CHRISTOPHER BRUCKMANN
(SDNY Bar No. CB-7317)
Attorney for Plaintiff
SECURITIES AND EXCHANGE COMMISSION
100 F Street, N.E.
Washington, D.C. 20549
(202) 551-5986
BruckmannC@sec.gov

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	Civil Action No. 23-cv-9518 Jury Trial Demanded

COMPLAINT

Plaintiff Securities and Exchange Commission ("SEC"), for its Complaint against Defendants SolarWinds Corp. ("SolarWinds" or "the Company") and Timothy G. Brown ("Brown") (collectively, "Defendants"), alleges as follows:

SUMMARY

1. From at least October 2018 through at least January 12, 2021 (the "Relevant Period"), Defendants SolarWinds and its then-Vice President of Security and Architecture, Brown, defrauded SolarWinds' investors and customers through misstatements, omissions, and schemes that concealed both the Company's poor cybersecurity practices and its heightened—and increasing—cybersecurity risks. SolarWinds' public statements about its cybersecurity practices and risks painted a starkly different picture from internal discussions and assessments

about the Company's cybersecurity policy violations, vulnerabilities, and cyberattacks. Illustratively, in October 2018, the same month that SolarWinds conducted its Initial Public Offering through a registration statement with only generic and hypothetical cybersecurity risk disclosures, Brown wrote in an internal presentation that SolarWinds' "***current state of security leaves us in a very vulnerable state for our critical assets***."[1]

2. The true state of SolarWinds' cybersecurity practices, controls, and risks ultimately came to light only following a massive cyberattack—***which exploited some of SolarWinds' poor cybersecurity practices***—and which impacted thousands of SolarWinds' customers. That attack, termed SUNBURST, compromised SolarWinds' Orion software platform, a flagship product that the Company considered to be a "crown jewel" asset and which accounted for 45% of its revenue in 2020.

3. SolarWinds, a publicly traded company, provides software that thousands of companies and many government agencies use to manage their information technology infrastructure by, for example, monitoring activity on networked servers.

4. SolarWinds and/or Brown made materially false and misleading statements and omissions related to SolarWinds' cybersecurity risks and practices in at least three types of public disclosures:

a) Statements that purported to describe the Company's cybersecurity practices and policies, including a "Security Statement" posted to the Company's website throughout the Relevant Period;

b) Form S-1 and S-8 Registration Statements and periodic reports filed with the SEC throughout the Relevant Period; and

[1] All emphasis in quotations in this Complaint is added unless otherwise noted.

c) A Form 8-K filed with the SEC on December 14, 2020 regarding the massive SUNBURST cybersecurity incident that impacted SolarWinds' Orion software platform.

5. The Security Statement was materially misleading because it touted the Company's supposedly strong cybersecurity practices. For example, that statement asserted that SolarWinds created its software products in a "secure development lifecycle [that] follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments." And the Security Statement claimed that SolarWinds' "password policy covers all applicable information systems, applications, and databases [and we] enforce the use of complex passwords." It also stated that SolarWinds had "[a]ccess controls to sensitive data in our databases, systems, and environments [that are] set on a need-to know / least privilege necessary basis." All those statements were materially false and misleading.

6. The misleading Security Statement concealed from the public the Company's known poor cybersecurity practices throughout the Relevant Period. These poor cybersecurity practices included SolarWinds' (a) failure to consistently maintain a secure development lifecycle for software it developed and provided to thousands of customers, (b) failure to enforce the use of strong passwords on all systems, and (c) failure to remedy access control problems that persisted for years.

7. SolarWinds' SEC filings similarly concealed the Company's poor cybersecurity practices. They contained general, high-level risk disclosures that lumped cyberattacks in a list of risks alongside "natural disasters, fire, power loss, telecommunication failures…[and] employee theft or misuse." The cybersecurity risk disclosure was generic and hypothetical, allowing for negative consequences "[i]f we sustain system failures, cyberattacks against our systems or

against our products, or other data security incidents or breaches." This disclosure failed to address known risks. For example, it warned of an inability to defend against "unanticipate[d]… techniques" but failed to disclose that SolarWinds had already determined that it was not taking adequate steps to protect against anticipated and known risks, including failing to follow the steps outlined in the Security Statement. These general warnings were then repeated verbatim in each relevant filing, despite both the ongoing problems and the increasing red flags in 2020 that SolarWinds was not only being specifically targeted for a cyberattack, but that the attackers had already gotten in.

8. In and around the same time that SolarWinds was making these materially misleading public statements, Brown and other SolarWinds employees knew that SolarWinds had serious cybersecurity deficiencies. Internal emails, messages, and documents describe numerous known material cybersecurity risks, control issues, and vulnerabilities. These internal statements dramatically contradict SolarWinds' public disclosures relating to its cybersecurity practices, risks, controls, and vulnerabilities. Among these internal statements are Brown's assessment that the Company's critical assets were "very vulnerable," and examples such as:

a. A January 2018 email to senior managers bluntly admitted that the Security Statement's Secure Development Lifecycle ("SDL") section was false, and described a "simple" scheme by which, rather than amend the Security Statement to make it accurate, SolarWinds would conceal the present falsity of the representations and work toward making them true eventually: "I've gotten feedback that ***we don't do*** some of the things that are indicated in the [Security Statement's 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."

b. In June 2018, SolarWinds Network Engineer D[2] identified a "security gap" relating to SolarWinds' remote access virtual private network, which allowed access from devices not managed by SolarWinds. Network Engineer D warned that this setup was "***not very secure***" and later explained that someone exploiting the vulnerability "can basically do whatever without us detecting it until it's too late" which could lead to a "***major reputation and financial loss***" for SolarWinds.

c. An August 2019 presentation warned that "[***a***]***ccess and privilege to critical systems / data is inappropriate.***"

d. Presentations in March and October 2020 highlighted "[***s***]***ignificant deficiencies***" in SolarWinds' access controls.

e. In 2020, portions of SolarWinds' flagship Orion software platform were still not developed under an SDL process, and SolarWinds employees noted this was a problem. In June 2020 an employee asked: "Do we have SDL process enforced for Orion Improvement Program ["OIP"] 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." As the employee surmised, the OIP was not in fact covered by the SDL as of June 2020.

f. In a July 2020 presentation, Brown warned about threat actors' familiarity with a critical SolarWinds software platform, noting that the threat actors "***[k]now how to deploy software, shut off backup, etc.***"

[2] Persons and entities not charged in this Complaint, but referred to repeatedly, are identified by pseudonyms.

g. In a July 2020 email to Brown, a member of the Engineering team described being "spooked" by activity at a SolarWinds' customer. Brown agreed that the incident was "***very concerning***" and continued, "As you guys know ***our backends are not that resilient*** and we should definitely make them better."

h. A September 2020 Risk Acceptance Form flagged for Brown and others "the risk of legacy issues in the Orion Platform" and warned "[t]he volume of security issues being identified over the last month have ***outstripped the capacity*** of Engineering teams to resolve."

i. In instant messages sent in November 2020, SolarWinds' Senior InfoSec Manager E expressed his own disgust with the Company's security posture, lamenting, "[***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."

j. In November 2020, a SolarWinds Information Security employee sent an instant message to Senior InfoSec Manager E with a link to a list of vulnerabilities in the Orion platform stating, "***The products are riddled and obviously have been for many years***." That same month, a SolarWinds' network engineer complained, "We filed more vulnerabilities then [sic] 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.*** Not good."

9. Even though Brown and/or other SolarWinds employees and executives knew about these risks, vulnerabilities, and attacks against SolarWinds' products, SolarWinds' cybersecurity

risk disclosures did not disclose them in any way, either individually or by disclosing the increased risk they collectively posed to SolarWinds.

10. To be clear, SolarWinds' poor controls, Defendants' false and misleading statements and omissions, and the other misconduct described in this Complaint, would have violated the federal securities laws even if SolarWinds had not experienced a major, targeted cybersecurity attack. But those violations became painfully clear when SolarWinds experienced precisely such an attack.

11. Between January 2019 and December 2020, SolarWinds experienced one of the worst cybersecurity incidents in history, the SUNBURST "'supply chain' cyberattack," which exploited some of the cybersecurity failings described above and compromised SolarWinds' "crown jewel" Orion product.

12. As early as June 2018, SolarWinds had a known vulnerability that allowed access to the Company's virtual private network ("VPN") through unmanaged devices such as cell phones and laptops that were neither owned nor operated by the Company. In January 2019, threat actors accessed SolarWinds' systems through the VPN using an unmanaged device. The actors then had broad, undetected access to SolarWinds' systems. (It is possible that the threat actors first accessed SolarWinds' systems at an earlier time and through other means, but the earliest confirmed access was through the VPN vulnerability.)

13. Using their access, the threat actors inserted malicious code into three software builds for SolarWinds' Orion products. SolarWinds then delivered these compromised products to more than 18,000 customers across the globe. The malicious code provided the threat actors with the ability to access the systems of these compromised customers, provided certain other conditions were met, and became known as the SUNBURST attack.

14. During 2020, Brown learned about increasing cybersecurity attacks against, and vulnerabilities involving, Orion and other SolarWinds' products. This included cybersecurity attacks against two customers who were using the Orion product, U.S. Government Agency A in May 2020 and Cybersecurity Firm B in October 2020.

15. Shortly after the October 2020 attack against Cybersecurity Firm B, SolarWinds employees including Brown recognized similarities between that attack and the attack on U.S. Government Agency A. But when personnel at Cybersecurity Firm B asked SolarWinds employees if they had previously seen similar activity, InfoSec Employee F falsely told Cybersecurity Firm B that they had not. He then messaged a colleague, "[***W***]***ell I just lied***."

16. In early December 2020, a third customer, Cybersecurity Firm C, discovered that it too had become the victim of a cyberattack through SolarWinds' Orion platform. Cybersecurity Firm C quickly identified the malicious code in SolarWinds' Orion product. On December 12, 2020, Cybersecurity Firm C notified SolarWinds' CEO of the malicious code and shared the relevant code with Brown in a manner that made the malicious code apparent to cybersecurity professionals. Brown immediately recognized that the malicious code identified by Cybersecurity Firm C was the same vulnerability in the Orion platform that had been previously exploited against U.S. Government Agency A and Cybersecurity Firm B.

17. On December 14, 2020, SolarWinds filed a Form 8-K with the SEC disclosing that its Orion network monitoring software contained malicious code that had been inserted by threat actors as part of a supply-chain attack. The Form 8-K was drafted by a group of executives, including Brown, and signed by SolarWinds' CEO. That Form 8-K was materially misleading in several respects, including its failure to disclose that the vulnerability at issue had been actively

exploited against SolarWinds' customers multiple times over at least a six-month period in the incidents involving U.S. Government Agency A, Cybersecurity Firm B, and Cybersecurity Firm C.

18. On December 14, 2020, the day it filed the Form 8-K first announcing the SUNBURST attack against the Orion platform, SolarWinds' stock price dropped more than 16%. It dropped at least an additional 8% the next day. The stock price continued to drop and lost approximately 35% of its value by the end of the month as SolarWinds disclosed more details of the SUNBURST attack, and as news outlets reported that internal sources had warned SolarWinds for several years about the Company's cybersecurity risks and vulnerabilities.

DEFENDANTS

19. **SolarWinds** is a Delaware corporation with its headquarters in Austin, Texas. Founded in 1999, SolarWinds conducted its first initial public offering ("IPO") in 2009 and remained a public company until February 2016, when it was acquired by several private equity firms in a take-private transaction. The Company conducted a second IPO in October 2018 and remains a public company.

20. **Timothy G. Brown**, age 59, is a resident of Salado, Texas. Brown was responsible for the overall security program at SolarWinds throughout the Relevant Period. Between July 2017 and December 2020, Brown was an officer of SolarWinds, serving as its Vice President of Security and Architecture, and head of the Information Security group at SolarWinds (referred to at SolarWinds and in this Complaint as "InfoSec"). Since January 2021, he has been SolarWinds' Chief Information Security Officer. In his role as Vice President of Security and Architecture, Brown was responsible for the Company's ongoing security efforts, as well as security architecture within its products. Brown also signed sub-certifications attesting to the adequacy of

SolarWinds' cybersecurity internal controls, which SolarWinds' executives relied on in connection with SolarWinds' periodic reports that were filed with the SEC.

