This was a highly sophisticated cyberattack on our systems that inserted a vulnerability within our Orion® Platform products. This particular intrusion is so targeted and complex that experts are referring to it as the SUNBURST attack. The vulnerability has only been identified in updates to the Orion Platform products delivered between March and June 2020, but our investigations are still ongoing. Also, while we are still investigating our non-Orion products, to date we have not seen evidence that they are impacted by SUNBURST.”
- “The vulnerability was not evident in the Orion Platform products’ source code but appears to have been inserted during the Orion software build process.”

- “We have retained industry-leading third-party cybersecurity experts to assist us with this work and are actively collaborating with our partners, vendors, law enforcement and intelligence agencies around the world.”

12/17/2020 Form 8-K at 3.

This Form 8-K, SolarWinds’ second in the five days after learning of SUNBURST, thus centrally reiterated that SolarWinds had been a “victim of a malicious cyberattack that impacted [its] Orion Platform products as well as [its] internal systems.” *Id.* It did not reproduce the text from the December 14 Form 8-K that the AC faults as “theoretical.” The AC, however, again faults the December 17 Form 8-K for not disclosing the USTP and PAN incidents.

For the reasons above, this was not a material omission. The AC does not allege that, between December 14 and 17, SolarWinds came upon new information requiring disclosure of the two incidents. It does not allege new investigative findings to that effect. It instead realleges that Brown had learned of the link between these incidents and SUNBURST on December 13.

AC ¶ 307.

The Court accordingly does not find either Form 8-K false or misleading.<sup>45</sup>

## 2. **Scienter**

In any event, the AC does not plausibly allege Brown’s scienter with respect to the post-SUNBURST Form 8-Ks.<sup>46</sup> It alleges that Brown was responsible for confirming the accuracy of the technical statements in these, and that he “knew facts or had access to non-public information contradicting [SolarWinds’] public statements” in the Form 8-Ks. *Scholastic Corp. Sec. Litig.*,

---

<sup>45</sup> For this reason, the Court dismisses the AC’s false filing claim based on the Form 8-Ks, and the aiding and abetting claim against Brown with respect to that claim.

<sup>46</sup> As with the cybersecurity risk disclosure, discussed above, the AC does not allege that Brown was the “maker” of these filings, over which he did not have ultimate authority. He thus cannot be liable, as a primary violator, under Section 10(b) of the Exchange Act and Rule 10b-5. But he can still be held liable under Section 17(a) of the Securities Act.

252 F.3d at 76. Specifically, it claims that Brown, aware of the USTP, PAN, and Mandiant incidents, appreciated that the Form 8-Ks were misleading in disclosing only that the vulnerability in Orion “*could potentially allow* an attacker to compromise the server on which the Orion products run,” AC ¶ 310, whereas in fact it had already done so.

This theory fails. With the Court having held that lack of a reference to these incidents did not make the Form 8-Ks materially misleading, it follows that Brown cannot be found to have “recklessly failed” to disclose to the responsible officers at the company these incidents so as to enable their inclusion. *In re Centerline Holdings Co. Sec. Litig.*, 613 F. Supp. 2d 394, 401 (S.D.N.Y. 2009), *aff’d*, 380 F. App’x 91 (2d Cir. 2010). “[W]hen it is arguable that [defendants] did not have a duty to disclose such information,” “[d]efendants’ conduct cannot be described as ‘highly unreasonable,’ nor can it be said that their conduct ‘represents an extreme departure from the standards of ordinary care.’” *Id.* at 404. And the AC does not plead, other than in a conclusory fashion, that Brown refrained from urging inclusion of these incidents in order to hide from investors the “true impact of SUNBURST.” AC ¶ 314.<sup>47</sup>

As such, the AC fails to adequately plead scienter.

---

<sup>47</sup> Also in tension with the AC’s claims of scienter are the Form 8-K’s disclosures that the company “ha[d] retained third-party cybersecurity experts to assist in an investigation of these matters,” presumably with the intent to report the outcome of that probe, and was “cooperating with the Federal Bureau of Investigation, the U.S. intelligence community, and other government agencies in investigations related to this incident,” 12/14/2020 8-K at 4; and that that SolarWinds disclosed the link between SUNBURST and the USTP and PAN incidents less than a month later (on January 11, 2021). *See, e.g., In re Bausch & Lomb, Inc. Sec. Litig.*, 592 F. Supp. 2d 323, 343 (W.D.N.Y. 2008) (complaint failed to plead recklessness, in part, because company “immediately launched a massive independent investigation” and “voluntarily reported the matter to the SEC and announced it to the public”).

