EFiled: Nov 04 2021 05:08PM EDT
Transaction ID 67071173
Case No. 2021-0940-SG

IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

CONSTRUCTION INDUSTRY LABORERS PENSION FUND, CENTRAL LABORERS' PENSION FUND, LAWRENCE MILES, and BRIAN SEAVITT, derivatively on behalf of SOLARWINDS CORPORATION, Plaintiffs, vs. MIKE BINGLE, WILLIAM BOCK, SETH BORO, PAUL J. CORMIER, KENNETH Y. HAO, MICHAEL HOFFMANN, DENNIS HOWARD, CATHERINE R. KINNEY, JAMES LINES, EASWARAN SUNDARAM, KEVIN B. THOMPSON, JASON WHITE, MICHAEL WIDMANN, Defendants, and SOLARWINDS CORPORATION, Nominal Defendant.	C.A. No. 2021-_____ **PUBLIC REDACTED VERSION FILED: NOVEMBER 4, 2021**

VERIFIED SHAREHOLDER DERIVATIVE COMPLAINT

Plaintiffs Construction Industry Laborers Pension Fund, Central Laborers' Pension Fund, Lawrence Miles, and Brian Seavitt (collectively, "Plaintiffs"), by and through their undersigned attorneys submit this Verified Shareholder Derivative

Complaint in the name and on behalf of nominal defendant SolarWinds Corporation ("SolarWinds" or the "Company") against the current and former directors of SolarWinds identified below (collectively, "Defendants"). Plaintiffs base the allegations herein on, *inter alia,* actual knowledge as to their own acts; the Company's public statements, press releases, and public filings with the United States Securities and Exchange Commission ("SEC"); documents produced by the Company pursuant to 8 *Del. C.* §220 (the "220 Production"); news reports and other publicly available information; and on information and belief as to all other allegations after due investigation by counsel.

SUMMARY OF THE ACTION

1. This action asserts derivative claims on behalf of SolarWinds against current and former members of the Company's board of directors (the "Board"), for their utter failure to implement or oversee any reasonable monitoring system concerning [redacted] cybersecurity risks fundamental to SolarWinds' only line of business. [redacted]

[redacted] These failures led to one of the most devastating cyberattacks against the United States in history.

2. SolarWinds is a monoline provider of information technology ("IT") infrastructure management software. The Company derives all of its revenues from sales of its proprietary software to government agencies, businesses, and other entities that use SolarWinds' products to manage, monitor, and control their IT environments. SolarWinds' software – particularly its flagship "Orion Platform" ("Orion") – is virtually ubiquitous in business and government in the United States and globally, with the Company's approximately 300,000 clients including almost all of the Fortune 500 and multiple government agencies, including the U.S. Departments of Defense, State, Treasury, Justice, Energy, and Homeland Security.

3. SolarWinds' software depends on trusted access to its clients' IT systems. This access makes SolarWinds a uniquely valuable target for hackers and subjects the Company to a profound and heightened risk of a so-called software "supply chain" cyberattack – *i.e.*, a common technique in which hackers gain access to their intended targets through trusted third-party software. According to the

Cybersecurity and Infrastructure Security Agency ("CISA")[1], "[t]o provide SolarWinds Orion with the necessary visibility . . . it is common for network administrators to configure SolarWinds Orion with pervasive privileges, making it a valuable target for adversary activity." In other words, SolarWinds is an attractive target for cyberattacks because hackers can use the Company's software to gain privileged access to SolarWinds' clients' systems.

4. That is exactly what happened in this case. In December 2020, SolarWinds announced that it had learned of a massive cybersecurity incident – dubbed "SUNBURST" – impacting up to 18,000 of its clients, including numerous U.S. national security agencies and leading technology companies. In simple terms, Russian hackers used SolarWinds' software as a "Trojan horse" to attack the Company's clients by hiding malicious code in SolarWinds' Orion software and exploiting its trusted access to gain entry to the Company's clients' systems. When SolarWinds' clients conducted routine software updates, they unknowingly brought this malware into their IT systems.

---

[1] CISA is an operational arm of the Department of Homeland Security ("DHS") and the leading federal agency focused on the security, resiliency, and reliability of America's cybersecurity and communications infrastructure.

5. [redacted]

6. These warnings underscored the specific and heightened risk from supply chain cyberattacks that was (or should have been) apparent to any fiduciary reasonably familiar with SolarWinds' business. In July 2018, the Office of the Director of National Intelligence ("ODNI") described 2017 as a "watershed in the reporting of software supply chain operations" and warned that "[a]s the number of events grows, so too are the potential impacts. Hackers are clearly targeting software

---

[2] All emphasis is added unless otherwise noted.

supply chains[.]" In October 2018 – just weeks before SolarWinds went public – CISA warned that "APT [("advanced persistent threat")] actors are conducting malicious activity against organizations that have trusted network relationships with potential targets."

7. Private sector cybersecurity experts were likewise warning about the increasing danger of supply chain cyberattacks. For example, in February 2019, cybersecurity company Symantec Corporation ("Symantec") issued a report titled "Internet Security Threat Report, Volume 24" ("ISTR 24"), which found that "supply chain attacks" had "increas[ed] by 78% in 2018" and warned that attackers were "increasingly arriving through trusted channels" and "hijacking software updates and injecting malicious code into legitimate software." Symantec's website provided an overview of ISTR 24 the following month in an article titled "Cyber Criminals Ramp Up Attacks on Trusted Software and Supply Chains," which explained that "[t]rusted, widely used software tools and supply chains present cyber criminals and other bad actors with almost irresistible attack avenues." [redacted]

8. [redacted]

9. [redacted]

10. [redacted]

[redacted]

11. These oversight failures had grave consequences for SolarWinds. As is now known, SolarWinds suffered from internal cybersecurity deficiencies that defied elementary cybersecurity standards for any modern company, let alone one with a heightened risk of a cyberattack due to its trusted access to thousands of sensitive networks, including multiple critical agencies of the U.S. government. The Company's poor password controls are a striking example. In 2019, prominent "malware hunter" Vinoth Kumar warned the Company that the obvious and ineffectual password "solarwinds123" for the Company's software download

website was available on the internet along with related user credentials. As Mr. Kumar explained at the time in a (later-publicized) email to the Company: "Via this any hacker could upload malicious exe [(*i.e.*, "malware")] and update it with release [of] SolarWinds product." SolarWinds has since acknowledged that "solarwinds123" was a password in use at the Company since 2017.

12. SolarWinds has also acknowledged that password vulnerabilities were among the "most likely candidates for initial entry" of SUNBURST. CISA has likewise concluded that the SUNBURST hackers' principal techniques involved "password guessing[,] password spraying[,] and [using] inappropriately secured administrative credentials [] accessible via external remote access services."

13. SolarWinds' directors had a fiduciary duty to monitor and oversee the Company's known mission critical cybersecurity risks and therefore (at the very least) should have known about and addressed these and other fundamental security deficiencies before SolarWinds became a channel for hackers to invade its clients' IT systems. SolarWinds' directors breached their fiduciary duties by utterly failing to monitor or oversee any aspect of the Company's known mission critical cybersecurity risks.

JURISDICTION

14. This Court has jurisdiction over this action pursuant to 10 *Del. C.* §341.

15. SolarWinds' charter designates the Court of Chancery as the sole and exclusive forum for derivative actions premised upon breaches of fiduciary duties.

16. Each director of SolarWinds' Board has consented to this Court's jurisdiction pursuant to 10 *Del. C.* §3114(a).

17. Officers of SolarWinds have consented to this Court's jurisdiction pursuant to 10 *Del. C.* §3114(b).

PARTIES

A. Plaintiffs

18. Plaintiffs are currently SolarWinds stockholders, purchased SolarWinds shares during the relevant period, and have held shares continuously since that time.

B. Nominal Defendant

19. Nominal Defendant SolarWinds is a Delaware corporation with its principal executive offices located at 7171 Southwest Parkway, Building 400, Austin, Texas 78735. The Company's shares trade on the New York Stock Exchange ("NYSE") under the ticker symbol "SWI." SolarWinds' registered agent in Delaware is The Corporation Trust Company, located at Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801.