OTHER RELEVANT PERSONS AND ENTITIES

21. U.S. Government Agency A is a federal agency that was a SolarWinds customer during the Relevant Period.

22. Cybersecurity Firm B is a cybersecurity firm that was a SolarWinds customer during the Relevant Period.

23. Cybersecurity Firm C is a cybersecurity firm that was a SolarWinds customer during the Relevant Period.

24. Network Engineer D is a former SolarWinds employee.

25. Senior InfoSec Manager E is a SolarWinds employee who, at all relevant times, reported directly to Brown.

26. InfoSec Employee F is a SolarWinds employee who, at all relevant times, reported directly to Senior InfoSec Manager E and indirectly to Brown.

27. Customer G is a multinational information technology company.

28. Engineering Manager H is a SolarWinds employee who, during the Relevant Period, reported to the Company's Chief Technology Officer.

29. SolarWinds Chief Executive Officer, Chief Financial Officer, Chief Technology Officer, and Chief Information Officer at the relevant times are referred to as the "CEO," "CFO," "CTO," and "CIO," respectively.

JURISDICTION AND VENUE

30. The SEC brings this action, and this Court has subject matter jurisdiction over this action, pursuant to Sections 20 and 22 of the Securities Act [15 U.S.C. §§ 77t and 77v], Sections 21 and 27 of the Exchange Act [15 U.S.C. §§ 78u and 78aa], and 28 U.S.C. § 1331.

31. Defendants SolarWinds and Brown, directly or indirectly, singly or in concert with others, made use of the means or instruments of transportation and communication in interstate commerce, or of the mails, or of the facilities of a national securities exchange in connection with the acts, transactions, and practices alleged in this Complaint.

32. Throughout the Relevant Period, SolarWinds was engaged in the offer and/or sale of securities. This included its October 2018 IPO, which was registered with the SEC through a Form S-1 registration statement that became effective on October 18, 2018 and an additional public offering of shares through a Form S-1 registration statement filed on May 20, 2019. The Company also registered additional offerings in April 2019, December 2019, and February 2020 on Forms S-8 for shares offered pursuant to the Company's Employee Stock Purchase Plan ("ESPP"). Multiple employees, including employees not participating in the fraud, purchased stock through the ESPP throughout 2019 and 2020, and the company received money from those purchases. Each Form S-8 incorporated by reference the Company's most recent annual report on Form 10-K, as well as all periodic reports filed between the date of the most recent annual report and the Form S-8.

33. During the Relevant Period, Brown was engaged in the offer and/or sale of securities and received money or property by selling SolarWinds stock at prices inflated, at least in part, by the misconduct described in this Complaint. Specifically, Brown exercised options and sold SolarWinds stock during 2020, receiving more than $170,000 in gross proceeds when

SolarWinds' stock price was inflated by the misstatements, omissions, and schemes discussed in this Complaint. This included the sales listed in the chart below, each of which was processed through the New York Stock Exchange:

Sale Date	**Shares Sold**	**Price**	**Gross Proceeds**
2/10/2020	1500	$18.92	$28.384.24
2/27/2020	1000	$17.65	$17,646.10
5/6/2020	1000	$17.22	$17,220.00
5/22/2020	500	$17.95	$8,973.80
8/13/2020	2500	$19.54	$48,849.00
8/18/2020	1500	$19.90	$29,842.71
8/31/2020	1000	$21.21	$21,205.00
Total	**9000**		**$172,120.85**

34. Venue lies in this District pursuant to Securities Act Section 22(a) [15 U.S.C. § 77v(a)] and Exchange Act Section 27(a) [15 U.S.C. § 78aa] because, among other things, some of the acts, practices, transactions, and courses of business alleged in this Complaint occurred within the Southern District of New York and were effected, directly or indirectly, by making use of means or instrumentalities of transportation or communication in interstate commerce, or the mails, or the facilities of a national securities exchange. For example, beginning with the Company's October 2018 IPO, and continuing through the present, the Company's stock was publicly traded using the ticker symbol "SWI" on the New York Stock Exchange, located in this District. The four lead investment firms that managed the Company's IPO are all either based in this District or maintain large offices in this District. An October 18, 2018 press release by SolarWinds directed persons interested in obtaining a copy of the prospectus for its IPO to contact one of those four firms and provided contact addresses. Three of those addresses were in this District, and the fourth was in the Eastern District of New York. In addition, individuals

residing in the Southern District of New York purchased and sold SolarWinds stock during the Relevant Period.

35. Additionally, throughout the Relevant Period, two private investment companies collectively owned more than 70% of SolarWinds' common stock. Each of those companies has business locations in this District.

FACTS

A. SolarWinds Designs and Sells Software That Other Companies and Government Agencies Use to Manage Their Computer Networks.

36. SolarWinds designs and sells network monitoring software used by many businesses, as well as state, federal, and foreign governments to manage their computer systems. Among other things, SolarWinds' products provide information technology professionals with visibility into network utilization and equip information technology departments to detect, diagnose, and resolve network performance issues. SolarWinds also sells its own cybersecurity products. During the Relevant Period, SolarWinds had more than 300,000 customers, including 499 of the companies making up the Fortune 500.

37. Orion is an information technology infrastructure and management platform consisting of a suite of products used by customers to manage network system configurations. Orion was SolarWinds' flagship product during the Relevant Period and accounted for 45% of the Company's revenue in 2020. Internally, SolarWinds considered Orion to be one of its "crown jewels," a term used to describe assets that, if compromised, could have a material impact on the Company.

B. SolarWinds and Brown Falsely Promoted SolarWinds' Cybersecurity Practices in Public Statements.

38. Throughout the Relevant Period, SolarWinds and Brown made false public statements touting the quality of the Company's cybersecurity practices.

39. Before the Company's IPO, SolarWinds posted a "Security Statement" on its public website. That Security Statement purported to describe the Company's cybersecurity practices. Brown was primarily responsible for creating and approving the Security Statement before it was posted. In multiple Company documents, Brown was identified as the "owner" or "approver" of the Security Statement. The "Trust Center" section of SolarWinds' website, which contained the Security Statement, prominently featured a picture of Brown, who was head of the relevant InfoSec group. Also, 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 which were posted on a SolarWinds' website.

40. The Security Statement purportedly informed the public of SolarWinds' cybersecurity practices. Similarly, SolarWinds' website assured the public that the Company "is committed to taking our customers [sic] security and privacy concerns seriously and makes it a priority," and that the Company's "security strategy covers all aspects of our business."

41. By its terms, the Security Statement applied to SolarWinds' "information system assets," which consisted of "customer and end-user assets as well as corporate assets." The Security Statement specifically incorporated "the procedures and guidelines defined by SolarWinds[']s security policies" and stated that personnel who handled information system assets had to comply with those policies, guidelines, and procedures.

42. Brown and the Company understood that SolarWinds' adherence to sound cybersecurity practices was material to SolarWinds' ability to obtain and retain business. The Company used the Security Statement to respond to inquiries from the public and customers about SolarWinds' cybersecurity practices. SolarWinds' employees, with Brown's knowledge,

regularly disseminated the Security Statement, sending customers hyperlinks in emails or other documents that linked directly to the Security Statement on SolarWinds' website and explicitly advising that the Security Statement detailed how SolarWinds was mitigating the risk of cyberattacks.

43. Securities analysts who followed SolarWinds considered the opinions of customers regarding SolarWinds products in conducting their evaluations and assessments of whether to recommend buying or selling SolarWinds stock.

44. SolarWinds' Security Statement remained virtually unchanged throughout the Relevant Period and covered areas including secure development lifecycle, password protection, and access controls, among others.

45. SolarWinds' Security Statement contained multiple materially false and misleading statements, assuring the public that SolarWinds followed well-recognized cybersecurity practices when, in reality, the Company's cybersecurity practices fell significantly short of those standards. The Security Statement also omitted information necessary to make the information included, in light of the circumstances, not misleading. The false statements and omissions in the Security Statement fall into four general categories: (1) compliance with the NIST Framework for evaluating cybersecurity practices; (2) using a secure development lifecycle when creating software for customers; (3) having strong password protection; and (4) maintaining good access controls.

46. Together, the individual failures, risks, issues, and incidents described in this Complaint so affected SolarWinds' cybersecurity posture that SolarWinds needed to, at a minimum, disclose their collective effect, especially in light of the Security Statement's positive portrayal of SolarWinds' cybersecurity practices.

1. SolarWinds and Brown Misleadingly Claimed to Follow the NIST Framework for Evaluating Cybersecurity Practices.

47. In the Security Statement, SolarWinds and Brown claimed that the Company followed the widely used and internationally recognized National Institute of Standards and Technology Cybersecurity Framework ("NIST Framework"), claiming, "SolarWinds follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect and respond to security incidents."

48. The NIST Framework includes "a set of cybersecurity activities, outcomes and informative references that are common across sectors and critical infrastructure" and is designed to "help an organization align and prioritize cybersecurity activities with its business/mission requirements, risk tolerances and resources." SolarWinds assessed its cybersecurity controls using the moderate level framework NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations (NIST 800-53). As part of its assessment, SolarWinds evaluated more than 300 controls in areas including "access controls," "identification and authentication," and "incident response." The Company measured its compliance with the NIST framework and maturity levels using a scale ranging from a low of zero ("no evidence") to a high of five ("refined practice, focused on improvements and efficiencies"), with associated language describing each level of compliance.

a) In Truth, SolarWinds Had No Policy or Practice in Place for Most of the NIST Framework.

49. Despite the claim in its Security Statement that it followed the NIST Framework, in multiple internal assessments between 2019 and 2021, SolarWinds met only a small fraction of the cybersecurity controls laid out in the NIST Framework and had "no program/practice in place" for the ***majority*** of the controls, as Brown and SolarWinds knew, or were reckless or negligent in not knowing.

50. For example, in a September 2019 assessment shared with Brown and SolarWinds' CIO, SolarWinds identified having a "program/practice in place" for only 21 of the 325—or 6%—of NIST 800-53 controls, and "No program/practice in place" for 198 of the 325—or 61%—of the controls. The remaining 106 controls fell into the category of "Program/Practice *may* be in place but requires detailed review."

51. A subsequent assessment in January 2021 that was sent to Brown identified similar deficiencies, noting that only 40% of the NIST 800-53 controls were "met or partially met[,]" leaving 60% ***completely unmet***.

52. The Security Statement was materially false and misleading. It contained positive information about the state of the Company's cybersecurity practices while failing to include information such as the fact that SolarWinds failed to meet more than half of NIST standards, or how poorly it scored on the NIST five-point scale for certain critical areas.

53. As detailed below, when evaluating its internal cybersecurity practices, SolarWinds consistently identified three critical areas that were particularly deficient: (1) secure development lifecycle; (2) password protocols; and (3) access controls.

b) SolarWinds and Brown's Misstatements and Omissions About Cybersecurity Practices, Including the NIST Framework, Were Material.

54. Reasonable investors considering whether to purchase or sell SolarWinds stock would have considered it important to know the true state of SolarWinds' cybersecurity practices because, among other reasons, poor cybersecurity practices could negatively impact sales and revenue, and, therefore, stock valuations. Cybersecurity practices are important to every publicly traded company. But they are especially important for a company like SolarWinds whose primary product is not only software, but software that other organizations install to manage their

own computer networks. As a result, cybersecurity disclosures are particularly material for SolarWinds.

55. Securities analysts generally consider it important for companies to accurately disclose their risks. And for a company like SolarWinds that sold cybersecurity products, analysts consider it particularly important to accurately describe their cybersecurity risks and practices.