The Court accordingly dismisses the AC's fraud and false filing claims based on conduct following SUNBURST.<sup>48</sup>

## V. Internal Accounting Controls Claims

The SEC next brings claims against SolarWinds under Section 13(b)(2)(B) of the Exchange Act for failure to devise and maintain appropriate "internal accounting controls."

Section 13(b)(2)(B) provides:

- (b) Form of Report; Books, Records, and Internal Accounting; Directives
- (2) Every issuer which has a class of securities registered pursuant to section 78l of this title and every issuer which is required to file reports pursuant to section 78o(d) of this title shall—
  - (A) Make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer;
  - (B) devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that—
    - i. transactions are executed in accordance with management's general or specific authorization;
    - ii. transactions are recorded as necessary (I) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and (II) to maintain accountability assets;
    - iii. access to assets is permitted only in accordance with management's general or specific authorization; and
    - iv. the recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.

15 U.S.C. § 78m(b)(2).

The AC alleges that SolarWinds' cybersecurity deficiencies are actionable under Section 13(b)(2)(B)(iii) because (1) the company's source code, databases, and products were its most vital assets, but (2) as a result of its poor access controls, weak internal password policies, and

---

<sup>48</sup> The Court dismisses the AC's claim of scheme liability relating to the post-SUNBURST filings for the same reasons as above. The AC does not allege Brown engaged in an "inherently deceptive act that is *distinct* from an alleged misstatement." *Kelly*, 817 F. Supp. 2d at 343.

VPN security gaps, the company failed to limit access to these “only in accordance with management’s general or specific authorization,” enabling access by external attackers. AC ¶¶ 320–24. SolarWinds counters that although the Section 13(b)(2)(B) term gives the SEC authority to regulate an issuer’s “system of internal accounting controls,” that term, as a matter of statutory construction, cannot reasonably be interpreted to cover a company’s cybersecurity controls such as its password and VPN protocols. SolarWinds is clearly correct.

“As with any question of statutory interpretation, [the Court] begin[s] with the text of the statute to determine whether the language at issue has a plain and unambiguous meaning.” *Louis Vuitton Malletier S.A. v. LY USA, Inc.*, 676 F.3d 83, 108 (2d Cir. 2012) (citations omitted). A statute’s “plain meaning can best be understood by looking to the statutory scheme as a whole and placing the particular provision within the context of that statute.” *Saks v. Franklin Covey Co.*, 316 F.3d 337, 345 (2d Cir. 2003). In general, the Court “need proceed no further than the statute’s text and context in the broader statutory scheme.” *United States v. Epskamp*, 832 F.3d 154, 162 (2d Cir. 2016) (internal quotation marks omitted). But extrinsic materials may “have a role in statutory interpretation . . . to the extent they shed a reliable light on the enacting Legislature’s understanding of otherwise ambiguous terms.” *Exxon Mobil Corp. v. Allapattah Servs., Inc.*, 545 U.S. 546, 568 (2005).

The text of Section 13(b)(2)(B)(iii) requires that public companies “devise and maintain a system of *internal accounting controls* sufficient to provide reasonable assurances that . . . access to assets is permitted only in accordance with management’s general or specific authorization.” The provision thus applies only to a company’s “system of internal *accounting* controls.” For the SEC’s claim to survive dismissal, that provision must be construed to cover an issuer’s cybersecurity controls.