C. Director Defendants

20. Defendant Mike Bingle ("Bingle") served as a director from February 2016 until May 2021, and as a member of the Board's NGC from October 2018 until May 2021. Bingle is currently a managing partner and managing director of Silver Lake, a private equity firm which he joined in 2000. Bingle also serves and has served on boards of directors of numerous businesses offering IT advisory services; point-of-sale transaction processing; electronic trading and analytics; online finance, retail, and brokerage services; and prepaid gift cards services; including, Ancestry.com LLC, Blackhawk Network Holdings, Inc., TD Ameritrade Holding Corp., Gartner, Inc., Fanatics, Inc., and Social Finance, Inc. ("Sofi").

21. Defendant William Bock ("Bock") has served as a director since October 2018, and as chair of the Board's Audit Committee since October 2018. Bock became Chair of the Board in August 2020. Bock has also served as a director since 2011 at SailPoint Technologies ("SailPoint"), a software developer that specializes in cybersecurity, and as chair of that company's board since 2018. He also currently serves and has served on the boards of directors of numerous public and private businesses that develop and manufacture computers and software, as well as e-commerce companies, including Convio and Entropic Communications. Bock was president of Silicon Labs, a global technology company that develops

software, from 2013 to 2016, and chief financial officer and senior vice president of Silicon Labs from 2006 to 2011. Before that Bock held senior executive positions in companies that develop and manufacture computers and IT management software, including Dazel Corporation, Tivoli Systems, and Convex Computer Corporation. He started his career at the technology company Texas Instruments and holds a B.S. in computer science from Iowa State University and an M.S. in industrial administration from Carnegie Mellon University.

22. Defendant Seth Boro ("Boro") has served as a director since February 2016. Boro has been a managing partner at the private equity firm Thoma Bravo since 2013 and was a principal with Thoma Bravo at its founding in 2007. Boro serves and has served on the boards of directors of numerous cybersecurity firms, and companies that develop and manufacture IT management software, including McAfee, Inc., SailPoint, ConnectWise, Inc., Barracuda Networks, Inc., Riverbed Technology, Inc., Hyland Software, Inc., Qlik Technologies, Inc., LogRhythm, Inc., Veracode, Inc., Blue Coat Systems, Inc., DigiCert, Inc., and Compuware Corporation, among others.

23. Defendant Paul J. Cormier ("Cormier") served as a director from July 2014 until February 2016, and then again from October 2018 until September 2020. He served as a member of the Board's Audit Committee from October 2018 until

February 2020, and as a member of the Board's NGC from October 2018 until September 2020. Cormier has also held senior executive positions at leading cybersecurity firms, web portal and internet services businesses, and companies that develop IT management software, including Netect Internet Software Company, AltaVista Internet Software, Inc., and BindView Development Corporation. He has served as executive vice president since 2011, and president since 2008, at Red Hat, Inc., a leading provider of enterprise open source IT management software. He has also served on boards of directors of other open source companies that develop software and cloud management tools, including Hortonworks, Inc. since 2011, and Cloudera, Inc. since 2019. Cormier has an M.S. in software development and management from the Rochester Institute of Technology.

24. Defendant Kenneth Y. Hao ("Hao") has served as a director since February 2016. Hao is currently chairman and a managing partner of Silver Lake, which he joined in 2000. Hao also currently serves and has served on boards of directors of leading cybersecurity firms and companies that develop IT management software and computer hardware, including SMART Global Holdings, Inc., NortonLifeLock, Inc. (formerly Symantec Corporation), ServiceMax, Inc., Broadcom, Inc., and NetScout Systems, Inc.

25. Defendant Michael Hoffmann ("Hoffmann") has served as a director since October 2018. Hoffmann is a principal at Thoma Bravo, which he joined in 2014. Hoffmann also serves on the boards of directors of leading businesses that develop IT management software, including ConnectWise, LLC, Riverbed Technology, Inc., and Empirix, Inc.

26. Defendant Dennis Howard ("Howard") has served as a director and member of the Board's Audit Committee since September 2020. Howard has been a senior executive and chief information officer at various companies, including the financial services firm Charles Schwab & Co., Inc. since 2016, and the cloud service provider Core Technology Services from 2014 until 2016. Howard also previously worked in the technology department at Commerce One, Inc., an e-commerce company that connected businesses to their suppliers, and served in numerous departments at Visa, including data analytics and client-facing product development, from in or around 2002 until in or around 2014.

27. Defendant Catherine R. Kinney ("Kinney") has served as a director since October 2018. She has served as chair of the Board's NGC since October 2018 and as a member of the Board's Audit Committee since in or around February 2019. Kinney currently serves and has served on boards of directors of insurance, mega-data center, financial analytics, and cloud software development companies,

including NetSuite, Inc., MetLife, Inc., MSCI, Inc., and Quality Technology Services (QTS) Realty Trust, Inc. Prior to SolarWinds, she had worked for the NYSE since 1974 in various management positions, including in trading floor operations and technology from 1987 to 1996, and as president and co-chief operating officer for NYSE Euronext from 2002 to 2008. She retired from NYSE Euronext in March 2009.

28. Defendant James Lines ("Lines") has served as a director since February 2016, and served as a member of the Board's Audit Committee from October 2018 until October 2019. Lines has been an operating partner at Thoma Bravo since 2002 and is currently a senior operating partner at that firm. Lines also currently serves and has served on the boards of directors of numerous companies that develop IT management software, including Riverbed Technology, Inc., Hyland Software, Inc., Qlik Technologies, Inc., Compuware Corporation, Dynatrace, LLC, Imprivata, Inc., ABC Financial Services, Inc., and SIGOS, LLC, among others.

29. Defendant Easwaran Sundaram ("Sundaram") has served as a director since February 2020, and as a member of both the Board's Audit Committee since February 2020 and NGC since September 2020. Sundaram has been the chief digital and technology officer and executive vice president of JetBlue Airways Corporation since 2017, and previously served as JetBlue's executive vice president of

innovation and chief information officer from 2012 until 2017. Sundaram also serves on the board of directors of the multinational IT and telecommunications company Société Internationale de Télécommunications Aéronautiques ("SITA"), and the electrical distribution services company WESCO International, Inc. He has also served in executive roles at McKesson Corporation, which (among other things) provides IT to health care facilities, and the chemical filtration and purification company Pall Corporation.

30. Defendant Kevin B. Thompson ("Thompson") served as a SolarWinds director from February 2016 until his resignation on December 7, 2020. Thompson was the Chief Executive Officer ("CEO") of SolarWinds from March 2010 until December 2020. Days after Thompson tendered his resignation because the Board had hired a new CEO, the Board purportedly learned of the SUNBURST attack. Instead of taking any steps to hold Defendant Thompson liable for his contributing role as CEO and as a fellow director for his fiduciary failures, the Board rehired Thompson in a lucrative role as a purported consultant, and provided him with a release for all of his actions or omissions while serving as the Company's CEO and Board member. Prior to joining SolarWinds, Thompson was chief financial officer of leading software developers Red Hat, Inc., Surgient, Inc., and the SAS Institute. Thompson has also served on the boards of directors of a cybersecurity firm and

various companies that develop software, including NetSuite, Inc. and Barracuda Networks, Inc., among others.

31. Defendant Jason White ("White") served as a director from February 2016 until his resignation in February 2020, and as a member of the Board's Audit Committee from October 2018 until January 2019. White is a managing director of Silver Lake, which he joined in 2006. He also currently serves as a director at Ancestry.com LLC, the prepaid gift card seller Blackhawk Network Holdings, Inc., and the computer hardware developer and manufacturer SMART Global Holdings, Inc.

32. Defendant Michael Widmann ("Widmann") has served as a director since February 2020. Widmann also serves as a director at Silver Lake, which he joined in 2011. Prior to joining Silver Lake, he worked in the Technology Investment Banking Group at Credit Suisse.