56. Brown himself stressed in a September 2020 blog post how important it was for companies to publicly issue—and follow—cybersecurity protocols:

> Over the past few years, security experts have increasingly emphasized the risks inherent in the software supply chain. Businesses rely on cloud applications that add complexity into an environment. The application itself could have bugs that leave an opening. Code libraries used by developers to simplify engineering could have flaws. The software could integrate with another application that may be insecure. In short, businesses do take on some additional risk in such an interconnected business environment. That's why it's important your software vendors take their roles as business partners seriously. Their security is your security. When looking for a vendor selling tools for your MSP—whether it's security tools, network management, or backup—it's important to not only match feature lists, but also kick the tires on their security. No software is perfect or vulnerability-free forever. But strong vendors put processes and protocols in place to reduce the risk and deal with threats if they crop up. And most importantly, strong vendors publish their security protocols and processes so you can evaluate whether they meet your standards. (If they don't, it's worth giving it a second thought on whether to trust them with your business and your data).

57. Claiming to "follow" the NIST framework, without disclosing just how poorly the Company was doing in following the framework, was misleading and deprived investors of material information necessary to make the claim that SolarWinds followed the framework not misleading. A reasonable investor would have wanted to know that the true state of SolarWinds' cybersecurity practices left it far more vulnerable to a cyberattack than Solar Winds' public statements conveyed and that its cybersecurity practices could cause significant financial and reputational damage.

2. SolarWinds and Brown Falsely Claimed That the Company Followed a Secure Development Lifecycle When Creating Software for Customers.

58. In the publicly available Security Statement, SolarWinds and Brown claimed that the Company followed a "Secure Development Lifecycle" or "SDL." An SDL is a software production methodology that standardizes industry best practices with the goal of creating secure software products. In the Security Statement, SolarWinds and Brown stated:

> We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products. Our products are deployed on an iterative, rapid release development lifecycle. Security and security testing are implemented throughout the entire software development methodology. Quality Assurance is involved at each phase of the lifecycle and security best practices are a mandated aspect of all development activities.
>
> Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments. The SolarWinds architecture teams review our development methodology regularly to incorporate evolving security awareness, industry practices and to measure its effectiveness.

59. Similarly, the public "Trust Center" of SolarWinds' website stated, "Secure Development Lifecycle. We follow a defined methodology to develop software designed to increase the resiliency and security of our products."

60. As discussed below, these statements were materially false and misleading.

a) In Truth, SolarWinds Did Not Always Develop Software in a Secure Development Lifecycle.

61. SolarWinds failed to follow an SDL throughout the Relevant Period, including for components of the Company's "crown jewel" Orion platform that were ultimately used in the SUNBURST attack. Instead, SolarWinds and Brown knew, or were reckless or negligent in not knowing, that the Company was still working to determine how to incorporate aspects of an SDL into its product development leading up to and throughout the Relevant Period.

62. For example, in a January 2018 email to multiple senior managers, including SolarWinds' CIO, Engineering Manager H bluntly admitted that the Security Statement's SDL section was false. Rather than suggest amending the Security Statement to make it accurate, Engineering Manager H explained that SolarWinds would continue to hide the falsity of these statements and work toward making them eventually true: "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." The email continued to describe a plan that "begins with general SDL training" and described deploying SDL "pilots" and working to "roll out the SDL to additional teams each quarter." A plan to begin taking steps to implement an SDL is a far cry from presently employing an SDL as represented to the public in the Security Statement.

63. Additionally, Engineering Manager H's statement to multiple senior managers that SolarWinds would cover-up the false Security Statement by attempting to start doing what it publicly claimed it had already done does not reflect a culture of honesty or effective controls regarding disclosure, cybersecurity, or other matters. Rather it reflects a culture of recklessness, negligence, and scienter at SolarWinds. It is also evidence of a scheme to conceal the true state of SolarWinds' cybersecurity practices from both its investors and customers.

64. The SDL problems and scheme to conceal them continued into and throughout the Relevant Period. In a May 2018 email to Brown and SolarWinds' CIO, Engineering Manager H wrote, "[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."

65. An August 16, 2019 Security and Compliance Program Quarterly Overview presentation listed "Secure Software Development Lifecycle" with an objective of "Employees are aware of [and] utilize a security software development lifecycle in their day to day activities" as only having a score of 2 on the NIST Five-Point scale, meaning it was an area where SolarWinds "does not routinely measure or enforce policy compliance." Brown was responsible for the cybersecurity content in the Security and Compliance Program Quarterly Overview presentations during the Relevant Period.

66. In June 2020, in connection with the U.S. Government Agency A incident (detailed below), a SolarWinds' engineer questioned by email whether the Orion Improvement Program ("OIP"), a component of the Orion platform, was developed under an SDL process. "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." Another engineer responded, "I don't believe we cover OIP today with the SDL, but we should." The email was forwarded to SolarWinds' CIO and Brown.

67. Brown confirmed in sworn testimony that the OIP was not built under an SDL process in 2020, and emails show he was aware of this fact at the time.

68. SolarWinds' internal policy pertaining to SDL required that products like OIP which store, process, or manage data must be scanned for vulnerabilities and security tested prior to their release. And the Security Statement represented that SolarWinds conducted security testing prior to releasing products. But a July 2020 internal presentation prepared by Brown and reviewed by SolarWinds' CIO and SolarWinds' CTO noted, "Inconsistent internal security testing as part of product final security reviews don't always include web application testing before release."

69. The Security Statement remained false and misleading throughout the Relevant Period. It was never updated during the Relevant Period to reflect any of these SDL issues or failures, nor did SolarWinds or Brown otherwise publicly disclose these issues or failures.

b) SolarWinds and Brown's Misstatements and Omissions Regarding a Secure Development Lifecycle Were Material.

70. The Company's public Security Statement regarding its SDL during the Relevant Period was not only false and misleading, but materially so. A reasonable investor, considering whether to purchase or sell SolarWinds stock, would have considered it important to know the true state of SolarWinds' security regarding product development, especially regarding the development of portions of a "crown jewel" product like Orion. But the Security Statement's misrepresentations about developing products using SDL deprived investors of that material information.

71. Also, in a September 2019 interview, Brown stressed the importance of a company protecting its "crown jewels" from a cybersecurity attack, and described failing to do so as an "extinction event":

> Enterprises, it is a choice. It is a risk choice that they have made to say 'Here is my budget. Here is what I'm going to spend on security. Hopefully, I've done a good job. Here are my crown jewels. I understand what would be an extinction event for me and I'm protecting against those.'
>
> * * *
>
> My broad-based mission is to basically eliminate anything that is material damage to my company. I know I can't eliminate everything. So, that's the first rule. So what do I eliminate that would be materially damaging to my company?

72. As discussed above, Orion was not the only software platform for which there were SDL failures, and Brown admitted the importance of companies following an SDL and maintaining a secure environment for all software products they develop in a September 2020 blog post:

> … try to inquire about how organizations develop their code. For example, some organizations implement the Secure Development Lifecycle [SDL], a framework standardized by US-CERT. Following these practices increases the likelihood of producing secure products. The [SDL] includes several components and practices for understanding security requirements, developing code securely, testing before code deployment, and incident response for issues that occur. (If you're curious and want to take a deep dive into the [SDL], visit US-CERT.) The most important takeaway here, however, is that organizations should have a strong, mature model for developing secure products and maintaining their own security.

3. SolarWinds and Brown Falsely Claimed that SolarWinds Implemented a Strong Password Policy.

73. SolarWinds' Security Statement falsely claimed the Company not only had, but enforced, a strong password policy. Specifically, SolarWinds and Brown stated:

> 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.

74. SolarWinds' password policy, which was incorporated by reference in the Security Statement, 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: upper case letter, lowercase letter, base-10 digit (0-9), and non-alphanumeric character.

75. Solar Winds' Security Statement also stated that "Passwords are individually salted and hashed." The phrase "individually salted and hashed" meant that the passwords were maintained in an encrypted state.

76. As discussed below, these statements were materially false and misleading.

a) In Truth, SolarWinds Failed to Enforce or Comply With Its Own Password Policy on Multiple Occasions.

77. Contrary to its Security Statement, SolarWinds did not enforce strong password requirements on all of its information systems, applications, and databases, as Brown and SolarWinds knew or were reckless or negligent in not knowing. Indeed, multiple instances of

password problems were flagged for company management, but the password problems persisted for years, as shown in numerous internal documents, including those discussed below.

78. In an April 2017 email to the newly hired CIO, a SolarWinds employee expressed surprise that things "like 'default passwords' are [still] plaguing us when the product has been in the market [this long,]" explaining, "[m]any of these vulnerabilities seem pretty well amateur hour." As an example, the employee noted one product for which the default password was "password." Senior InfoSec Manager E testified that having a default password of "password" is a "poor security practice."

79. An April 2018 audit shared with SolarWinds' CIO identified multiple critical systems that did not comply with the password policy. The audit found systems where "shared SQL legacy account login credentials [were] used," contrary to the Security Statement's claim that SolarWinds "require[s] that authorized users be provisioned with unique account IDs."

80. That same April 2018 audit also found database passwords that were "not encrypted within the configuration file," login credentials that were "stored in plain text in configuration files," and passwords that were "stored in plain text on the public web server in the web configuration file and in the system registry of the machine." In other words, the passwords were not individually stored in an encrypted state or "salted as hashed," as SolarWinds and Brown represented in the Security Statement. Sarbanes-Oxley ("SOX") audits in 2019 and 2020 documented additional instances in which "[p]assword requirements" and "password history" requirements were not met.

81. Passwords for other systems at the Company likewise fell well short of its stated password policy. A September 2019 email from the same compliance employee to SolarWinds' CIO described security risks for SolarWinds' network authentication system, including,

"Passwords have no specific parameters, as stated in the IT guidelines;" and "Passwords are able to be reused and are not changed at a set number of days."

82. A September 2019 email attached an internal FedRAMP security controls assessment conducted by a SolarWinds compliance employee against the 300-plus controls in the NIST Framework discussed above. The controls were broken down into sub-categories and assessed as either having "Program/Practice in place," "Program / Practice may be in place but requires detailed review," or "No program / practice in place." For the subcategory "Identification and Authentication" zero controls were rated "in place," seven were rated as "may be in place" and twenty controls had "No program/practice in place."

83. During the Relevant Period, SolarWinds used an Akamai server to distribute software updates to its customers. In November 2019, an outside security researcher notified SolarWinds that the password for the Company's Akamai server was publicly available, and that a threat actor could use that public password to infect SolarWinds' software updates: "I have found a public Github repo which is leaking ftp credential belong[ing] to SolarWinds…. Via this any hacker could upload malicious exe [executable code] and update it with release [of] SolarWinds product." Senior InfoSec Manager E confirmed the security researcher's description. The password that was publicly available was "solarwinds123," an astonishingly simple password that did not comply with the Company's stated password complexity requirements.

84. SolarWinds used Quarterly Risk Review presentations that were compiled by Brown and others in the Company's Information Technology group to highlight the current information technology status and risks. They were routinely shared with the CIO, CTO, and other senior executives. A March 2020 email and Quarterly Risk Review presentation that was drafted with input from Brown and shared with SolarWinds' CIO and CTO (who then updated

SolarWinds' CEO), described findings from SolarWinds' SOX audit of internal controls. That included "SOX Control Deficiencies" such as situations where "[p]assword requirements [were] not met[.]"

85. The Security Statement was never updated during the Relevant Period to reflect any of these password issues or failures, nor did SolarWinds or Brown otherwise publicly disclose these issues or failures.

b) SolarWinds and Brown's Misstatements and Omissions Regarding SolarWinds Password Policy Were Material.

86. SolarWinds and Brown's misstatements and omissions regarding password issues were not only false and misleading, but materially so. A reasonable investor, considering whether to purchase or sell SolarWinds stock, would have considered it important to know the true state of SolarWinds' password policies, especially considering that these issues were long-standing and potentially affected customer-facing areas such as the Akamai server used to send updates to customers.