As a matter of statutory construction, that reading is not tenable. In various respects, the text of the statute strongly supports that the term “system of internal accounting controls” instead refers to a company’s *financial accounting*. The term “accounting” is widely defined in this manner—for example, as “the system of recording and summarizing *business and financial* transactions and analyzing, verifying, and reporting the results.” *Accounting*, Merriam-Webster Dictionary, <https://www.merriam-webster.com/dictionary/accounting> (emphasis added).<sup>49</sup> The SEC has not identified any dictionary definition favoring its construction. And the surrounding terms that Congress used in Section 13(b)(2)(B)—which refer, *inter alia*, to “transactions,” “preparation of financial statements,” “generally accepted accounting principles,” and “books and records”—are uniformly consistent with *financial* accounting. See *Yates v. United States*, 574 U.S. 528 (2015) (“[W]e rely on the principle of *noscitur a sociis*—a word is known by the company it keeps—to ‘avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words, thus giving unintended breadth to the Acts of Congress.’” (quoting

---

<sup>49</sup> Other dictionary definitions are in accord. See, e.g., *Accounting*, Black’s Law Dictionary (12th ed. 2024) (“(1) The act, practice, or system of establishing or settling financial accounts; esp., the process of recording transactions in the financial records of a business and periodically extracting, sorting, and summarizing the recorded transactions to produce a set of financial records.—Also termed *financial accounting*.”); *Accounting*, Oxford English Dictionary, [https://www.oed.com/dictionary/accounting\\_n?tab=meaning\\_and\\_use#36519035](https://www.oed.com/dictionary/accounting_n?tab=meaning_and_use#36519035) (“The action or process of reckoning, counting, or computing; numeration, computation, calculation.”); *Accounting*, The American Heritage Dictionary, <https://ahdictionary.com/word/search.html?q=accounting>, (“The practice or profession of maintaining the financial records of a business, including bookkeeping as well as the preparation of statements concerning the assets, liabilities, and operating results.”). Dictionaries of the time period in which the statute was enacted—that is, around 1977—used similar definitions of accounting. See, e.g., The Random House Dictionary 10 (1973) (“[T]he theory or system of organizing, maintaining, and auditing the books of a firm; art of analyzing the financial position and operating results of a business house from a study of its sales, purchases, overhead, etc. (distinguished from *bookkeeping*).”); *Accounting*, Black’s Law Dictionary (4th ed. 1968) (“An act or system of making up or settling accounts; a statement of account, or debit and credit in financial transactions.”); The American Heritage Dictionary 72 (1982) (“To make or render a reckoning, as of funds received and paid out or of persons or things.”).

*Gustafson v. Alloyd Co.*, 513 U.S. 561, 575 (1995)); *United States v. Williams*, 553 U.S. 285, 294 (2008) (“a word is given more precise content by the neighboring words with which it is associated”). The text thus defeats the SEC’s attempt to apply this provision to cybersecurity controls. And there is no evidence of any other sort that Congress intended its reference to “a system of internal accounting controls” to reach cybersecurity controls. That is no surprise. The statute was enacted in 1977—long before cybersecurity became a relevant concept in business or society.

Unsurprisingly, the few courts that have construed the term “internal accounting controls” as used in Section 13(b)(2)(B)(iii) have consistently construed it to address financial accounting. In *SEC v. World-Wide Coin Investments, Ltd.*, 567 F. Supp. 724 (N.D. Ga. 1983), Judge Robert L. Vining defined “internal accounting controls” as those controls that “safeguard assets and assure the reliability of financial records, one of their main jobs being to prevent and detect errors and irregularities that arise in the accounting systems of the company. Internal accounting controls are basic indicators of the reliability of the financial statements and the accounting system and records from which financial statements are prepared.” *Id.* at 750.<sup>50</sup> In

---

<sup>50</sup> The SEC contends that *World-Wide Coin Investments* adopted a broader conception of “internal accounting controls.” That is wrong. The company there was engaged in the sale of rare coins, precious metals, gold and silver coins, and bullion. In finding a violation of Section 13(b)(2)(B), the court noted that the “internal recordkeeping and accounting controls” at the company had been in “sheer chaos.” *World-Wide Coin Invs.*, 567 F. Supp. at 752. It did not have a “procedure implemented with respect to writing checks,” it did not employ a “separation of duties in the areas of purchase and sales transactions, and valuation procedures for ending inventory,” and employees were not “required to write source documents relating to the purchase and sale of coins, bullion, or other inventory.” *Id.* These deficiencies quintessentially relate to financial matters. The SEC seizes on the court’s passing observation that the company had “extremely lax security measures such as leaving the vault [of its rare coins and other inventory] unguarded.” *Id.* But that observation was not the heart of its analysis. In any event, because the company bought and sold rare coins, the physical security of its rare coin collection directly affected its inventory controls and its ability to financially audit “transactions and the disposition of World-Wide’s assets.” *Id.* The same cannot be said of SolarWinds’ cybersecurity measures.