SUBSTANTIVE ALLEGATIONS

I. SolarWinds' Business

33. SolarWinds is a monoline company that produces and markets IT infrastructure management software. All of the Company's revenue comes from

sales of its software products.[3] SolarWinds' products are primarily tailored for software developers, in-house IT operations managers, and managed services providers ("MSPs"), *i.e.*, firms providing IT operations management as a service, typically to small and medium-sized business. As of December 31, 2019, the Company had over 320,000 customers in 190 countries, including 499 of the Fortune 500, major U.S. technology companies such as Intel and Microsoft, all of the top ten U.S. telecommunications companies, all of the top five U.S. accounting firms, and hundreds of hospitals and universities. SolarWinds has also procured over $230 million in government contracts, and its products are used by the federal government's core security agencies, including all five branches of the U.S. military, the Federal Bureau of Investigation ("FBI"), DHS, Pentagon, Secret Service, National Security Agency ("NSA"), National Aeronautics and Space Administration, National Nuclear Security Administration (which safeguards America's nuclear weapons stockpile), and the Defense, State, Treasury, Justice, and Energy Departments.

---

[3] Specifically, SolarWinds generates revenue through a combination of "license" revenue derived from sales of perpetual licenses of its software products, and "recurring" revenue derived from subscription and maintenance fees charged for its "software as a service" products.

34. The Company's flagship software is the Orion Platform (previously defined as "Orion"). Orion is a network management software suite that, as described by SolarWinds, provides "[c]entralized monitoring and management of your entire IT stack, from infrastructure to application." With Orion, customers can monitor and manage three core IT areas: "network products," "IT operations products," and "security products." A former NSA hacking expert stated that Orion "was the first software of its kind" and that "Orion is to network management systems what Kleenex is to tissue" because it was "the first actually easy-to-use network management system." Orion has over 33,000 users in varied industries and sectors. Sales from Orion accounted for roughly 45% of SolarWinds total revenue, or approximately $343 million, for the nine months ended September 30, 2020.

35. To perform its core functions, Orion requires trusted access with full administrative privileges to users' IT systems. This means that Orion enters highly privileged accounts and locations on users' computer networks, and that anyone who accesses Orion can alter, delete, or exfiltrate (*i.e.*, steal) vital files and applications, reboot or disable connected IT, and engage in "lateral movement" across the network. Attackers use lateral movement to "progress from the original foothold [and] find valuable information, get access to business-critical systems or execute an attack" – and "exploiting privileged access is the way to facilitate this

movement."[4] Indeed, SolarWinds identified "trust among technology professionals" as a leading factor that had "enabled [SolarWinds] to increase [its] customer base" in the Company's 2018 and 2019 Form 10-Ks.

36. The Company was founded in 1999 and went public in May 2009 through an IPO, after which it was traded for nearly seven years on the NYSE. In February 2016, two private equity firms that specialize in acquiring software companies – Silver Lake and Thoma Bravo – took SolarWinds private through a $4.5 billion purchase of the Company. Less than three years later, SolarWinds went public again in October 2018 through its second IPO.

37. Between October 2018 and December 2020, three executives from Thoma Bravo (Defendant Directors Boro, Hoffmann, and Lines) and four executives from Silver Lake (Defendant Directors Bingle, Hao, White, and Widmann) served on the Company's Board. Thoma Bravo and Silver Lake each owned 41.4% (82.8% together) of SolarWinds' outstanding common stock following the Company's October 2018 IPO and through at least October 31, 2020.

---

[4] Lavi Lazarovitz, *Stop the Cyber-Attack Cycle with Privileged Access Management*, INFOSECURITY (Aug. 21, 2020), https://www.infosecurity-magazine.com/blogs/stop-cyberattack-privileged-access/.

II. SolarWinds' Board Knew About the Company's Mission Critical Cybersecurity Risks

38. SolarWinds' Board knew about the mission critical cybersecurity risks facing the Company, including because: [redacted]; (ii) from 2017 to 2020, numerous widely publicized reports from prominent public and private cybersecurity organizations warned that supply chain cyberattacks were increasing in prevalence and severity and that companies with trusted access to third-parties' IT were key targets for these operations; and (iii) in 2018, the SEC imposed on boards of directors disclosure and oversight obligations concerning cybersecurity risks, the Company's SEC filings acknowledged these risks and the need to monitor them, and the NYSE's cybersecurity guidelines for directors issued in 2015 likewise recognized directors' critical cybersecurity monitoring obligations.

(a) [redacted]

39. [redacted]

40. [redacted]

[redacted] As CISA explained in an alert in October 2018,[5] attackers conduct "malicious activity against organizations that have ***trusted network relationships with . . . a parent company, a connected partner, or a contracted managed service provider (MSP)***" in order to "***access other devices and other trusted networks.***" [redacted]

41. [redacted]

[5] Discussed further in section II.B, *infra*.

42. [redacted]

[redacted]

43. [redacted]

(b) The Heightened Risk of Supply Chain Cyberattacks Was Well Publicized Both Before and After [redacted]

44. [redacted] at a time when prominent outside actors – such as major U.S. cybersecurity and national security agencies and leading cybersecurity firms – were publicly warning about the significant and increasing threat of supply chain cyberattacks. For example, [redacted], the National Institute of Standards and Technology ("NIST") highlighted the importance of proper supply chain risk management, and the ODNI and CISA warned about the growing danger of supply chain cyberattacks.

45. In April 2018, NIST updated its Cybersecurity Framework[6] (the "Framework") to include a "[g]reatly expanded explanation of using [the] Framework for Cyber Supply Chain Risk Management purposes." The updated Framework explained that "supply chain risk management (SCRM) is a critical organizational function" and included the below figure depicting "Cyber Supply Chain Relationships" to "highlight ***the crucial role of cyber SCRM in addressing cybersecurity risk in critical infrastructure and the broader digital economy***":

[6] NIST's Cybersecurity Framework was first issued in February 2014 and was developed to "improve cybersecurity risk management in critical infrastructure" but "can be used by organizations in any sector or community." The Framework has been downloaded over half a million times and is widely used within the private sector. Use of the Framework became mandatory for all U.S. federal agencies through a 2017 Presidential Executive Order.

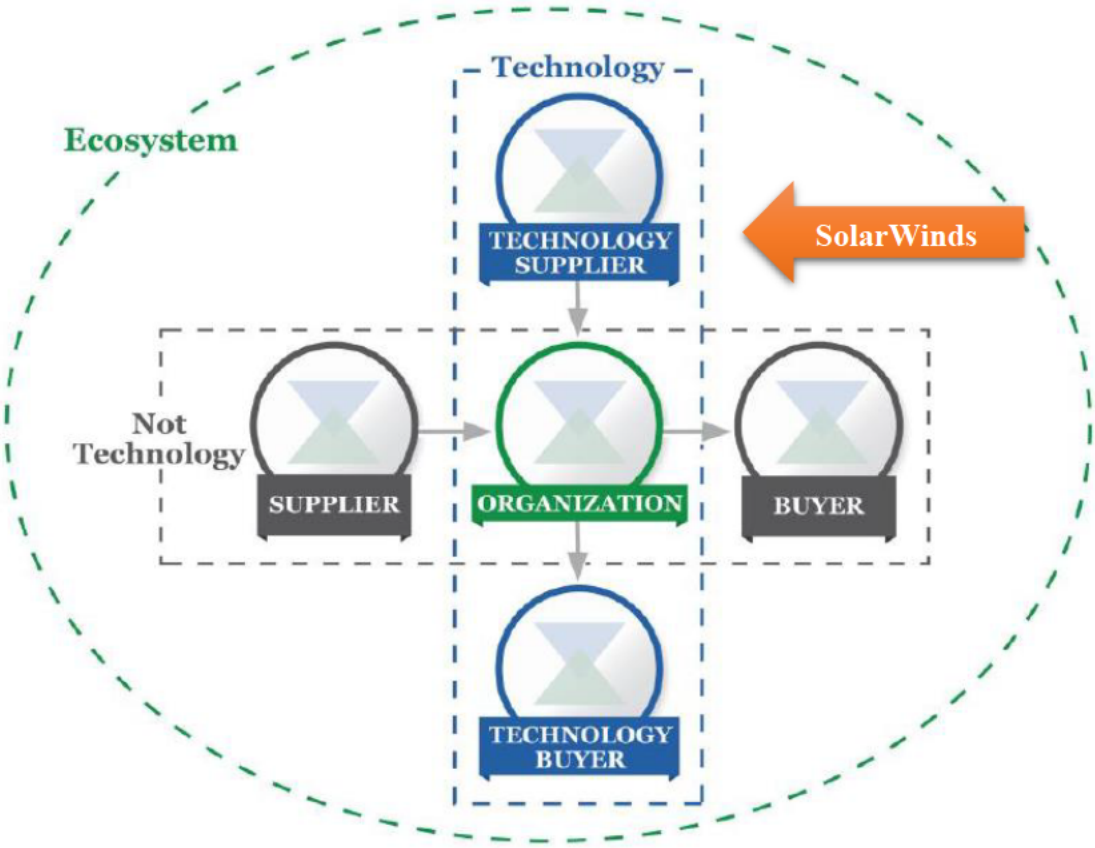


Figure 3: Cyber Supply Chain Relationships

46. SolarWinds is the "Technology Supplier" in this figure[7]; as the Framework explains: the "'[Technology] Supplier' encompasses upstream product and service providers that are used for an organization's internal purposes (***e.g., IT infrastructure***)" and the "'Buyer' refers to the downstream people or organizations that consume a given product or service from an organization." The Framework

---

[7] The "SolarWinds" text and arrow were added to the figure and are not in the original.

stressed that "[t]hese relationships" and "the products and services they provide, and the risks they present should be identified and factored into the protective and detective capabilities of organizations[.]"