87. Brown recognized the importance of such password issues in a September 2019 interview:

> Enterprises that get breached. That was their choice. It seriously was. It was 100 percent their choice. If you look at the attacks that have been successful, most of them have been silly mistakes. Passwords that were stored in the wrong way. Machines that were vulnerable. Systems that weren't patched.

4. SolarWinds and Brown Falsely Claimed That the Company Maintained Strong Access Controls.

88. SolarWinds 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 [sic] the use of privileged and non-privileged access." Individuals at the company used the phrases "access management" and "access controls"

interchangeably. Password policies can be considered one part of access controls, but access controls also include other policies such as what rights or privileges a user has and for which portions of a company's computer network. For example, a person with "administrator" or "admin" rights typically has broader privileges to make significant changes to the software in a given area, such as changing security settings, installing software and hardware, accessing all files on the computer, and making changes to other user accounts.

89. SolarWinds' Security Statement included a section regarding "Access Controls" in which Brown and SolarWinds claimed that SolarWinds implemented strong Access Control policies:

> 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.

The statement continued:

> 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 work-flow tools that maintain audit records of changes.

90. As discussed below, these statements were materially false and misleading.

a) In Truth, SolarWinds Had Allowed Significant Access Problems to Persist for Years.

91. SolarWinds access control environment was diametrically different from the description in the Security Statement. SolarWinds actually had poor access controls—a problem that it failed to remedy for years. Among other things, SolarWinds and Brown claimed in the Security Statement that employees had access on a "least privilege necessary basis." The concept

of "least privilege" is an industry-wide concept that persons should be granted the minimum system resources and authorizations needed to perform their job functions. SolarWinds and Brown further represented, "Role based access controls are implemented for access to information systems," and "SolarWinds employees are granted a limited set of default permissions to access company resources."

92. In reality, between 2017 and 2020, as Brown and SolarWinds' senior management knew, or were reckless or negligent in not knowing, SolarWinds routinely and pervasively granted employees unnecessary "admin" rights, giving them access and privileges to more systems than necessary for their work functions and violating the concept of "least privilege." Indeed, there is evidence that most employees had "Admin" rights at times during the Relevant Period.

93. Internal Company assessments identified numerous access control violations, including expansive use of "admin" privileges and a virtual private network vulnerability that was exacerbated by the Company's failure to enforce its remote access policies.

94. A June 2017 presentation prepared by SolarWinds' Director of IT and shared with its CIO described an "unnecessary level of risk" from too many accounts having admin level access, including the "[s]ystem team" using admin accounts during routine operations.

95. A January 2018 presentation prepared by a SolarWinds project manager and shared with Brown, as well as SolarWinds' CIO, Director of IT and others, warned that "Currently there is a collection of people who have access to many systems and many people involved in provisioning access." The presentation specified that the "lack of standardized user access management processes…create a loss risk of organizational assets and personal data."

96. Brown and Senior InfoSec Manager E prepared a March 2018 Security Projects slide presentation and provided it to SolarWinds' CIO. That presentaiton warned that the "[c]oncept of least privilege [is] not followed as a best practice" and described the "[u]se of shared accounts throughout internal and external applications."

97. An August 2019 Security & Compliance Program Quarterly Review that Brown prepared, the CIO reviewed, and the CEO received, acknowledged, "Access and privilege to critical systems/data is inappropriate." That same presentation noted the need to improve internal practices and procedures. And it assessed that for "Authentication, Authorization and Identity Management," where the control objective was "User identity, authentication and authorization are in place and actively monitored across the company," SolarWinds had a NIST score of 1. That meant the Company had an ad-hoc, inconsistent, or reactive approach to meeting that cybersecurity control objective.

98. The same September 2019 internal FedRAMP security controls assessment discussed above also assessed the subcategory "Access controls." That subcategory contained forty-three controls, with just two rated "in place," eighteen rated "may be in place," and twenty-three rated "No program/practice in place." Of those forty-three evaluated access controls, six related specifically to the concept of least privilege. Of those six least privilege controls, SolarWinds had "No program/practice in place" for four. The other two noted: "This is included in the Access/Security Guidelines document. An audit that this is in place has never been performed."

99. A September 18, 2019 email from a SolarWinds program manager to Brown and SolarWinds' CIO identified multiple cybersecurity deficiencies associated with a SolarWinds authentication system. Specifically, she observed that "passwords have no specific parameters"

in violation of policy, that "access is not audited nor monitored," and that multiple problems existed with product development requirements. In all, the email assessed that 27% of security controls for the product were unmet.

100. As discussed above, Brown helped draft Quarterly Risk Review presentations that sometimes highlighted cybersecurity issues to SolarWinds' senior executives. For example, Quarterly Risk Review presentations in March and October 2020 that were drafted with input from Brown and shared with SolarWinds' CIO and CTO, who in turn updated SolarWinds' CEO, noted "[s]ignificant deficiencies in user access management." Nonetheless, at times or concerning certain specific issues, Brown failed to ensure that other senior executives were sufficiently aware of, or understood, the severity of cybersecurity risks, failings, and issues that he and others knew about. These failures were exacerbated by the Company's poor or inadequate controls.

101. Again, the Security Statement remained materially false and misleading throughout the Relevant Period as it was never updated during the Relevant Period to reflect any of these access control issues or failures, nor did SolarWinds or Brown otherwise publicly disclose these issues or failures.

b) Brown Ignored Warnings About a Critical Access Management Problem With SolarWinds' Virtual Private Network.

102. In June 2018, Network Engineer D identified a "security gap" relating to access to SolarWinds' virtual private network or VPN, by which a user with credentials could evade SolarWinds' data loss prevention software by logging on to SolarWinds' VPN network from a device that was not owned or managed by the Company's information technology department. Such unmanaged devices, sometimes referred to as "Bring Your Own Device," often are

personal cell phones and laptops that employees use to connect to a company's computer network through a VPN to perform work, including remote work or telework.

103. This VPN vulnerability was exacerbated by the fact that many SolarWinds' employees had administrator rights, allowing them to make changes to security settings, among other things. Additionally, SolarWinds did not follow its existing Enterprise Security Standards and Guidelines requiring client device integrity checks for the VPN.

104. Network Engineer D sent an email to various SolarWinds employees, including the Company's Director of IT and Senior InfoSec Manager E, detailing the vulnerability. In the email, Network Engineer D explained that the configuration was "not very secure for resources currently accessible via VPN and data stored there." Network Engineer D proposed a solution involving the use of "certificates for machine authentication," limiting access to "verified/trusted devices…under IT control," while other users could utilize VPN, but with "access to less resources."

105. After receiving pushback to his initial recommendation and seeing no action to remediate the vulnerability, on August 24, 2018, Network Engineer D sent a more urgent message seeking to draw attention to the issue. In his message, which he again sent to SolarWinds' Director of Information Technology and Senior InfoSec Manager E, Network Engineer D explained that it was a common practice for users to access SolarWinds' network from unmanaged devices. He explained that, because of the vulnerability to SolarWinds' VPN, anyone with standard log-in credentials could:

> access [SolarWinds'] corporate wifi or corporate VPN from ANY device, no matter if [C]ompany owned or not….While on corporate wifi, or VPN, such device can basically do whatever without us detecting it until it's too late: It can easily download any content without being detected by [SolarWinds' data loss prevention software], which is normally installed on all domain PCs.

106. On top of his email warnings, Network Engineer D created a presentation describing his concerns ("August 2018 VPN Vulnerability Presentation"). He then delivered that presentation on or around August 28, 2018 at a meeting that included managers such as Senior InfoSec Manager E. In the presentation, Network Engineer D explained that in its current state, SolarWinds' VPN ran the risk that an attacker could access and upload code without detection by SolarWinds' data loss prevention software, serve as a backdoor for future attacks, and reside on SolarWinds' network for an extended period without anyone noticing. Network Engineer D warned that this setup was "not very secure" and explained that someone exploiting the vulnerability "can basically do whatever without us detecting it until it's too late" which could lead to "major reputation and financial loss" for SolarWinds.

107. On August 31, 2018, Senior InfoSec Manager E shared the August 2018 VPN Vulnerability Presentation with Brown. Despite the gravity of the concern raised by the network engineer and his expressed view that exploitation of the vulnerability could lead to significant reputational and financial loss to SolarWinds, Brown failed to elevate the matter further.

108. SolarWinds and Brown took no steps to remediate the vulnerability in 2018 or 2019. In January 2020, Senior InfoSec Manager E, who had previously forwarded the presentation to Brown, sent it to him again, noting that the recommendation "did not get any traction" when it was raised in 2018.

109. Despite the warnings in August 2018, Brown and others aware of the issue did not take steps to ensure that this vulnerability was either fixed or disclosed. No one, including Brown, raised the issue with SolarWinds' Disclosure Committee, nor did SolarWinds have sufficient procedures and controls in place to ensure that he did so. Nor did he, or anyone else at

SolarWinds, ensure that SolarWinds enforced its existing internal guidelines requiring client device integrity checks for the VPN.

110. Further, the VPN Vulnerability identified by Network Engineer D was not addressed by compensating or technical controls or other means. Instead, the Company went forward with its October 2018 IPO offering without disclosing this known vulnerability (or even assessing the materiality of the vulnerability for disclosure purposes), thus depriving investors of key information. Nor did the Company take straightforward steps to remedy the vulnerability to render it immaterial, which would have only required enforcing best practices and using existing, in-place software with little or no cost to block non-managed devices from accessing SolarWinds' network. The risk of non-managed devices accessing corporate resources is well-known in the security field, and the Company failed to put even minimal compensating controls in place once the vulnerability was identified. For example, the Company failed to make any effort to regularly detect or automatically alert the presence of non-managed devices, and did not undertake an investigation during the Relevant Period to determine whether the vulnerability had been exploited.

111. The Security Statement remained materially false and misleading, as, again, it was never updated during the Relevant Period to reflect any of these access control issues or failures (including the VPN issue), nor did SolarWinds or Brown otherwise publicly disclose these issues or failures.

c) SolarWinds and Brown's Misstatements and Omissions Regarding Access Controls Were Material.

112. SolarWinds' and Brown's misstatements and omissions regarding access controls were not only false and misleading, but materially so. A reasonable investor, considering whether to purchase or sell SolarWinds stock, would have considered it important to know the

true state of SolarWinds' security, especially regarding the state of the Company's access controls for "information systems" and "sensitive data." For analysts who followed SolarWinds at the time and issued reports regarding its stock, expansive use of administrator privileges could have been important in determining whether to recommend that investors purchase or sell SolarWinds stock. Indeed, the expansive use of administrator rights is so problematic that it could cause a reasonable analyst to question all of a company's operations.

5. Brown Made Misstatements in Company-Approved Press Releases, Blog Posts, and Podcasts.

113. The Security Statement was not the only place where Brown and the Company made materially false and misleading statements related to SolarWinds' cybersecurity practices. Brown acted as SolarWinds' primary cybersecurity spokesperson during the Relevant Period. He highlighted SolarWinds' cybersecurity practices in SolarWinds' podcasts, blog posts, and press releases. Both the blog posts and podcasts were promoted by the Company. And the blog posts were posted on a SolarWinds' website, identified Brown as a SolarWinds' employee, discussed his professional background, contained information about SolarWinds' products, and linked to the Trust Center and/or other portions of SolarWinds' website.

114. In a March 2019 podcast referring to SolarWinds' cybersecurity practices, Brown stated that the company was "focused on…heavy-duty hygiene," which Brown described in sworn testimony as the "things that…make up cyber best practices."

115. Similarly, in a 2020 blog post linked to SolarWinds' website, Brown assured the public 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." Brown then included a hyperlink in this blogpost to the Trust Center of SolarWinds' website containing the Security Statement, further disseminating the Security Statement. Brown's statement in the blog

post that SolarWinds "makes sure everything is backed by sound security processes, procedures and standards" is false because, as discussed above, in truth SolarWinds had multiple unaddressed cybersecurity problems, including its failure to abide by SDL, password issues, and access control issues.