*McConville v. SEC*, 465 F.3d 780 (7th Cir. 2006), as amended on denial of reh'g and reh'g en banc, (Jan. 17, 2007), the Seventh Circuit gave examples of internal accounting controls as including: “manual or automated review of records to check for completeness, accuracy and authenticity; a method to record transactions completely and accurately; and reconciliation of accounting entries to detect errors.” *Id.* at 790 (citing *In re Albert Glenn Yesner, CPA*, Initial Decision, Exchange Act Release No. 184, 2001 WL 587989, at \*33 (May 22, 2001); *Montgomery's Auditing* 9-2 (John Wiley & Sons, Inc. 12th ed. 1998)). And in a public administrative cease and desist proceeding brought by the SEC, Administrative Law Judge (“ALJ”) Robert G. Mahony, interpreted internal accounting controls as:

the policies and procedures adopted within an organization that operate as a means of promoting operational efficiency, reliability in financial reporting, and encouraging adherence to managerial policies, applicable laws, and regulations. Internal accounting controls are one element of a control system implemented to safeguard assets and promote reliable financial records. They provide reasonable assurance that transactions are authorized and recorded as necessary to permit the preparation of financial statements in conformity with GAAP, or other applicable criteria, as well as limiting access to records and providing for periodic review to test for inconsistencies.

*In re Albert Glenn Yesner, CPA*, Initial Decision, Exchange Act Release No. 184, 2001 WL 587989, at \*33 (May 22, 2001) (internal citations omitted).

In light of the above, the statutory requirement that a public issuer “devise and maintain a system of internal accounting controls” is properly read to require that issuer to accurately report, record, and reconcile *financial* transactions and events. A cybersecurity control does not naturally fit within this term, as a failure to detect a cybersecurity deficiency (*e.g.*, poorly chosen passwords) cannot reasonably be termed an *accounting* problem. Cybersecurity controls are undeniably vitally important, and their failures can have systemically damaging consequences. But these controls cannot fairly be said to be in place to “prevent and detect errors and

irregularities that arise in the accounting systems of the company.” *World-Wide Coin Ins.*, 567 F. Supp. at 750.

The SEC counters by arguing that *SEC v. Cavco Industries Inc.*, No. 21 Civ. 01507 (PHX) (SRB), 2022 WL 1491279, at \*4 (D. Ariz. Jan. 25, 2022), embraced its reading of the statutory term. The court there found that Cavco’s failure to follow its insider trading policy constituted an “internal accounting control” failure. *Id.* at \*3–4. But its decision little avails the SEC here. Cavco had internal policies “to control corporate investing (‘Investment Policy’) and prevent insider trading (‘Insider Trading Policy’)” that required the company to invest its surplus cash assets in low-risk cash equivalents. *Id.* at \*1. The company’s CEO created an end-run around the process that ordinarily required the CEO to obtain pre-approval for its investment of surplus cash from the CFO and the board of directors, and thereby invested funds in a publicly traded company without review or approval by the CFO or board. *Id.* at \*1–2. The SEC’s claim under Section 13(b)(2)(B) was that the company had “insufficient checks for how investments outside the [Investment and Insider Trading policies] would be identified and reported and for how improper investments would be prevented.” *Id.* at \*3. Unlike the allegedly deficient cybersecurity controls in this case, the internal policies and controls in *Cavco* directly related to ensuring the integrity of the company’s *financial* transactions. The decision cannot responsibly be read as supporting the SEC’s argument here that Section 13(b)(2)(B) reaches cybersecurity controls.

The SEC next argues that it needs authority to regulate cybersecurity controls under Section 13(b)(2)(B) because such adequate controls are necessary “to provide reasonable assurances that . . . access to assets is permitted only in accordance with management’s general or specific authorization.” 15 U.S.C. § 78m(b)(2)(B)(iii). It notes that deficient cybersecurity