47. Then in July 2018, the ODNI issued a report titled "Foreign Economic Espionage in Cyberspace." This report "discusse[d] several potentially disruptive threat trends that warrant close attention," the first of which was "[s]oftware supply chain infiltration." The report alerted that supply chain cyberattacks had increased in 2017 and that software supply chains were particularly vulnerable:

> ***Last year represented a watershed in the reporting of software supply chain operations.*** In 2017, seven significant events were reported in the public domain compared to only four between 2014 and 2016. . . . ***Hackers are clearly targeting software supply chains*** to achieve a range of potential effects to include cyber espionage, organizational disruption, or demonstrable financial impact[.]

48. In October 2018 (the month SolarWinds conducted its IPO), CISA issued an "Alert" on its "National Cyber Awareness System" webpage – a free subscription service that provides, *inter alia*, "timely information about current security issues, vulnerabilities, and exploits" – titled "Using Rigorous Credential Control to Mitigate Trusted Network Exploitation." This alert warned of supply chain-type cyberattacks and was explicitly intended for companies, such as SolarWinds, that have "trusted network relationships." Specifically, the alert warned:

> APT [advanced persistent threat] actors are conducting malicious activity against organizations that have ***trusted network relationships with potential targets, such as a parent company, a connected partner, or a contracted managed service provider (MSP).*** APT actors can use legitimate credentials to expand unauthorized access, maintain persistence, exfiltrate data, and conduct other operations, while appearing to be authorized users. ***Leveraging legitimate credentials to exploit trusted network relationships also allows APT actors to access other devices and other trusted networks, which affords intrusions a high level of persistence and stealth.***

49. Thus, prominent public and private cybersecurity organizations were issuing public alerts about the increasing threat of supply chain cyberattacks many months before [redacted]. These warnings continued unabated from 2019 through 2020 – any board of directors acting in good faith would have taken heed.

50. For example, [redacted], Symantec[8] – whose reports are widely cited by NIST and CISA[9] – issued its annual threat report for 2019, which is

---

[8] Symantec Corporation changed its corporate name to NortonLifeLock Inc. in November 2019.

[9] *See* Key Practices in Cyber Supply Chain Risk Management: Observations from Industry, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8276-draft.pdf; Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report, Status Update on Activities and Objectives of the Task Force (September 2019), https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20

titled "Internet Security Threat Report, Volume 24" (previously defined as "ISTR 24"). This report alerted readers that supply chain attacks had "increas[ed] by 78 percent in 2018" and that attackers were "increasingly arriving through trusted channels" and "hijacking software updates and injecting malicious code into legitimate software." Symantec's website provided an overview of ISTR 24 the following month (March 2019) in an article titled "ISTR 2019: Cyber Criminals Ramp Up Attacks on Trusted Software and Supply Chains," which explained that "[t]rusted, widely used software tools and supply chains present cyber criminals and other bad actors with almost irresistible attack avenues."

51. [redacted] Defendant Hao has also sat on Symantec's board of directors since March 2016.

52. Months later in April 2019, another leading cybersecurity company whose reports are routinely referenced by NIST[10] – Carbon Black, Inc. – issued its "Global Incident Response Threat Report" and titled it "The Ominous Rise of 'Island

---

Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf.

10 *See id.*

Hopping'[;] Advanced Cyberattacks Are Evolving as Attackers Target Supply Chains and Battle Back Against Cybersecurity Teams." "Island hopping" is another name for a supply chain cyberattack. As the report's opening pages explained: "[e]xactly half (50%) of today's attacks leverage 'island hopping.' This means that attackers are after not only your network but all those along your supply chain as well." The rise in "island hopping" (*i.e.*, supply chain cyberattacks) was listed as number one of the report's five "Key Findings."

53. In July 2019, one of America's leading technology media companies, WIRED, published an article titled "The Biggest Cybersecurity Crises of 2019 So Far[;] Ransomware attacks, ***supply chain hacks***, escalating tensions with Iran—the first six months of 2019 have been anything but boring." Similar to the ISTR 24, the WIRED article foreshadowed the SUNBURST incident at SolarWinds, stating that "[a] legitimate software vendor pushes out what looks like a trustworthy software update to users, but it's really a destructive instrument of cyberwar. That is the evil genius of the supply chain attack . . . [which] has been a *particular* signature of 2019 so far." (emphasis in original).

54. Publicity concerning the rising threat of supply chain attacks continued through the end of 2019 and into 2020. In September 2019, CISA's Information and

Communications Technology ("ICT") Supply Chain Risk Management Task Force[11] released its "Interim Report" and cited a May 2019 Presidential Executive Order that "[r]ecogniz[ed] a 'catastrophic' impact stemming from sustained ICT supply chain threats" and echoed the findings from Symantec's ISTR 24, stating that "[a] 2018 Symantec report detailed that the number of observed supply chain attacks was 78 percent higher in 2018 than it was in 2017, as malicious actors sought to exploit vulnerabilities in third-party software[.]"

55. In February 2020, NIST released a report titled "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry" which warned that "[m]any of the recent cyber breaches have been linked to supply chain risks." The report again foreshadowed the SUNBURST hack, stating that "a recent high-profile attack" involved "***compromised software [that] was served to users through the manufacturer's official website***" and that this attack was "reminiscent of" a 2013

---

[11] This task force was formed in October 2018 and chartered "with the express purpose of advising the government and private sector critical infrastructure owners and operators on means for assessing and managing risks associated with the ICT supply chain." *See Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report, Status Update on Activities and Objectives of the Task Force*, CISA (September 2019), https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf.

cyberattack in which a "group successfully inserted malware into software that was available for download through the manufacturers' websites."

56. One month later (March 2020) the FBI's Cyber Division issued a "Flash" alert warning of malware that was specifically targeting software supply chains. The report noted: "***Software supply chain companies are believed to be targeted in order to gain access to the victim's strategic partners and/or customers[.]***" The FBI's Cyber Division re-issued that alert the same month (March 2020) in a "Private Industry Notification" and explained that malware was targeting hospitals and using software supply chain vendors as a conduit: "The FBI assesses [malware] actors gained access to a large number of global hospitals ***through vendor software supply chain*** and hardware ***products***."

57. In sum, [redacted], any fiduciary reasonably familiar with SolarWinds' monoline business must have known that leading cybersecurity organizations in the public and private sectors were widely publicizing the catastrophic and surging risks that supply chain cyberattacks posed for SolarWinds.

(c) Affirmative Regulatory Requirements, the Company's SEC Filings, and Stock Exchange Guidelines Further Underscore Directors' Oversight Obligations Concerning Mission Critical Cybersecurity Risks at SolarWinds

58. The Board's failure to monitor or oversee any aspect of the Company's cybersecurity risk exposure [redacted] also took place in the context of affirmative SEC regulatory guidance imposing cybersecurity oversight and disclosure obligations on boards of directors.