116. SolarWinds and Brown also promoted the Company's purported commitment to cybersecurity in multiple press releases that were publicly distributed and are maintained on the investor section of the Company's website. This included an October 7, 2019 press release in which SolarWinds stated that the Company "equips technology professionals with tools to help monitor, manage, and secure today's complex IT environments." In that same release, SolarWinds disseminated 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."

117. It also included a December 12, 2019 press release touting "SolarWinds' commitment to high security standards, which its partners rely on to help keep the systems they manage secure and compliant." In that same release, SolarWinds disseminated Brown's statements 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."

118. These statements were materially false misleading, and contained material omissions. They described a SolarWinds' cybersecurity practices to the public in a positive light, touting things such as SolarWinds purported "commitment to high security standards," which are

belied by the numerous internal statements quoted in this Complaint regarding SolarWinds' poor cybersecurity practices and policy violations.

6. SolarWinds Had Pervasive Cybersecurity Deficiencies.

119. The specific cybersecurity issues highlighted above were part of a pervasive cybersecurity problem throughout SolarWinds during the Relevant Period and reflected a culture that did not take cybersecurity issues with sufficient seriousness, and a scheme to conceal these issues from investors and customers.

120. For example, during the same month as SolarWinds' IPO, Brown sent a presentation to SolarWinds' CIO that warned SolarWinds needed to "Lock down our critical assets that could cause a major event" and that the "[c]urrent state of security leaves us in a very vulnerable state for our critical assets." The presentation included multiple red text warnings such as "Many independent user stores still in use and not well controlled." And the presentation flagged the risk that "[l]ack of cyber hygiene leaves us open to being a target of opportunity." As discussed below, despite this frank recognition of SolarWinds' multi-faceted and significant cybersecurity problems and risks, the Company made no effort to adequately disclose the true state of its cybersecurity in disclosures to investors, including in connection with the IPO, which instead only included generic warnings.

121. An October 2019 presentation sent to Brown warned of "Problems with [SolarWinds'] Security initiative" including that there was "No true expertise for security" and that core SolarWinds teams "do[] NOT understand security!"

122. Likewise, an April 15, 2020 email to Brown warned "we have a systemic issue around lack of awareness for Security/Compliance requirements with most if not all DOIT projects."

123. In instant messages sent in October 2020, Senior InfoSec Manager E expressed his own disgust with 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."

124. Indeed, the poor state of SolarWinds' cybersecurity posture seemed to be a joke for employees in its InfoSec group, at least prior to the SUNBURST hack being revealed. In October 2020, InfoSec Employee F and Senior InfoSec Manager E exchanged the following messages before Senior InfoSec Manager E's vacation:

F: …I hope you have a good time off and I will try to man the fort!

E: more like keep the house from burning down! lol

F: hard with all these faulty electrics

125. As described above, SolarWinds and Brown knew, or were reckless or negligent in not knowing, that the listed statements in the Security Statement, podcasts, and blogs contained materially false and misleading statements, and that SolarWinds and Brown had omitted and failed to disclose (either in the Security Statement or in other public statements) the true state of SolarWinds' cybersecurity practices, including the risks, issues, and violations discussed in this Complaint. Those omissions made the statements made, in light of the circumstances, materially misleading.

126. The materiality of many of the issues described above is heightened by the presence of many of the other issues. For example, the materiality of SolarWinds having both the VPN issue and the pervasive use of admin rights is greater than either issue alone.

127. Brown was the maker of these statements for the reasons described above and his knowledge, recklessness, and/or negligence imputes to the Company for the reasons described

above and by virtue of his role as an officer of SolarWinds, head of its InfoSec group, chief spokesperson on cybersecurity issues, and the literal "face" of cybersecurity at the Company (his picture was prominently displayed on the "Trust Center" of SolarWinds' website where the Company posted the Security Statement).

128. Additionally and alternatively, the SolarWinds employees involved in and responsible for these issues, including those described above, collectively knew, or were recklessness or negligent in not knowing, that the Security Statement was false and misleading and contained material and misleading omissions for the reasons described above.

129. Finally, given all of SolarWinds' cybersecurity problems discussed above, Brown and/or other SolarWinds executives could have reasonably anticipated that SolarWinds would be subject to a material cyberattack.

C. SolarWinds Made Materially False and Misleading Statements About Its Cybersecurity Practices in Its SEC Filings.

130. SolarWinds returned to being a publicly traded company through a (second) Initial Public Offering registered via a Form S-1 that was filed with the SEC on October 18, 2018, and which was signed by the Company's CEO and CFO. This registration statement contained a boilerplate disclosure regarding cybersecurity risks.

131. SolarWinds' sole cybersecurity risk disclosure in its October 2018 Registration Statement on Form S-1 provided that:

> **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 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.

(emphasis in original)

132. This disclosure recited the harm that could befall SolarWinds and generic and hypothetical cybersecurity risks that most companies face. But it did nothing to alert investors to the elevated risks that existed at SolarWinds. Those risks are not being assessed in hindsight by the SEC. Brown and others at SolarWinds assessed and documented them at the time. Indeed, as Brown stated (internally) during the very month that SolarWinds made the above public disclosure: the "current state of security leaves us in a very vulnerable state for our critical assets."

133. SolarWinds' disclosures failed to convey the known risks discussed above, or even that known risks of this type had been identified. Even if some of the individual risks and incidents discussed in this Complaint did not rise to the level of requiring disclosure on their own, at least collectively they created such an increased risk to SolarWinds that the failure to disclose their collective impact on SolarWinds' cybersecurity posture rendered the risk disclosures that SolarWinds made materially misleading.

134. Despite internally documenting all the cybersecurity issues and problems discussed above, and despite multiple internal warnings about their severity, SolarWinds neither specifically disclosed the issues nor generally disclosed that known, unremediated issues with NIST compliance, SDL, access controls (including the known VPN vulnerability), or passwords existed. Nor did SolarWinds even disclose Brown's assessment that it was "very vulnerable" to a cyberattack. As a result, SolarWinds' October 18, 2018 Form S-1—and especially the risk disclosure quote above—was materially misleading.

135. Risk factors, and changes to risk factors, in a company's SEC filings are commonly reviewed by investors and securities analysts in connection with decisions and recommendations to purchase or sell stock. A reasonable investor, considering whether to purchase or sell SolarWinds stock, would have considered it important to know the true nature and scale of the cybersecurity risks facing the Company, not merely generic risk disclosures that did not accurately reflect the known significance of the Company's vulnerabilities. A reasonable investor would have also wanted to know about the Company's known and increasing risk of cyberattacks, which could have materially negative effects on the Company, and which were not adequately conveyed through the Company's generic disclosure. Additionally, as discussed

above, for SolarWinds, increased risk of a cybersecurity event had particular significance. SolarWinds' misleading Form S-1 deprived investors of that material information.

136. SolarWinds then repeated (or incorporated by reference) the exact same materially misleading risk disclosures, in the following SEC filings throughout the Relevant Period:

Filing Type	**Date Filed with SEC**
Form 10-Q, Quarterly Report	November 27, 2018
Form 10-K, Annual Report	February 25, 2019
Form S-8, Registration Statement	April 11, 2019
Form 10-Q, Quarterly Report	May 10, 2019
Form S-1, Registration Statement	May 20, 2019
Form 10-Q, Quarterly Report	August 12, 2019
Form 10-Q, Quarterly Report	November 7, 2019
Form S-8, Registration Statement	December 11, 2019
Form 10-K, Annual Report	February 24, 2020
Form S-8, Registration Statement	February 24, 2020
Form 10-Q, Quarterly Report	May 8, 2020
Form 10-Q, Quarterly Report	August 10, 2020
Form 10-Q, Quarterly Report	November 5, 2020

137. Worse still, SolarWinds made these repeated misleading disclosures even as an accumulating number of red flags piled up throughout 2020. In other words, this generic warning was materially false and misleading when first made and only became worse over time. The Company's failure to disclose the accumulating red flags left investors without sufficient warning that there had been multiple successful intrusions against Orion, or that SolarWinds' overall cybersecurity posture was so poor that something far worse could be just around the corner.

138. SolarWinds also failed to remediate the issues described above ahead of its IPO in October 2018, and for many of them, for months or years afterwards. Thus, threat actors were able to later exploit the ***still unremediated*** VPN vulnerability to access SolarWinds' internal systems in January 2019, avoid detection for nearly two years, and ultimately insert malicious code resulting in the SUNBURST cyberattack.

D. SolarWinds and Brown Failed to Disclose Red Flags and Warning Signs of a Cyberattack Leading up to the Revelation of the SUNBURST Cyberattack.

1. In January 2019 Threat Actors Accessed SolarWinds' Network Environment via VPN Using an Unmanaged Device.

139. In January 2019, just months after SolarWinds' IPO, the threat actors responsible for the SUNBURST cyberattack accessed SolarWinds' corporate VPN by using an unmanaged third-party device and stolen credentials, exploiting the vulnerability that Network Engineer D had identified six months earlier. During those six months, SolarWinds and Brown had neither remediated nor disclosed this vulnerability.

140. From approximately January 2019 through approximately November 2020, the threat actors repeatedly accessed SolarWinds' network through a VPN. During that time, the threat actors 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 that would be deployed during later stages of the campaign.

141. As anticipated in Network Engineer D's August 2018 presentation, once the threat actors accessed the system through a VPN connection on an unmanaged device, they were able to access SolarWinds' entire network, moving laterally between its corporate and software development zones. In part due to access control deficiencies described above, the threat actors 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. The threat actors used multiple accounts that had administrator privileges, exploiting a security problem that SolarWinds had known about since at least June 2017. The threat actors were also able to access and monitor network access and emails of SolarWinds' key personnel without detection. This included exfiltrating approximately 7 million

emails from more than 70 SolarWinds employees between approximately December 2019 and December 2020, including emails from employees in the Information Technology and Security groups.

142. Following months of reconnaissance and data exfiltration from the SolarWinds' networks, in November 2019, the threat actors used information gained from their access to SolarWinds' networks and data to begin a trial run of what ultimately became the SUNBURST attack. The threat actors conducted this trial run by first inserting non-malicious test code into SolarWinds' Orion software builds to determine whether they could successfully evade detection.

143. Seeing that their insertion of non-malicious code went undetected, in February 2020, the threat actors began inserting malicious code into Orion software builds. Over the next several months, the threat actors inserted malicious code into three different Orion software builds that went out to nearly 18,000 customers. The impacted customers included numerous federal and state government agencies, and more than 1,500 publicly traded U.S. companies, banks, broker-dealers, accounting firms, and other entities regulated by the SEC. The malicious code provided the 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. The threat actors utilized the SUNBURST attack to conduct additional secondary attacks on approximately 100 of the 18,000 impacted companies and government agencies.

144. In certain reports, the SUNBURST attack has been attributed to a Nation-State actor. But the vulnerabilities that the threat actors exploited to access SolarWinds' system and ultimately infect its customers' systems were vulnerabilities that SolarWinds and Brown had

known about for months and that could have been remedied through straightforward steps. The possibility that SUNBURST was committed by a Nation-State actor neither excuses SolarWinds' failure to adhere to ***basic*** cybersecurity practices, nor justifies the Company hiding those failures from the investing public.

2. Throughout 2020, SolarWinds and Brown Learned of Focused Attacks on Its Orion Products and Other Platforms.

145. Beginning in early 2020, SolarWinds and Brown learned of an increase in threats to its products and customers, including multiple attacks against customers' Orion platforms. In addition, the Company and Brown learned of multiple serious vulnerabilities in the Orion platform products. The additional risks, attacks, and vulnerabilities served as red flags indicating that SolarWinds had been, or was at increased risk of soon becoming, the victim of a significant cyberattack. None of these red flags were disclosed during the Relevant Period, either in the Company's periodic filings or otherwise.

a) SolarWinds Learned of Multiple Attacks Against Its MSP Platforms During 2020.