controls can expose a company's core assets to damage or destruction, reducing their value. But that argument does not engage with the critical word that delimits the statute's reach: "a system of internal *accounting* controls." *Id.* § 78m(b)(2)(B). By its terms, Section 13(b)(2)(B) does not govern *every internal system* a public company uses to guard against unauthorized access to its assets, but only those qualifying as "internal accounting" controls. The SEC's rationale, under which the statute must be construed to broadly cover all systems public companies use to safeguard their valuable assets, would have sweeping ramifications. It could empower the agency to regulate background checks used in hiring nighttime security guards, the selection of padlocks for storage sheds, safety measures at water parks on whose reliability the asset of customer goodwill depended, and the lengths and configurations of passwords required to access company computers. That construction—and those outcomes—cannot be squared with the statutory text. *See, e.g., United States v. Dauray*, 215 F. 3d 257, 264 (2d Cir. 2000) ("A statute should be interpreted in a way that avoids absurd results."). Congress does not "hide elephants in mouseholes," *Cyan, Inc. v. Beaver Cnty. Emps. Ret. Fund*, 583 U.S. 416, 431 (2018), and the SEC does not recite any basis to conclude that Congress, in enacting Section 13(b)(2)(B), intended to confer such power upon the SEC.

The history and purpose of the statute confirm that cybersecurity controls are outside the scope of Section 13(b)(2)(B). Sections 13(b)(2)(A) and 13(b)(2)(B) were enacted as part of the 1977 Foreign Corrupt Practices Act ("FCPA"), amending the 1934 Securities Exchange Act, *In re Yesner*, 2001 WL 587989, at \*33, and together are referred to as the "accounting provisions," *Foreign Corrupt Practices Act of 1977*, Statement of Policy, 21 SEC Docket 1466, 1468 (Jan. 29, 1981). The FCPA was passed in response to "a pattern of questionable payments to foreign government officers by prominent American corporations." *Id.* The accounting provisions were

enacted “to assure books and records accurately and fairly reflected transactions and the disposition of assets, to protect the integrity of the independent audit, and to promote reliability and completeness of financial information that is disseminated to investors.” *In re Yesner, CPA*, 2001 WL 587989, at \*31. And with regard to Section 13(b)(2)(B) in particular, Congress’s explicit purpose, as codified in the text, was to “provide reasonable assurances that, among other things, transactions are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted *accounting principles* or any other applicable criteria.” S. Rep. No. 95-114 at 7 (1977) (emphasis added). Indeed, Congress recognized that because “the accounting profession has defined the objectives of a system of accounting control, the definition of the objectives contained in this subparagraph is taken from the *authoritative accounting literature*.” *Id.* (citing American Institute of Certified Public Accountants, Statement on Auditing Standards No. 1, 320.28 (1973)) (emphasis added).

To that end, these provisions require public companies, in addition to filing with the SEC annual and quarterly reports containing detailed financial information, to put in place systems to ensure that the information reported is accurate and complete. Section 13(b)(2)(A) regulates financial recordkeeping. It requires public companies to “make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of [their] assets.” And Section 13(b)(2)(B), at issue here, requires issuers to “devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances” that assets are safeguarded from unauthorized use, that corporate transactions conform to managerial authorizations, and that records are accurate. As evinced by the broader statutory scheme, the internal accounting controls identified in Section 13(b)(2)(B) thus are intended to provide extra assurance of the accuracy and completeness of the financial

information on which the issuer's annual and quarterly reports rely. To state the obvious, cybersecurity controls are not—and could not have been expected to be—part of the apparatus necessary to the production of accurate such reports.

The Court therefore dismisses the AC's internal accounting control claim against SolarWinds for failure to state a claim.<sup>51</sup>

## VI. Disclosure Controls Claims

Finally, the SEC brings a claim against SolarWinds under Exchange Act Rule 13a-15(a). That rule requires companies to “maintain disclosure controls and procedures.” 17 C.F.R. § 240.13a-15. It defines these as:

controls and other procedures of an issuer that are designed to ensure that information required to be disclosed by the issuer in the reports that it files or submits under the Act (15 U.S.C. § 78a *et seq.*) is recorded, processed, summarized and reported, within the time periods specified in the Commission's rules and forms. Disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed by an issuer in the reports that it files or submits under the Act is accumulated and communicated to the issuer's management, including its principal executive and principal financial officers, or persons performing similar functions, as appropriate to allow timely decisions regarding required disclosure.

*Id.* § 240.13a-15(e).