59. In response to the enormous rise in cyberattacks on American companies, and months after the massive NotPetya supply chain attack and Equifax hack were publicized,[12] the SEC unanimously approved and issued new interpretive guidance in February 2018 to "reinforc[e] and expand[] upon the staff's 2011 guidance" concerning cybersecurity (the "2018 Cybersecurity Release").[13] As the

---

[12] The NotPetya malware infected government entities and approximately 600 companies in over 65 countries, including American pharmaceutical company Merck & Co., the multinational law firm DLA Piper, FedEx, and the Danish shipping company Maersk. NotPetya has cost Merck, FedEx, and Maersk at least $300 million *each*. Equifax announced in September 2017 that hackers had stolen nearly 148 million customers' personally identifiable information (*i.e.*, social security numbers, birth dates, and addresses) and over 200,000 customers' credit card data. The attack has cost Equifax over $1.7 *billion* to date.

[13] In October 2011, the SEC's Division of Corporation Finance issued the Commission's first guidance on disclosure obligations concerning cybersecurity

guidance states, "[t]his interpretive release outlines the Commission's views with respect to cybersecurity disclosure requirements under the federal securities laws as they apply to public operating companies." The SEC release stresses that "[c]ompanies are required to establish and maintain appropriate and effective disclosure controls and procedures[,] ***including those related to cybersecurity***" and places this obligation on boards of directors, stating:

> [T]he Commission believes that the development of effective disclosure controls and procedures ***is best achieved when a company's directors . . . are informed about the cybersecurity risks and incidents that the company has faced or is likely to face.***

60. The SEC's 2018 Cybersecurity Release expressly requires public companies to include "a description ***of how the board administers its risk oversight function***." For companies like SolarWinds, where cybersecurity risks are "material to [the] company's business," these guidelines require additional disclosures concerning (i) "***the nature of the board's role in overseeing the management of that risk***"; (ii) "***how the board of directors engages with management on***

---

risks and incidents. The guidance explained that "material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures" not misleading, and that "as with other operational and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents." After this guidance was issued, many companies included additional cybersecurity disclosures in their SEC filings, typically in the form of risk factors.

cybersecurity issues"; and (iii) the "company's cybersecurity risk management program." As the 2018 Cybersecurity Guidelines explain, these more detailed disclosures "allow investors to assess how ***a board of directors is discharging its risk oversight responsibility in this increasingly important area.***"

61. The Board's failure to monitor cybersecurity risk thus took place against a backdrop of increasing positive legal requirements promulgated by the SEC that reflect the mission critical nature of cybersecurity oversight, particularly for a company like SolarWinds where material cybersecurity risks are fundamental to its business.

62. SolarWinds' SEC filings further underscore the mission critical nature of the Company's cybersecurity risks and the Board's obligation to monitor and oversee these risks. For example, in its September 21, 2018 IPO prospectus SolarWinds stated:

> ***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.***
>
> * * *
>
> ***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.

63. The Company's annual proxy filings for 2019 and 2020 (the only proxy filings between the IPO and the SUNBURST incident) acknowledged the Board's oversight obligation concerning these cybersecurity risks, stating that "[o]ur nominating and corporate governance committee also monitors and assesses the effectiveness of our corporate governance guidelines and our policies, plans and programs relating to cyber and data security[.]" As detailed below, despite recognizing this mission critical oversight responsibility and claiming the NGC monitored the company's cyber and data security, [redacted]

[redacted].

64. The NYSE – where SolarWinds trades – has also issued detailed cybersecurity guidelines emphasizing the critical role that corporate directors play in cybersecurity oversight. In October 2015 [redacted] the NYSE issued a 355-page "groundbreaking, practical guide to cybersecurity . . . developed to reflect a body of knowledge that is unsurpassed on this topic" titled "Navigating the Digital Age: ***The Definitive Cybersecurity Guide for Directors and Officers***" (the "Cybersecurity Guide").[14] This guide is one of the most comprehensive resources on cybersecurity for directors and officers anywhere. Its content spans a variety of topics specifically tailored for boards of directors and corporate executives, and includes such chapters as "Cyber risk and the board of directors," "Cyber risk corporate structure," and "Cybersecurity beyond your network" (which addresses supply chain attacks), among others.

---

[14] *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers*, NEW YORK STOCK EXCHANGE (October 2015), https://www.securityroundtable.org/wp-content/uploads/2015/09/Cybersecurity-9780996498203-no_marks.pdf.

65. The NYSE Cybersecurity Guide confirms in clear terms the mission critical nature of corporate directors' cybersecurity oversight obligations. The guide identifies "several elements that we have found to be critical to ensuring an effective security program," including that: "***Active, hands-on engagement by the executive team and the board is required. The risk is existential. Nothing is more important.***"

66. In a section titled "The Risks to Boards of Directors and Board Member Obligations," the Cybersecurity Guide further underscores the important role boards of directors play in overseeing their companies' cybersecurity. This section explains that "[t]houghtful, well-planned ***director involvement in cybersecurity oversight***" is a "critical part of a comprehensive [cybersecurity] program," and goes on to detail the specific steps boards can take to exercise their oversight responsibilities. Such steps include (i) "***devoting board meeting time to presentations from management responsible for cybersecurity and discussions on the subject***," (ii) "directing management to implement a cybersecurity plan" and "***monitoring the effectiveness of such plan*** through internal and/or external controls"; and (iii) "***invest[ing] effort in these actions, on a repeated and consistent basis***, ***and mak[ing] sure that these actions are clearly documented in board and committee packets, minutes, and reports.***"

67. This section further notes that "[b]usiness judgment rule protection is strengthened by ensuring that board members receive periodic briefings on cybersecurity risk" and that "[m]ost importantly, directors cannot recklessly ignore the information they receive."

68. As demonstrated above, [redacted] occurred not only in the context of growing public awareness of the increasing threat posed by supply chain cyberattacks, but also at a time when express SEC guidance imposed affirmative cybersecurity disclosure and oversight obligations on boards of directors, SolarWinds' SEC filings acknowledged these risks and the obligation to monitor them, and the NYSE's seminal guide on cybersecurity emphasized the critical need for corporate directors to engage in "[a]ctive, hands-on" oversight concerning "existential" cybersecurity risks.

III. SolarWinds' Board Utterly Failed to Conduct Any Reasonable Oversight Concerning the Company's Mission Critical Cybersecurity Risks

69. SolarWinds' Board breached their fiduciary duties by failing to exercise any reasonable oversight concerning the Company's mission critical cybersecurity risks. This failure allowed basic cybersecurity deficiencies to develop and persist at the Company, leaving SolarWinds extremely vulnerable to the supply

chain style cyberattack that eventually impacted the Company and infected many of its customers.

70. As fiduciaries to the Company and its stockholders (as well as under express SEC guidance) SolarWinds' Board was obligated to implement and oversee corporate monitoring and reporting systems concerning the Company's mission critical cybersecurity risks. This means that, at a minimum, SolarWinds was obligated to: (i) implement protocols requiring management to keep SolarWinds' Board apprised of cybersecurity compliance practices, risks, and reports, on an ongoing basis; (ii) nominate and appoint directors with appropriate expertise in cybersecurity and technology and regularly educate board members on these matters; (iii) discuss, on a regular basis, any key cybersecurity issues; and (iv) take remedial action when apprised of cybersecurity deficiencies. [redacted]

71. [redacted]

[redacted]

72. Following the Company's IPO, the Board delegated cybersecurity oversight to the Audit Committee. Under SolarWinds' "Corporate Governance Guidelines," the Audit Committee must "oversee[]" all "risk[] associated with . . . data security." The Audit Committee Charter further explains that its members must "[d]iscuss with management the Company's major financial risk exposures, including . . . ***cyber and data security***." [redacted]

73. [redacted]

[redacted]

[redacted]

74. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

75. [redacted]

[redacted]

76. [redacted]

[redacted]

77. [redacted]

78. [redacted]