146. During the Relevant Period, SolarWinds had a business unit that focused on Managed Service Providers ("MSPs"), companies that used SolarWinds products to provide network management services to end users. Those end users often included small or medium-sized companies that wished to outsource their network management.

147. In the first half of 2020, at least nine MSPs who were SolarWinds customers suffered attacks through SolarWinds' MSP products, including ransomware attacks. All nine of the attacks involved the use of accurate credentials on the threat actors' first attempt, suggesting that the threat actors had somehow obtained the credentials before the attacks. The attacks led SolarWinds to investigate whether its database of customer credentials may have been

compromised, a concern that SolarWinds was unable to resolve and a red flag that its own systems may have been compromised.

148. In March 2020, SolarWinds learned that a threat actor had attacked SolarWinds' MSPs using a list of 19,000 single sign-on customers, meaning that the threat actors had information to distinguish between customers who had enabled more secure multi-factor authentication and customers who did not have it enabled. This was another red flag that malicious actors had access to SolarWinds' network and/or systems.

149. In both cases, SolarWinds failed to determine how the threat actors had obtained the credentials or list of single sign-on customers, though Company personnel, including Senior InfoSec Manager E, theorized that it might have been through a breach of SolarWinds' systems.

150. In June 2020, Brown noted the ongoing problems with the Company's MSP products, including that the threat actors exhibited a high degree of familiarity with the Company's MSP products. This indicated that the threat actors had likely conducted reconnaissance on, and were specifically targeting, SolarWinds' MSP products and customers. Brown also provided SolarWinds' CIO and CTO at least partial updates regarding these issues, including information evidencing the threat actor's high level of familiarity with the MSP products. In a July 2020 presentation, Brown stated that the threat actors "know N-Central [SolarWinds' MSP product]…Know how to deploy software, shut off backup etc." The threat actors' ability to "deploy software, shut off backup" was another red flag.

151. But none of the MSP issues, or Brown's assessment of them, was disclosed to investors during the Relevant Period, either by (a) specifically listing the issues, (b) disclosing a general statement that alerted investors that SolarWinds was facing increased cybersecurity

issues that signified a potential focused attack on, and compromise to, their systems, or (c) any other form.

152. These attacks on SolarWinds' MSPs were material. As Brown acknowledged, like Orion, the MSP products were among the Company's "crown jewels" that needed to be protected. In a September 2019 interview, Brown 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?'

3. SolarWinds and Brown Learned of Attacks on, and Vulnerabilities in, Its Orion Products in 2020.

153. Several times before December 2020, customers alerted SolarWinds to evidence that threat actors were not only specifically targeting SolarWinds' Orion platform and customers, but had breached SolarWinds' systems. U.S. Government Agency A and Cybersecurity Firm B notified SolarWinds of incidents that took place in May and October 2020, respectively, that were later linked to the SUNBURST cyberattack. SolarWinds did not publicly disclose any of these incidents (either individually or through their collective impact), update the Company's overall risk disclosure in any way, or identify and remediate the vulnerabilities to render them immaterial.

a) The May 2020 Attack on U.S. Government Agency A Reveals Too Many Vulnerabilities for SolarWinds to Handle.

154. In June 2020, U.S. Government Agency A notified SolarWinds about malicious activity by the Orion software after it was installed on the agency's system in May 2020. U.S. Government Agency A informed SolarWinds that the Orion software was attempting to contact unknown websites and asked the Company to investigate. SolarWinds uncovered evidence that

the threat actors who were attacking U.S. Government Agency A had conducted reconnaissance on the Orion platform since at least mid-2019.

155. Brown was aware of the May 2020 attack against U.S. Government Agency A by June 2020. Despite the potential severity of this issue, SolarWinds' internal investigation failed to uncover the root cause for the malicious activity or otherwise remediate the vulnerability in the widely used Orion software. SolarWinds' inability to determine the root cause for this attack was another red flag.

156. In a subsequent July 1, 2020 email to Brown, a member of the Engineering team described being "spooked" by Orion's activity at U.S. Government Agency A. Brown determined that there were only two possible scenarios: (1) the attacker was already present on the customer's system or (2) the attack was looking closely at Orion "for methods to utilize it in larger attacks." Brown asserted that the incident was "very concerning" and continued, "As you guys know our backends are not that resilient and we should definitely make them better." At no point during the Relevant Period did Brown or SolarWinds disclose Brown's assessment that portions of SolarWinds' information technology structure were "not that resilient" or that the attack was "very concerning" due in part to possibility that SolarWinds' systems were compromised.

157. The Company's internal investigation of the attack uncovered "numerous" vulnerabilities—some of which had been present and identifiable for years—that needed to be remedied to protect the Orion platform from future attacks. The large increase in incidents and vulnerabilities led SolarWinds' employees to complain 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, and that fixing all of the issues—even with adequate staff—would take years.

158. SolarWinds used Risk Acceptance Forms to document instances where risks fell outside SolarWinds' "standard guidelines," regarding cybersecurity. Brown was one of the small group of people authorized by the company to accept and approve such risks, and generally was one of the two people who would approve them. In September 2020, a manager from SolarWinds' engineering team submitted for approval a Risk Acceptance Form that went to Brown and others. The form asked them to "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 Engineering teams to resolve."

159. In October 2020, an engineering employee sent an instant message to an InfoSec manager stating that "there is no way we fix what is in Jira [SolarWinds' vulnerability tracking system] in next five years…[e]ven if we hire like crazy." Undersized staff to respond to cybersecurity incidents was not a new complaint—SolarWinds' CIO had identified it to SolarWinds' CEO as a "key risk" in 2019. The backlog and inadequate staffing were additional red flags. None of the backlog or staffing issues were disclosed to the investing public during the Relevant Period.

b) The October 2020 Attack on Cybersecurity Firm B Prompts SolarWinds to Lie to Conceal Orion's Flaws.

160. In October 2020, another SolarWinds customer, Cybersecurity Firm B, notified the Company about malicious activity by Orion software. SolarWinds' employees then recognized and discussed internally that the activity was similar to the activity reported a few months earlier by U.S. Government Agency A. Individuals in SolarWinds' InfoSec team recognized the unique

nature of the intrusion and noted that both attacks utilized SolarWinds' Business Layer Host to download malicious files from the internet.

161. In October 2020, Brown was informed of the Cybersecurity Firm B incident and the similarities between it and the May 2020 U.S. Government Agency A incident. An email on October 14, 2020 that was later forwarded to Brown on October 16, 2020 says in part "[Cybersecurity Firm B] in touch with customer support and it seems they had a breach similar to [U.S. Government Agency A]…" This was another red flag, especially because it strongly indicated that of the two possible scenarios Brown outlined after the attack on U.S. Government Agency A, the reality was that SolarWinds' systems were compromised. In other words, by October 2020 if not earlier, SolarWinds and Brown knew, or were reckless or negligent in not knowing, that the Company's systems had been breached.

162. SolarWinds InfoSec staff had multiple communications with Cybersecurity Firm B regarding this attack. Prior to one such telephone conversation, InfoSec Employee F confirmed with Senior InfoSec Manager E that SolarWinds was not disclosing anything about the U.S. Government Agency A attack to Cybersecurity Firm B, despite their knowledge of similarities between the attacks. On a telephone call on November 5, 2020, personnel from Cybersecurity Firm B asked if SolarWinds had ever seen Orion act as it had during the attack. In truth, as InfoSec Employee F and others at SolarWinds knew, Orion had acted the same way during the U.S. Government Agency A attack. Nonetheless, in accordance with Senior InfoSec Manager E's guidance, InfoSec Employee F falsely informed Cybersecurity Firm B that they had not previously seen similar activity from the Orion platform. In contemporaneous instant messages sent during the telephone call with the customer, InfoSec Employee F messaged his colleague, "***Well I just lied***." Then, despite recognizing the similarities with the earlier incident, InfoSec

employees falsely informed Cybersecurity Firm B that they believed the activity was linked to a different, known issue because Cybersecurity Firm B had not applied a previous patch.

163. After the call, Cybersecurity Firm B emailed SolarWinds stating that it appeared to be an "unknown vulnerability" at play, rather than what SolarWinds had suggested, and strongly encouraging SolarWinds to handle the incident as "an external attacker." Despite repeated requests from the customer for assistance, SolarWinds again failed to investigate sufficiently, uncover the root cause for the malicious activity, or otherwise remediate the vulnerability in the Orion software, which was being used by thousands of customers worldwide.

164. SolarWinds and Brown knew, or were reckless or negligent in not knowing, that the similar attacks on U.S. Government Agency A and Cybersecurity Firm B, both through Orion, suggested a problem with the Orion software and a compromise in SolarWinds systems. Nonetheless, even after the Cybersecurity Firm B attack, SolarWinds and Brown did not disclose to investors any warning about this situation or determine the source of the potential problem and remediate it.

165. The failure to disclose either the U.S. Government Agency A or Cybersecurity Firm B attacks was part of an overall scheme to conceal both the problems with Orion specifically, and the overall poor state of SolarWinds' cybersecurity. This scheme included other deceptive business practices. Brown and SolarWinds, on multiple occasions, misled customers regarding the quality of its cybersecurity controls to win contracts. For example, in 2019, Customer G needed information about SolarWinds' internal security testing before moving forward with a "pending deal." Brown said to other SolarWinds employees, "I'm in control of what we share" and that, in his response to Customer G, "I called the [pending issues] that were partially

mitigated as mitigated. This should give [Customer G] enough to move forward with the purchase."

166. And in 2020, following the incident described above involving U.S. Government Agency A, that agency was still considering whether to purchase Orion. A member of SolarWinds' sales team misrepresented to U.S. Government Agency A that the Company was compliant with a federal government-wide compliance program—while knowing, or recklessly or negligently not knowing, that the Company was not compliant—to convince U.S. Government Agency A to purchase and use the Orion platform, despite the prior incident.

4. Brown and Others Knew About the Extensive Risks to SolarWinds' Orion Products.

167. Brown was aware of the extensive risks and vulnerabilities to SolarWinds' Orion platform and other products, as shown by multiple internal documents.

168. A July 2020 presentation to SolarWinds Product Management group (prepared by Brown and reviewed by SolarWinds' CIO and SolarWinds' CTO) noted that "SolarWinds [was] no longer under the radar." The presentation described "[Distributed Denial of Service] attacks against marketing sites," "targeted attacks against products," and "sophisticated phishing attacks increasing." It also noted "Recon [was] conducted as early as mid-2019 against SWI" and that Solar Winds' "[i]nternal investigation [had] uncovered additional risks with OIP [the Orion Improvement Program] as an overall service." And the presentation pointed to evidence of reconnaissance against the Company's MSP products, noting that the MSP attackers "know N-Central [the MSP product]. Know how to deploy software, shut off backup etc…"

169. In a July 1, 2020 email to members of SolarWinds' engineering department, Brown 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."

170. An October presentation that Brown helped prepare gave a similar description, noting 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.

171. During October and November 2020, SolarWinds was informed of at least eight other high-risk vulnerabilities affecting the Orion platform through the Zero Day Initiative, a program that rewards security researchers for privately reporting vulnerabilities. The Zero Day Initiative vulnerabilities included remote code execution vulnerabilities, which SolarWinds' InfoSec team members described as "the most serious" form of vulnerabilities. SolarWinds never disclosed these vulnerabilities during the Relevant Period.

172. An October 2020 Quarterly Risk Review presentation sent to Brown and others highlighted what Brown had said previously: "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."

173. In October 2020, an InfoSec employee sent an instant message to Senior InfoSec Manager E with a link to a list of vulnerabilities in the Orion platform stating, "The products are riddled and obviously have been for many years." The next month, a SolarWinds' network engineer complained, "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. Not good."

174. None of these risk factors affecting "crown jewel" products were disclosed to the investing public during the Relevant Period.

5. Despite Increasing Warnings, SolarWinds Repeated Its Same Materially False and Misleading Risk Disclosures in SEC Filings.