The SEC has explained that “to assist principal executive and financial officers in the discharge of their responsibilities in making the required certifications, as well as to discharge their responsibilities in providing accurate and complete information to security holders, it is necessary for companies to ensure that their internal communications and other procedures operate so that important information flows to the appropriate collection and disclosure points in a timely manner.” *Certification of Disclosure in Companies' Q. & Ann. Reps.*, Release No. 8124 (Aug. 28, 2002). These procedures are “intended to cover a broader range of information than is

---

<sup>51</sup> In light of this dismissal, the Court also dismisses the aiding and abetting claim against Brown.

covered by an issuer's internal controls related to financial reporting." *Id.* They "should ensure timely collection and evaluation of information potentially subject to disclosure" and "should capture information that is relevant to an assessment of the need to disclose developments and risks that pertain to the issuer's businesses." *Id.*

The AC alleges that SolarWinds had ineffective disclosure controls in place. *See* AC ¶ 327–28. It primarily bases this claim on its allegation that the company internally misclassified the USTP and PAN incidents under its Incident Response Plan ("IRP"). The company rated both incidents as a level "0," but, the SEC contends, it should have classified each as a level "2". Such a classification would have elevated the incidents to SolarWinds for disclosure evaluation by the CEO, CTO, and other top executives. *See* AC ¶¶ 328–30. The SEC also notes that, on one occasion, in June 2018, the company failed to elevate a VPN vulnerability it had identified. *Id.* ¶ 201.

For two independent reasons, these allegations do not plead a viable Rule 13a-15(a) claim.

First, as the AC itself pleads, SolarWinds had a system of controls in place to facilitate the disclosure of potentially material cybersecurity risks and incidents. As pled, the IRP was designed to ensure that material cybersecurity information was timely communicated to the executives responsible for public disclosures. The IRP scored incidents on a scale from "0" (minimal) to "3" (high), with incidents scored "2" or higher requiring notification to SolarWinds' executives, including the CEO and CTO, who were responsible for evaluating whether the circumstances necessitated public disclosure. *Id.* ¶ 273. An incident involving "a security compromise that affects multiple customers, whose impact could have an adverse effect on

SolarWinds' reputation, revenue, customer(s), partner(s) or the public" was to be scored a "2" or higher under the IRP, and elevated to SolarWinds' executives for disclosure evaluation. *Id.*

The SEC does not plead any deficiency in the construction of this system. On the contrary, as pled, the IRP as designed was capable of "ensur[ing] that information required to be disclosed . . . is recorded, processed, summarized and reported" within a reasonable time. 17 C.F.R. § 240.13a-15(e); *see SEC v. Siebel Sys., Inc.*, 384 F. Supp. 2d 694, 709 (S.D.N.Y. 2005) (disclosure controls and procedures "designed to ensure the proper and timely handling of information required to be disclosed in the reports filed or submitted under the Exchange Act, and to ensure that management has the information it needs to make timely disclosure decisions."). And the AC does not plead that the IRP frequently yielded errors. Indeed, it does not plead that the IRP had ever misclassified an incident before the USTP and PAN incidents. It merely pleads that those two incidents were wrongly classified, and from this basis alone pleads that Brown was either "unaware of the requirements in the Incident Response Plan" or "failed to recognize the applicability of the Incident Response Plan notification." AC ¶ 330. However, errors happen without systemic deficiencies. Without more, the existence of two misclassified incidents is an inadequate basis on which to plead deficient disclosure controls. *See, e.g., Siebel Systems*, 384 F. Supp. 2d at 710 ("The complaint is bereft of any particular factual allegations demonstrating that Siebel Systems did not have sufficient controls and procedures in place to enable the company to fully comply with Regulation FD."); *In re Banco Bradesco S.A. Sec. Litig.*, 277 F. Supp. 3d 600, 648 (S.D.N.Y. 2017) (finding representation that company's "internal control over financial reporting was effective" not false or misleading, and rejecting as insufficient allegations that "those controls *must* have been deficient because they may have failed to detect some weaknesses in its financial reports or disclosures"); *Barrett v. PJT Partners*