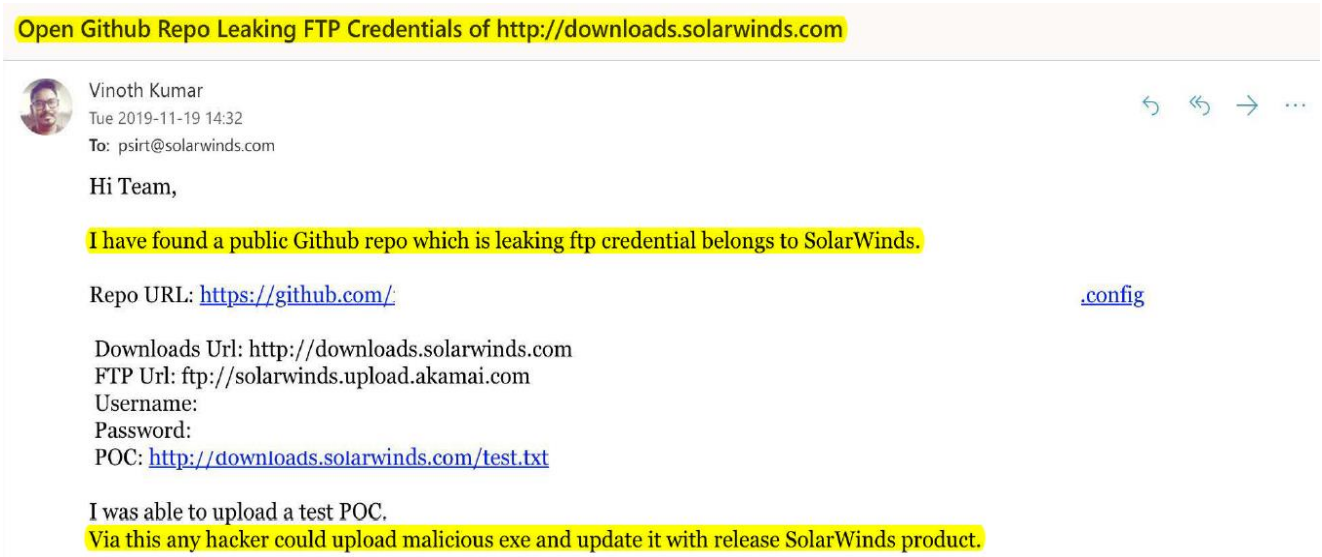
79. By utterly failing to implement or oversee any reasonable monitoring system concerning the Company's cybersecurity risks, SolarWinds' Board disabled itself from being informed of mission critical risks at the Company and breached its fiduciary duties to the Company and its shareholders.

IV. SolarWinds' Cybersecurity Suffered from Gross Deficiencies from 2018 through 2020

80. Serious deficiencies in SolarWinds' cybersecurity developed and persisted at the Company between 2018 and 2020 as a result of the Board's complete failure to oversee known mission critical cybersecurity risks. For example, from the Company's IPO in October 2018 until its disclosure of the SUNBURST hack in December 2020, SolarWinds: (i) used weak passwords for its software download webpages; (ii) did not properly segment its IT network; (iii) directed its clients to disable antivirus scanning and firewall protection on its Orion software; (iv) cut investments in cybersecurity; and (v) listed its sensitive and high-value clients on its webpage for anyone to see. The Company's top technology executives were also alerted about SolarWinds' inadequate cybersecurity from the Company's own Global Cybersecurity Strategist before the IPO in April 2017.

81. In November 2019, cybersecurity expert and prominent "malware hunter" Vinoth Kumar warned SolarWinds' Information Security team through an email that file transfer protocol ("ftp") credentials – *i.e.*, a username and password –

for SolarWinds' software download website were publicly available on the internet (*i.e.*, through a "public Github repo[sitory]"[15]). Kumar showed in his email that, using the ftp credentials, "any hacker could upload malicious exe [*i.e.*, malware]" to the Company's software download website and infect SolarWinds' software and software updates:


Open Github Repo Leaking FTP Credentials of http://downloads.solarwinds.com

Vinoth Kumar
Tue 2019-11-19 14:32
To: psirt@solarwinds.com

Hi Team,

I have found a public Github repo which is leaking ftp credential belongs to SolarWinds.

Repo URL: https://github.com/ .config

Downloads Url: http://downloads.solarwinds.com
FTP Url: ftp://solarwinds.upload.akamai.com
Username:
Password:
POC: http://downloads.solarwinds.com/test.txt

I was able to upload a test POC.
Via this any hacker could upload malicious exe and update it with release SolarWinds product.

82. Kumar posted the above image on his Twitter account in December 2020 immediately following SolarWinds' public disclosure of SUNBURST, and for security purposes, omitted the ftp login password (as noted, the password was publicly available on the Github website in November 2019 when Kumar first

---

15 GitHub is a website that enables software developers and programmers to work collaboratively on writing and refining computer code; the projects on GitHub are examples of "open-source software."

emailed the Company about this deficiency). However, Kumar has disclosed publicly – and numerous SolarWinds executives have acknowledged – that the actual ftp login password was "***solarwinds123***." The Company's current CEO has since confirmed that the "solarwinds123" password was in use as early as 2017.

83. A generic password such as "solarwinds123" defies elementary cybersecurity standards, and disclosure of this information garnered significant media attention and was a major topic of interest at the House Oversight and Homeland Security Committee and Senate Intelligence Committee hearings on SUNBURST. SolarWinds' former (and current) CEOs both blamed an intern for the Company's password defects at the hearings, stating the password issue was "a mistake that an intern made." The Company's CEOs nonetheless did not explain why an intern had privileges to set the login credentials for the software download webpage of a Company whose monoline product is IT management software.

84. The Company's current CEO has since expressed regret about these comments, stating "you want your employees, including interns, to make mistakes and learn from those mistakes . . . so what happened at the congressional hearing where we attributed [the Company's password problems] to an intern was not appropriate and is not what we are about."

85. SolarWinds also did not implement proper network segmentation, which can "prevent[] attackers or threats from spreading ***or moving laterally***, or 'east-west,' in data centers, clouds, or campus networks" and is "one of the best mitigations against data breaches, ransomware infections, and other types of cybersecurity threats."[16]

86. Simply put, network segmentation is the practice of dividing larger computer networks or IT environments into smaller sub-networks ("subnets"). IT within the same subnet can communicate directly without interference, but any communication between IT in separate subnets must flow through "demarcation points" (typically firewalls). Traffic flow across demarcation points – *i.e.*, lateral movement – is controlled and monitored by network security personnel and security AI that can help stop malicious actors at their point of origin and prevent access to subnets that contain valuable information and hardware. As the director of security research at the cybersecurity firm CyberArk has explained: "Limiting lateral movement [across subnets] forces attackers to use tactics that are 'louder' and more easily identifiable so organizations can be alerted and work to halt progression of the attack before the business is dramatically impacted."

---

16 *What is Network Segmentation*, ILLUMIO, https://www.illumio.com/cybersecurity-101/network-segmentation.