175. At no point between the time of its IPO in October 2018 and the disclosure of Sunburst in 2020 did SolarWinds disclose the numerous risks, vulnerabilities, and incidents affecting its products in its SEC filings or elsewhere. Instead, in each periodic disclosure and registration statement during the period, SolarWinds disclosed the same hypothetical, generalized, and boilerplate description that had appeared in its October 2018 Form S-1. SolarWinds had experienced events, attacks, and red flags prior to and throughout 2020. As described above, Brown knew, or was reckless or negligent in not knowing, that SolarWinds' critical assets were vulnerable, that SolarWinds was not following important cybersecurity policies, and that it had been the subject of attacks. Nonetheless, Brown signed sub-certifications relied on by senior executives, confirming that all material incidents had been disclosed to the executives responsible for the Company's securities filings. But despite Brown's knowledge of the increased risks, SolarWinds repeatedly failed to disclose the known cybersecurity risks in the Company's periodic reports, rendering them materially misleading.

176. Instead, in quarterly reports on Forms 10-Q from the first quarter of 2020 through the third quarter of 2020, filed on May 8, 2020, August 10, 2020, and November 5, 2020, SolarWinds stated that there had been "no…material changes" to the risk factors quoted above. Those statements were materially false and misleading. A reasonable investor, considering whether to purchase or sell SolarWinds stock, would have considered it important to know the

true risks facing the Company (including both the ongoing cybersecurity controls and the increased risks to Orion), not merely generic risk disclosures. This is especially the case because Orion represented 45% of SolarWinds' revenue in 2020 and there were multiple red flags suggesting both intrusions at SolarWinds and specific problems with Orion. The attacks also affected SolarWinds' MSP products, another "crown jewel."

177. As described above, SolarWinds and Brown knew, or were reckless or negligent in not knowing, that the risk disclosure in the listed SEC filings contained materially false and misleading statements, and that SolarWinds omitted and failed to disclose (either in the SEC filings or elsewhere) the true state of SolarWinds' cybersecurity risks, including the issues, attacks, and violations discussed above. Those omissions made the statements made, in light of the circumstances, misleading.

178. Brown signed sub-certifications for each quarter during the Relevant Period in which he certified in relevant part that:

> The processes listed below as part of the designed internal controls over financial reporting are adequately designed, documented, and the associated key controls have been adequately performed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for internal and bank reporting purposes in accordance with generally accepted accounting principles. All discrepancies, issues or weaknesses have been communicated to the CFO and/or President.
>
> …I have reviewed the represented control matrix for the quarter stated above to ensure to the best of my knowledge that the controls accurately reflects [sic] the procedures performed (all material changes to the process have been properly documented) and in my opinion all of the key controls have been identified.

179. In documents attached to, or referred to by, these certifications, Brown is designated as responsible for certifying these issues for the Information Technology General Computing Controls relating to "Security."

180. As Brown knew, or was reckless or negligent in not knowing, that certification was false because the numerous, documented cybersecurity failures prevented SolarWinds from having effective controls.

181. Additionally and alternatively, the SolarWinds employees involved in and responsible for these issues, including those described above, collectively knew, or were recklessness or negligent in not knowing, that the SEC filings listed above were false for the reasons described above.

E. Once SolarWinds Learned of the SUNBURST Attack, It Did Not Fully Disclose Its Known Impact.

1. In December 2020, a Third SolarWinds Customer Detected Orion Problems and Uncovered the SUNBURST Attack.

182. In December 2020, yet another customer, Cybersecurity Firm C, notified SolarWinds of an attack against its Orion platform. After identifying the attack and determining that the Orion platform was the likely attack vector, Cybersecurity Firm C reverse-engineered the SolarWinds' code to identify what was causing the malicious activity. Within a matter of days, Cybersecurity Firm C had identified the root cause of the malicious activity within the Orion software code.

183. Cybersecurity Firm C contacted SolarWinds' CEO on December 12, 2020, and explained that there was a vulnerability in the Orion software as a result of malicious code that had been inserted into the Orion product by a threat actor. Cybersecurity Firm C shared the decompiled code with SolarWinds during a call with Brown and others on December 12, 2020.

184. Upon reviewing the decompiled code, and no later than December 13, 2020, Brown immediately linked the Cybersecurity Firm C attack to both the earlier May 2020 attack against U.S. Government Agency A and the October 2020 attack against Cybersecurity Firm B. According to Brown's sworn testimony, there was no additional work that he or SolarWinds

needed to do to link the May and October 2020 attacks to the malicious code provided by Cybersecurity Firm C in December:

> Q: …Was there additional analysis that was done to determine that happened in the [Cybersecurity Firm B] incident and it happened in the [U.S. Government Agency A] incident?
>
> A: It wasn't necessary, right? The code that he saw that was dropped that was supplied by [Cybersecurity Firm C], 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 [U.S. Government Agency A] 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.

2. SolarWinds Made Materially False and Misleading Public Statements About the SUNBURST Attack.

185. After learning on December 12, 2020 that malicious code had been inserted into the Orion platform, Brown and other executives worked to prepare a Form 8-K announcing the vulnerability. Brown participated in drafting the Form 8-K and was responsible for confirming the accuracy of the technical statements made in it.

186. On December 14, 2020, SolarWinds filed a Form 8-K with the SEC that publicly disclosed the SUNBURST attack but created a materially misleading picture of the Company's knowledge of the impact of the attack in at least three respects.

187. First, the December 14, 2020 Form 8-K stated that SolarWinds had "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 knew that this vulnerability was not theoretical but rather, as described above, that the vulnerability definitively allowed the attacker to compromise the server on which the Orion products were running. In fact, SolarWinds knew that attackers had

already utilized the vulnerability to do so on at least three occasions (U.S. Government Agency A, Cybersecurity Firm B, and Cybersecurity Firm C) since at least May 2020.

188. Second, SolarWinds stated that it hired 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." In fact, SolarWinds knew that the vulnerability had been exploited as a point of infiltration of customers' systems on at least three prior occasions–in the U.S. Government Agency A, Cybersecurity Firm B, and Cybersecurity Firm C incidents.

189. Third, SolarWinds stated that it was "***still investigating whether, and to what extent, a vulnerability in the Orion products was successfully exploited***" in any reported attacks. In fact, SolarWinds knew the vulnerability in the Orion products had been successfully exploited on at least three prior occasions (U.S. Government Agency A, Cybersecurity Firm B, and Cybersecurity Firm C) since as early as May 2020.

190. Brown—who, among other things, was an officer of SolarWinds, head of its InfoSec group, and its point person on cybersecurity issues—participated in the meeting when this statement was drafted, assisted in drafting it, and was responsible for reviewing it and approving its technical/factual accuracy. When the statement was drafted, Brown knew, or was reckless or negligent in not knowing, that the attacks against Cybersecurity Firm C and those against U.S. Government Agency A and Cybersecurity Firm B, were connected. And Brown therefore knew, or was reckless or negligent in not knowing, that the Form 8-K contained materially false and misleading statements, and that during the Relevant Period SolarWinds omitted and failed to disclose (either in the Form 8-K filings or elsewhere) the true impact of SUNBURST, including the connections to the attacks on U.S. Government Agency A,

Cybersecurity Firm B, and Cybersecurity Firm C discussed above. Those omissions made the statements made, in light of the circumstances, misleading.

191. Brown's knowledge, recklessness, and/or negligence is attributable to the Company by virtue of his role in the company as an officer of SolarWinds, head of its InfoSec group, and chief internal cybersecurity expert, and his presence and involvement in the drafting of the Form 8-K, and his approval of the statement regarding its accuracy.

192. Additionally and alternatively, the SolarWinds employees involved in and responsible for these issues, including those described above, collectively knew, or were reckless or negligent in not knowing, that the Form 8-K was false for the reasons described above.

193. The impact of SolarWinds' December 14, 2020 Form 8-K disclosing the SUNBURST attack resonated with investors, even in its materially misstated form, and SolarWinds' stock price declined more than 16% the day of the announcement and at least another 8% the next day. As the Company provided more information regarding the attacks and the impact on its customers, and as news articles described SolarWinds' preexisting cybersecurity problems, SolarWinds' stock price dropped approximately 35% below its pre-disclosure price by the end of the month.

F. SolarWinds Had Multiple Internal Controls Failures.

1. SolarWinds Lacked Sufficient Internal Accounting Controls to Protect Its Key Assets.

a) SolarWinds Was Required to Have Reasonable Internal Accounting Controls.

194. As an Exchange Act Section 13(a) reporting company, SolarWinds was required to "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." In that regard, SolarWinds was required to develop reasonable

safeguards against unauthorized access to Company assets by designing and maintaining reasonable controls to prevent and detect unauthorized access to, or use of, its assets.

195. SolarWinds' information technology network environment, source code, and products were among the Company's most critical assets. As discussed above, Orion was among SolarWinds' "crown jewel" assets. SolarWinds' Code of Conduct also described the Company's software code and information technology infrastructure among its most important assets and emphasized employees' responsibility to protect such information. In its October 18, 2018 Form S-1, SolarWinds stressed the importance of its "technology infrastructure to sell [its] products and operate [its] business" as well as its customers' reliance on SolarWinds' technology to manage their own information technology infrastructure.

196. SolarWinds assessed the effectiveness of its internal controls using the framework in *Internal Control – Integrated Framework* issued in 2013 by the Committee of Sponsoring Organization of the Treadway Commission ("COSO Framework"). For cybersecurity controls, the COSO Framework requires an organization to select and develop internal control activities over technology that are designed and implemented to restrict technology access rights to authorized users and to protect the entity's assets from external threats.

197. Under the COSO Framework, SolarWinds chose to use the NIST Framework described above to conduct assessments. As discussed above, SolarWinds admitted in internal documents that it had no program or practice in place for a majority of the controls in the NIST Framework, and had assessed itself to be performing poorly on multiple critical controls.

b) SolarWinds Did Not Have Sufficient Controls to Reasonably Protect Its Critical Assets.

198. As a result of the above shortcomings to SolarWinds' cybersecurity controls, the Company failed to devise and maintain a system of internal controls sufficient to provide

reasonable assurance that access to the Company's assets was only in accordance with management's general or specific authorization.

199. SolarWinds did not follow its own certification control concerning cybersecurity, including failing to use and document a list of controls in connection with certifications by Company officials. Brown certified to the effectiveness of the Company's information technology controls around financial reporting. But neither he nor the Company were able to identify the list of relevant controls to the SEC during the SEC's investigation. Brown instead certified based on his general sense of the quality of those controls, while failing to identify the Company's extensive shortcomings in areas such as access controls.

200. SolarWinds' cybersecurity-related policies and procedures went largely unimplemented or were subject to extensive problems or violations. Internal assessments applying the NIST Framework, which the Security Statement said SolarWinds followed, showed that between 2019 and 2021, the Company had "no program/practice in place" for most of the controls. In particular, as discussed above, the Company had significant lapses around access controls, frequently violated its own internal password policy, and failed to apply SDL to at least some of its products, including the Orion Improvement Program portion of the Orion platform.

2. SolarWinds Had Deficient Disclosure Controls.

201. SolarWinds was also required by Exchange Act Rule 13a-15(a) to maintain disclosure controls and procedures, including controls and procedures designed to ensure that information required to be disclosed by an issuer is accumulated and communicated to management to allow for timely decisions regarding disclosure.

202. SolarWinds lacked controls to ensure that information regarding potentially material cybersecurity risks, incidents, and vulnerabilities was reported to the executives responsible for disclosures. For example, SolarWinds' Incident Response Plan, which Brown

helped implement and maintain, provided for a classification of risks based on the impact to customers, and only incidents that impacted multiple customers were reported upward to management responsible for disclosure. As a result, multiple cybersecurity issues that had the potential to materially impact SolarWinds, but which SolarWinds determined at the time did not yet impact multiple customers, went unreported. This included (1) the VPN vulnerability that could allow an attacker to access SolarWinds' network undetected; (2) attacks against U.S. Government Agency A and Cybersecurity Firm B (which were inappropriately treated separately even though Brown and the InfoSec team had linked them); and (3) following discovery of the SUNBURST incident, the fact that the vulnerability inserted by the attackers had been previously exploited on multiple occasions.