*Inc.*, No. 16 Civ. 2841 (VEC), 2017 WL 3995606, at \*6 (S.D.N.Y. Sept. 8, 2017) (“The fact that a code of conduct prohibits certain conduct by employees is not a factual representation that those policies will always be followed by all employees or that they are 100% effective.”); *Janbay v. Canadian Solar, Inc.*, No. 10 Civ. 4430 (RWS), 2012 WL 1080306, at \*8 (S.D.N.Y. Mar. 30, 2012) (“The Complaint contains no facts explaining how the revisions to the 4Q 2009 financials revealed that CSI’s internal controls were not effective during any earlier period of time.”); *but see In re Barclays PLC Sec. Litig.*, No. 22 Civ. 8172 (KPF), 2024 WL 757385, at \*11 (S.D.N.Y. Feb. 23, 2024) (finding actionable and misleading statement that “[a] framework of disclosure controls and procedures is in place to support the approval of the financial statements of [defendant],” when defendant “failed to implement, much less bother to design, any internal controls whatsoever to track and monitor the issuance of securities.”).

Second, the AC’s claim that the USTP and PAN incidents were mischaracterized within the IRP framework is inadequately pled. The AC pleads that the incidents merited a “2” score on the ground that each involved a security “compromise for which other customers are susceptible.” AC ¶ 273 (under IRP, an incident that “affects multiple customers” must be rated a 2).<sup>52</sup> The AC’s claim thus turns on the factual contention that the two incidents were related. But, as reviewed above, SolarWinds investigated both incidents promptly after they were reported and had not so found. It pleads that, on the information available to it, the company had *not* uncovered the root cause of the malicious activity or definitively determined that the two incidents were related. *Id.* ¶¶ 270, 284. The AC does not plead that prior to SUNBURST the

---

<sup>52</sup> In full, a level “2” classification entails an incident that: “[a]ffects multiple [SolarWinds] customers, involves [SolarWinds’] accounts with elevated privileges, involves a compromise to personal data [] or data that should be protected from general access, and/or whose impact could have an adverse effect on SolarWinds’ reputation, revenue, customer, partner or the public.” Turner Decl., Ex. 17 at 3.

company had determined it had been the victim of an incident affecting multiple customers. Whether the facts pled might plausibly claim that the relevant personnel made an erroneous factual determination by the relevant personnel, *cf. id.* ¶ 271 (noting speculation among employees that the incidents might be related), seeing that the company had not found the two incidents to be related, the AC cannot plausibly claim a misapplication of the IRP standards. *See, e.g., Barrett*, 2017 WL 3995606, at \*6 (“Plaintiff appears to be proceeding on the premise that because Caspersen did bad things while employed by PJT, its statements regarding the existence of its internal controls that are designed and intended to prevent fraud are per se false.”).

That leaves the AC’s allegation that Brown’s failed to elevate the VPN vulnerability in June 2018. As pled, Engineer D raised the issue to the director of IT and to senior infosec Manager E through an internal presentation, and they later elevated it to Brown. AC ¶¶ 206, 209. SolarWinds argues that Brown should have elevated the issue to the CEO and CTO for public disclosure, and that his failure to do so bespeaks a failure of the company’s disclosure control apparatus. That claim has traction only with the benefit of post-SUNBURST hindsight. As pled, in real time, Engineer D “receiv[ed] pushback to his initial recommendation” regarding the VPN security gap, *id.* ¶ 204, reflecting that the VPN issue was at a minimum a subject of internal debate. That this one lapse was not elevated to the company’s top rung does not, without more, plausibly impugn the company’s disclosure controls systems. *See Podany v. Robertson Stephens, Inc.*, 318 F. Supp. 2d 146, 155 (S.D.N.Y. 2004) (“second-guessing by hindsight” a company’s decisions in securities fraud claim disfavored).

The Court accordingly dismisses the disclosure controls claims for failure to state a claim.<sup>53</sup>

### CONCLUSION

For the foregoing reasons, the Court grants in part and denies in part defendants' motion to dismiss. The Clerk of Court is respectfully requested to terminate the motions pending at Dockets 44 and 88.

Pursuant to Federal Rule of Civil Procedure 12(a)(4)(A), SolarWinds' answer to the Amended Complaint is due 14 days from today.

SO ORDERED.

  
\_\_\_\_\_  
PAUL A. ENGELMAYER  
United States District Judge

Dated: July 18, 2024  
New York, New York

---

<sup>53</sup> In light of this dismissal, the Court also dismisses the related aiding and abetting claim against Brown.