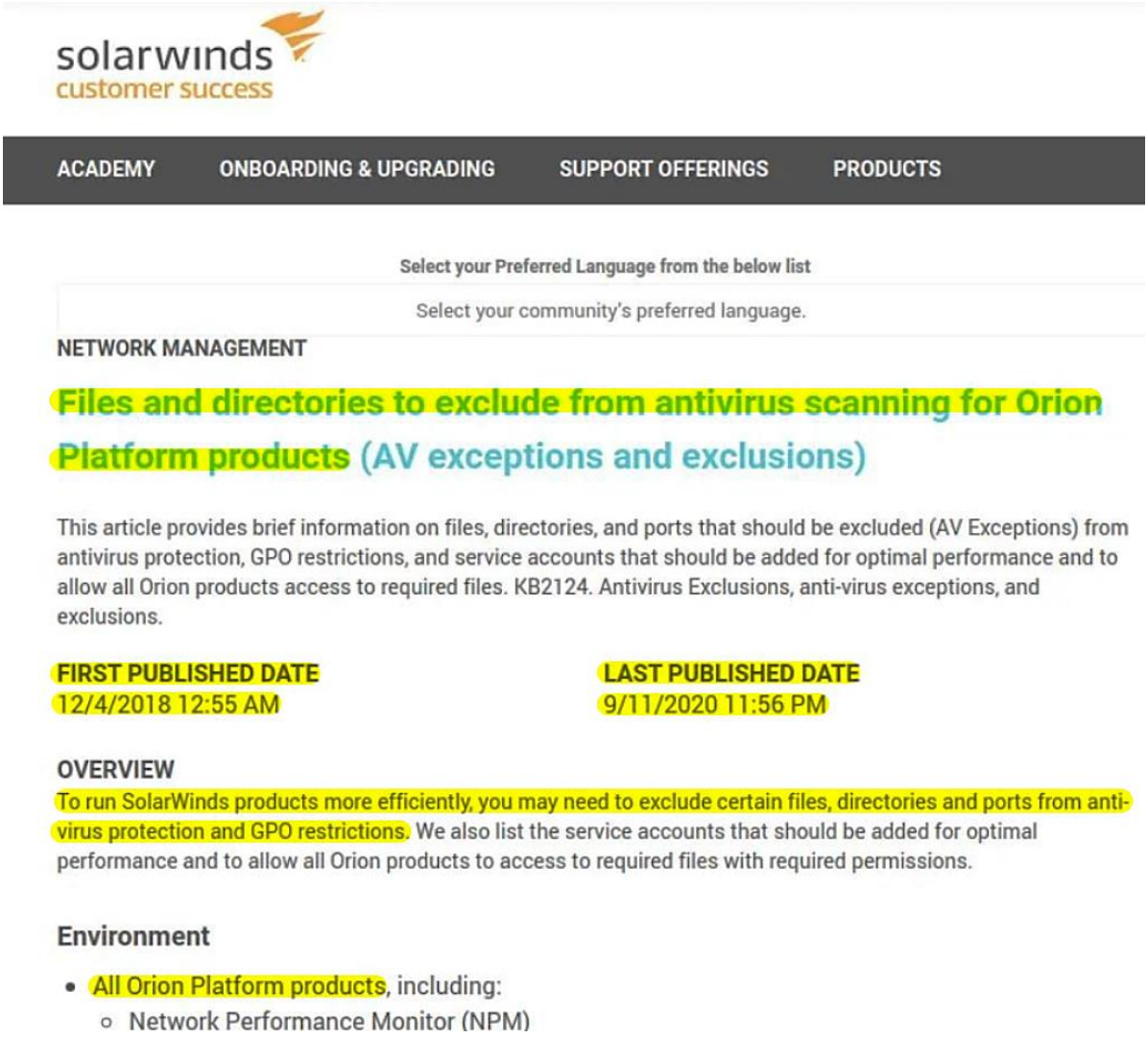
87. FireEye (the company that first discovered SUNBURST) noted in a detailed report on the SUNBURST hack that "[o]nce the attacker gained access to [SolarWinds'] network with compromised credentials, ***they moved laterally***," further suggesting SolarWinds had poor or non-existent network segmentation. The CEO of the cybersecurity software firm Remediant echoed this, stating that "***[l]ateral movement*** is an attack vector that has plagued the industry for several decades now" and was "a key theme around the SolarWinds attack."

88. Further, a few days after SolarWinds publicly disclosed SUNBURST in December 2020, an executive at the internet cybersecurity firm Kaspersky[17] posted on his Twitter account a SolarWinds webpage – titled "solarwinds customer success" – that directed Orion software users to "exclude certain files, directories and ports from anti-virus protection and GPO[18] restrictions" on "[a]ll Orion Platform products" in order to "run SolarWinds products more efficiently":

---

[17] Kaspersky is "the world's largest privately held vendor of Internet security solutions for businesses and consumers."

[18] "GPO" means "Group Policy Object" and refers to a set of Group Policy configurations. "Group Policy" is a feature of Microsoft Windows operating systems that functions as a firewall protection by controlling which portions of an IT environment certain user and computer accounts can access.



solarwinds
customer success

ACADEMY ONBOARDING & UPGRADING SUPPORT OFFERINGS PRODUCTS

Select your Preferred Language from the below list

Select your community's preferred language.

NETWORK MANAGEMENT

Files and directories to exclude from antivirus scanning for Orion Platform products (AV exceptions and exclusions)

This article provides brief information on files, directories, and ports that should be excluded (AV Exceptions) from antivirus protection, GPO restrictions, and service accounts that should be added for optimal performance and to allow all Orion products access to required files. KB2124. Antivirus Exclusions, anti-virus exceptions, and exclusions.

FIRST PUBLISHED DATE
12/4/2018 12:55 AM

LAST PUBLISHED DATE
9/11/2020 11:56 PM

OVERVIEW

To run SolarWinds products more efficiently, you may need to exclude certain files, directories and ports from anti-virus protection and GPO restrictions. We also list the service accounts that should be added for optimal performance and to allow all Orion products to access to required files with required permissions.

Environment

- All Orion Platform products, including:
  - Network Performance Monitor (NPM)

As indicated on the webpage, SolarWinds first issued this guidance as early as December 2018 (shortly after the Company's IPO) and still endorsed this directive as late as September 2020 (three months before it publicly disclosed SUNBURST).

89. The recommendation by SolarWinds that its customers "exclude certain files, directories and ports from . . . GPO restrictions [*i.e.*, firewall protection]" is particularly troubling because it is now known that adequate firewalls could have

significantly limited the SUNBURST malware. In a letter from CISA's executive director to Senator Ron Wyden regarding the "2020 SolarWinds supply chain cybersecurity compromise," the agency stated the following: "CISA agrees that a firewall blocking all outgoing connections to the internet would have neutralized the [SUNBURST] malware," and that "CISA did observe victim networks with this configuration that successfully blocked connection attempts and had no follow-on exploitation."

90. The SolarWinds webpage urging Orion customers to disable anti-virus and firewall protections on the Company's software further noted that "at minimum" users should "[e]xclude whole folders, including subdirectories" from "antivirus or security software" installed on SolarWinds' products. The cybersecurity director at Kaspersky that posted this information on Twitter, stated in the same post: "This is nuts. Solarwinds had a support page (now removed) advising users to DISABLE antivirus scanning for Orion products' folders."

91. SolarWinds was also cutting its investments in cybersecurity from 2018 until December 2020 at the direction of its Thoma Bravo and Silver Lake directors, who together comprised the majority of the Board's directors. For example, the Company offshored some of its cybersecurity to a "[l]ow cost development center in Romania," and "[r]eplaced 2 US-based SEO [search engine optimization] analysts

with 6 Krakow[, Poland]-based SEO analysts" because this produced "a lower overall employee cost[.]"

92. Thoma Bravo and Silver Lake are well known for acquiring software companies and then cutting operating costs and offshoring operations to increase profits in the short-term. As the *The Wall Street Journal* reported: "Thoma Bravo identifies software companies with a loyal customer base . . . and transforms them into moneymaking engines by retooling pricing, shutting down unprofitable business lines and ***adding employees in cheaper labor markets***."[19]

93. For example, Thoma Bravo recently carried out this strategy after purchasing the software company Ellie Mae through a $2.2 billion leveraged buyout in April 2019. Following the acquisition, Thoma Bravo "reduc[ed] operating costs; invest[ed] more heavily in lower-cost geographies; refocus[ed] sales and product resources on the core business," and then sold the company in August 2020 for $11 billion. In discussing private equity firms, and Silver Lake in particular, a financial executive and former investment banker explained that "[f]undamentally these funds

---

[19] Miriam Gottfried, *Orlando Bravo Rides Software Deals to Heights of Private-Equity Industry*, THE WALL STREET JOURNAL (Sept. 22, 2020), https://www.wsj.com/articles/orlando-bravo-rides-software-deals-to-heights-of-private-equity-industry-11600767001.

are not set up to be long-term holders of capital" and that "[t]he exit is going to be the primary return for them."

94. In the years before the SUNBURST hack, SolarWinds' employees took notice that the Company's cybersecurity was an apparent low priority, recounting that "every part of the business was examined for cost savings and common security practices were eschewed because of their expense."[20] A former software engineer at SolarWinds said that the Company "appeared to prioritize the development of new software products over internal cybersecurity defenses."