FIRST CLAIM FOR RELIEF
Violations of Section 17(a) of the Securities Act
(*Against SolarWinds and Brown*)

203. All of the foregoing paragraphs are incorporated by reference herein.

204. Defendants SolarWinds and Brown, by engaging in the conduct above, singly or in concert with others, in the offer or sale of securities, by the use of means or instruments of transportation or communication in interstate commerce or by use of the mails, directly or indirectly:

(a) while acting knowingly or recklessly, employed devices, schemes, or artifices to defraud;

(b) while acting knowingly, recklessly, or negligently, obtained money or property by means of untrue statements of a material fact or by omitting 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; and

(c) while acting knowingly, recklessly, or negligently, engaged in transactions, practices, or courses of business which operated or would operate as a fraud or deceit upon the purchasers of SolarWinds stock.

205. By engaging in the foregoing conduct, Defendants SolarWinds and Brown violated, and unless restrained and enjoined will continue to violate, Section 17(a) of the Securities Act [15 U.S.C. § 77q(a)].

SECOND CLAIM FOR RELIEF
Aiding and Abetting Violations of Section 17(a) of the Securities Act
(Against Brown)

206. All of the foregoing paragraphs are incorporated by reference herein.

207. As alleged above, Defendant SolarWinds violated Section 17(a) of the Securities Act [15 U.S.C. § 77q(a)].

208. Through his false statements, false sub-certifications, and other means alleged above, Defendant Brown knowingly provided substantial assistance to, and thereby aided and abetted, SolarWinds' violations of the securities laws.

209. By engaging in the foregoing conduct, pursuant to Securities Act Section 15(b) [15 U.S.C. § 77o], Defendant Brown violated Securities Act Section 17(a) [15 U.S.C. § 77q(a)].

THIRD CLAIM FOR RELIEF
Violations of Section 10(b) of the Exchange Act and Rule 10b-5(b) Thereunder
(*Against SolarWinds and Brown*)

210. All of the foregoing paragraphs are incorporated by reference herein.

211. By engaging in the conduct described above, Defendants SolarWinds and Brown directly or indirectly, singly or in concert with others, in connection with the purchase or sale of a security and by the use of means or instrumentalities of interstate commerce, or the mails, or of the facilities of a national securities exchange, with scienter:

(a) employed devices, schemes, or artifices to defraud;

(b) made one or more untrue statements of a material fact or omitted to state one or more material facts necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading; and

(c) engaged in acts, practices or courses of business which operated or would operate as a fraud or deceit upon the purchasers of SolarWinds stock, and other persons.

212. By engaging in the foregoing conduct, Defendants SolarWinds and Brown violated, and unless restrained and enjoined will continue to violate, Section 10(b) of the Exchange Act [15 U.S.C. § 78j(b)] and Rule 10b-5 thereunder [17 C.F.R. § 240.10b-5].

FOURTH CLAIM FOR RELIEF
Aiding and Abetting Violations of Exchange Act 10(b) and Rule 10b-5 Thereunder
(Against Brown)

213. All of the foregoing paragraphs are incorporated by reference herein.

214. As alleged above, Defendant SolarWinds violated Exchange Act Section 10(b) [15 U.S.C. § 78j(b)] and Rule 10b-5 thereunder [17 C.F.R. § 240.10b-5].

215. Through his false statements, false sub-certifications, and other means alleged above, Defendant Brown knowingly provided substantial assistance to, and thereby aided and abetted, SolarWinds' violations of the securities laws.

216. By engaging in the foregoing conduct, pursuant to Exchange Act Section 20(e) [15 U.S.C. § 78t(e)], Defendant Brown violated Exchange Act Section 10(b) [15 U.S.C. § 78j(b)] and Rule 10b-5 thereunder [17 C.F.R. § 240.10b-5].

FIFTH CLAIM FOR RELIEF
Violations of Section 13(a) of the Exchange Act and Exchange Act Rules 12b-20 and 13a-1, 13a-11, and 13a-13 Thereunder (*Against SolarWinds*)

217. All of the foregoing paragraphs are incorporated by reference herein.

218. Section 13(a) of the Exchange Act [15 U.S.C. § 78m(a)] and Rules 13a-1, 13a-11, and 13a-13 thereunder [17 C.F.R. §§ 240.13a-1, 240.13a-11, and 240.13a-13] require issuers of registered securities to file with the SEC factually accurate annual reports (on Form 10-K), quarterly reports (on Form 10-Q), and current reports (on Form 8-K). Exchange Act Rule 12b-20 [17 C.F.R. § 240.12b-20] provides that, 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 light of the circumstances under which they were made, not misleading.

219. By engaging in the foregoing conduct, Defendant SolarWinds violated Section 13(a) of the Exchange Act [15 U.S.C. § 78m(a)] and Rules 12b-20, 13a-1, 13a-11, and 13a-13 thereunder [17 C.F.R. §§ 240.12b-20, 240.13a-1, 240.13a-11, and 240.13a-13].

SIXTH CLAIM FOR RELIEF
Aiding and Abetting Violations of Exchange Act Section 13(a) and Rules 12b-20, 13a-1, 13a-11, and 13a-13
(Against Brown)

220. All of the foregoing paragraphs are incorporated by reference herein.

221. As alleged above, Defendant SolarWinds violated Exchange Act Section 13(a) and Rules 12b-20, 13a-1, 13a-11, and 13a-13.

222. Through his false statements, false sub-certifications, and other means alleged above, Defendant Brown knowingly provided substantial assistance to, and thereby aided and abetted, SolarWinds' violations of the securities laws.

223. By engaging in the foregoing conduct, pursuant to Exchange Act Section 20(e) [15 U.S.C. § 78t], Defendant Brown violated Exchange Act Section 13(a) [15 U.S.C. § 78m(a)] and Rules 12b-20, 13a-1, 13a-11, and 13a-13 [17 C.F.R. §§ 240.12b-20, 240.13a-1, 240.13a-11, and 240.13a-13].

SEVENTH CLAIM FOR RELIEF
Violations of Section 13(b)(2)(B) of the Exchange Act
(*Against SolarWinds*)

224. All of the foregoing paragraphs are incorporated by reference herein.

225. By engaging in the conduct described above, SolarWinds failed to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that SolarWinds' access to assets is permitted only in accordance with management's general or specific authorization, in violation of Exchange Act Section 13(b)(2)(B) [15 U.S.C. § 78m(b)(2)(B)].

226. By reason of the foregoing, SolarWinds violated Exchange Act Section 13(b)(2)(B) [15 U.S.C. § 78m(b)(2)(B)].

EIGHTH CLAIM FOR RELIEF
Aiding and Abetting Violations of 13(b)(2)(B) of the Exchange Act
(*Against Brown*)

227. All of the foregoing paragraphs are incorporated by reference herein.

228. As alleged above, Defendant SolarWinds violated Exchange Act Section 13(b)(2)(B) [15 U.S.C. § 78m(b)(2)(B)].

229. Through his false sub-certifications attesting to the adequacy of SolarWinds' cybersecurity internal controls and other means alleged above, Defendant Brown knowingly provided substantial assistance to, and thereby aided and abetted, SolarWinds' violations of the securities laws.

230. By engaging in the foregoing conduct, pursuant to Exchange Act Section 20(e) [15 U.S.C. § 78t(e)], Defendant Brown violated Section 13(b)(2)(B) of the Exchange Act [15 U.S.C. § 78m(b)(2)(B)].

NINTH CLAIM FOR RELIEF
Violations of Exchange Act Rule 13a-15(a)
(Against SolarWinds)

231. All of the foregoing paragraphs are incorporated by reference herein.

232. Exchange Act Rule 13a-15(a) requires publicly traded companies to maintain disclosure controls and procedures that, as defined in Rule 13a-15(e), "are designed to ensure that information required to be disclosed by the issuer" in reports it files with the SEC "is recorded, processed, summarized and reported" in a timely fashion. And that "[d]isclosure 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." Exchange Act Rule 13a-15(e) [17 C.F.R. § 240.13a-15(e)].

233. By engaging in the foregoing conduct, Defendant SolarWinds violated Exchange Act Rule 13a-15(a) [17 C.F.R. § 240.13a-15(a)].

TENTH CLAIM FOR RELIEF
Aiding and Abetting Violations of Exchange Act Rule 13a-15(a)
(Against Brown)

234. All of the foregoing paragraphs are incorporated by reference herein.

235. As alleged above, Defendant SolarWinds violated Exchange Act Rule 13a-15(a) [17 C.F.R. § 240.13a-15(a)].

236. Through his false statements, false sub-certifications, failure to elevate or disclose the VPN, U.S. Government Agency A, or Cybersecurity Firm B incidents, and other means alleged above, Defendant Brown knowingly provided substantial assistance to, and thereby aided and abetted, SolarWinds' violations of the securities laws.

237. By engaging in the foregoing conduct, pursuant to Exchange Act Section 20(e) [15 U.S.C. § 78t], Defendant Brown violated Exchange Act Rule 13a-15(a) [17 C.F.R. § 240.13a-15(a)].

PRAYER FOR RELIEF

WHEREFORE, the SEC respectfully requests that this Court enter a Final Judgment:

A. Finding that Defendants SolarWinds and Brown committed the violations alleged in this Complaint;

B. Permanently restraining and enjoining Defendants SolarWinds and Brown from violating, directly or indirectly, Section 17(a) of the Securities Act [15 U.S.C. § 77q(a)], Sections 10(b), 13(a) and 13(b)(2)(B) of the Exchange Act [15 U.S.C. §§ 78j(b), 78m(a), 78m(b)(2)(B)], and Rules 10b-5, 12b-20, 13a-1, 13a-11, 13a-13, and 13a-15(a) thereunder [17 C.F.R. §§ 240.10b-5, 240.12b-20, 240.13a-1, 240.13a-11, 240.13a-13, and 240.13a-15(a)];

C. Ordering Defendants SolarWinds and Brown to disgorge all ill-gotten gains they received directly or indirectly as a result of the alleged violations, with pre-judgment interest thereon, pursuant to Exchange Act Sections 21(d)(3), (5), and (7) [15 U.S.C. §§ 78u(d)(3), (5) and (7)];

D. Ordering Defendants SolarWinds and Brown to pay civil monetary penalties pursuant to Section 20(d) of the Securities Act [15 U.S.C. § 77t(d)], and Section 21(d)(3) of the Exchange Act [15 U.S.C. § 78u(d)(3)];

E. Permanently prohibiting Defendant Brown, under Section 20(e) of the Securities Act [15 U.S.C. § 77t(e)] and Section 21(d)(2) of the Exchange Act [15 U.S.C. § 78u(d)(2)], from acting as an officer or director of any issuer that has a class of securities registered under Section 12 of the Exchange Act [15 U.S.C. § 78l] or that is required to file reports under Section 15(d) of the Exchange Act [15 U.S.C. § 78o(d)]; and

F. Granting any other and further relief this Court may deem just and proper.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38, the SEC demands a trial by jury on all issues so triable.

Dated: October 30, 2023

Respectfully submitted,

/s/ Christopher M. Bruckmann

Christopher M. Bruckmann
(SDNY Bar No. CB-7317)
Kristen M. Warden
(*pro hac vice* motion forthcoming)
William B. Ney
(*pro hac vice* motion forthcoming)
Benjamin Brutlag
(SDNY Bar No. BB-1196)
Lory Stone
(*pro hac vice* motion forthcoming)
Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549
202-551-5986 (Bruckmann)
202-551-4661 (Warden)
202-551-5317 (Ney)
202-551-2421 (Brutlag)
202-551-4931 (Stone)
BruckmannC@sec.gov
WardenK@sec.gov
NeyW@sec.gov
BrutlagB@sec.gov
StoneL@sec.gov
Attorneys for Plaintiff Securities and Exchange Commission