95. One effect of SolarWinds' cost-cutting strategy was the offshoring of its software development to foreign-owned firms in Belarus, Poland, Romania, and the Czech Republic. Countries that were formerly part of the Soviet Union or the Eastern Bloc are well known to present a heightened risk from Russian operatives that pose a threat to American interests. For example, Russian agents first infiltrated computer servers in Kiev, Ukraine in 2017 to carry out what is now the second-largest supply chain attack in history (after SUNBURST) – the previously discussed

---

[20] David E. Sanger, *et al*., *As Understanding of Russian Hacking Grows, So Does Alarm*, THE NEW YORK TIMES (Jan. 2, 2021), https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

"NotPetya" attack. Many cybersecurity experts believe that SolarWinds' Eastern Europe-based satellite offices were ground zero for the attack: "[S]ome of those measures [referring to SolarWinds' offshoring to countries in East Europe] may have put the company and its customers at greater risk for attack"[21]; "I believe that the company put itself at risk by outsourcing its software development to Eastern Europe"; "[t]he use of foreign-owned offshore companies to provide software engineering is a great threat." [redacted]

96. The Company also included on its online marketing website the following detailed list of its high-profile clients, including such entities as the Pentagon, State Department, NSA, Department of Justice ("DOJ"), and the White House, among others:

---

21 *Id.*

SolarWinds' Customers

SolarWinds' comprehensive products and services are used by more than 300,000 customers worldwide, including military, Fortune 500 companies, government agencies, and education institutions. Our customer list includes:

- More than 425 of the US Fortune 500
- All ten of the top ten US telecommunications companies
- All five branches of the US Military
- The US Pentagon, State Department, NASA, NSA, Postal Service, NOAA, Department of Justice, and the Office of the President of the United States
- All five of the top five US accounting firms
- Hundreds of universities and colleges worldwide

Partial customer listing:

Acxiom
Ameritrade
AT&T
Bellsouth Telecommunications
Best Western Intl.
Blue Cross Blue Shield
Booz Allen Hamilton
Boston Consulting
Cable & Wireless
Cablecom Media AG
Cablevision
CBS
Charter Communications
Cisco
CitiFinancial
City of Nashville
City of Tampa
Clemson University
Comcast Cable
Credit Suisse
Dow Chemical
EMC Corporation
Ericsson
Ernst and Young
Faurecia
Federal Express
Federal Reserve Bank
Fibercloud
Fiserv
Ford Motor Company
Foundstone
Gartner
Gates Foundation
General Dynamics
Gillette Deutschland GmbH
GTE
H&R Block
Harvard University
Hertz Corporation
ING Direct
IntelSat
J.D. Byrider
Johns Hopkins University
Kennedy Space Center
Kodak
Korea Telecom
Leggett and Platt
Level 3 Communications
Liz Claiborne
Lockheed Martin
Lucent
MasterCard
McDonald's Restaurants
Microsoft
National Park Service
NCR
NEC
Nestle
New York Power Authority
New York Times
Nielsen Media Research
Nortel
Perot Systems Japan
Phillips Petroleum
Pricewaterhouse Coopers
Procter & Gamble
Sabre
Saks
San Francisco Intl. Airport
Siemens
Smart City Networks
Smith Barney
Smithsonian Institute
Sparkasse Hagen
Sprint
St. John's University
Staples
Subaru
Supervalu
Swisscom AG
Symantec
Telecom Italia
Telenor
Texaco
The CDC
The Economist
Time Warner Cable
U.S. Air Force
University of Alaska
University of Kansas
University of Oklahoma
US Dept. Of Defense
US Postal Service
US Secret Service
Visa USA
Volvo
Williams Communications
Yahoo

Cybersecurity analysts have described this catalog of high-value targets as being "like a shopping list for adversaries." SolarWinds removed this list from its website following the Company's revelation of the SUNBURST hack as a supposed "courtesy to [its] customers."

97. Before the IPO, SolarWinds employed a Global Cybersecurity Strategist, Ian Thornton-Trump,[22] who warned the Company about the foregoing cybersecurity failures in a 23-page PowerPoint presentation that he delivered to the Company's top technology and marketing executives in April 2017. In his presentation, Thornton-Trump warned the executives that "[t]here was a lack of security at the technical product level" and "minimal security leadership at the top." He insisted that "the survival of [SolarWinds'] customers depends on a commitment to build secure solutions," and that "the survival of the company depends on an internal commitment to security," which he believed the Company lacked at the time. In an email the following month to the Company's Chief Marketing Officer, who reported directly to the CEO, Thornton-Trump resigned from SolarWinds in protest, explaining that the Company appeared "unwilling to make the corrections"

---

[22] Thornton-Trump is currently the Chief Information Security Officer at the cybersecurity firm Cyjax Ltd.

necessary to rectify its major cybersecurity lapses. Thornton-Trump has publicly voiced his views about SolarWinds' security posture since public revelation of SUNBURST. He told *Bloomberg* News in December 2020 that "from a security perspective, SolarWinds was an incredibly easy target to hack" and that he saw "a major breach as inevitable."

98. The failure of the Company's Board to engage in any reasonable oversight concerning the Company's mission critical cybersecurity risks resulted in serious cyber deficiencies, including weak passwords such as "solarwinds123"; a lack of proper network segmentation that hackers exploited; the Company telling customers to disable anti-virus and firewall safeguards, which CISA has stated could "have neutralized the [SUNBURST] malware"; cutting investments in cybersecurity for short-term profit; and advertising the Company's sensitive clients on its webpage.

V. The SUNBURST Incident

99. In December 2020, SolarWinds disclosed that hackers, now believed to be directed by Russia's Foreign Intelligence Service, had used SolarWinds' Orion software as a conduit to infect roughly 18,000 SolarWinds customers.

100. Hackers compromised the Orion software through two major steps. ***First***, as early as January 2019, attackers gained entry into the Orion software build

environment. The "Orion software build environment" is the collection of hardware and software tools – some of which were based in the IT of foreign-owned firms located in Belarus, Poland, Romania, and the Czech Republic – that SolarWinds' software developers used to construct Orion software and any related software updates, including the webpage through which Orion users download updates for the software. SolarWinds has acknowledged that, as many cybersecurity experts believe, hackers were able to infiltrate the Orion software build environment because of the password deficiencies that cybersecurity experts like Vinoth Kumar had been warning the Company about since as early as 2019.

101. Shortly after the attack was made public, CISA issued an "alert" in January 2021 concerning the SolarWinds cyberattack on its "National Cyber Awareness System" webpage. The alert, titled "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations," explained that the SUNBURST hackers' signature techniques involved "password guessing" and "password spraying,"[23] and using "inappropriately secured administrative credentials" accessible on the internet.

---

[23] "Password guessing" is a technique in which an adversary "systematically guess[es] the password using a repetitive or iterative mechanism." An attacker "may

102. Further, on May 7, 2021, SolarWinds' current CEO acknowledged that a "[b]rute-force attack, such as a password spray attack" was one of the "three most likely candidates for initial entry" by the attackers into the Orion software build environment. As detailed above, SolarWinds' directors and executives were warned about the Company's weak passwords and basic cybersecurity deficiencies as early as 2017.

103. ***Second***, once inside the Company's Orion software build space, the attackers inserted the SUNBURST malware into software updates for Orion. Approximately 18,000 Orion users subsequently downloaded the SUNBURST tainted software updates from a SolarWinds' webpage between March and June 2020. The SUNBURST malware was especially damaging because it enabled the hackers to create entry vectors or "backdoors" in any Orion software that was upgraded with the tainted updates.

---

guess login credentials without prior knowledge of system or environment passwords during an operation by using a list of common passwords."

"Password spraying" is a technique in which an attacker "uses one password (*e.g.,* 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain" and then "[l]ogins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords."

104. Although the full extent of the SUNBURST hackers' access to SolarWinds' clients' IT systems is not publicly known, it is clear that the attackers have been able to steal extensive proprietary information, confidential emails, and intellectual property from some of America's most sensitive government agencies and private businesses.

105. The compromised businesses and government entities include, *inter alia*, Microsoft, Cisco, and Belkin; the Defense, Commerce, State, Treasury, Justice, Homeland Security, and Energy Departments, the National Nuclear Security Administration, and the Pentagon. It is now known that the SUNBURST hackers accessed the private emails of the former secretary of the DHS, and other high-level officials in that department who are expressly tasked with identifying foreign threats to U.S. national security. The DOJ has also disclosed that the SUNBURST hackers accessed the email accounts of employees in at least 27 prominent U.S. Attorney's Offices across 14 states, including all sent, received, and stored emails and attachments of ***at least 80%*** of the employees in all four of New York's U.S. Attorney's Offices.

106. The SUNBURST compromise was particularly devastating because, as CISA has explained, "SolarWinds Orion typically leverages a significant number of highly privileged accounts and access to perform normal business functions," and

"[s]uccessful compromise of one of these systems can therefore enable further action and privileges in any environment where these accounts are trusted." In addition, the hackers can now use the mass of identity data they harvested to load additional password spraying and credential stuffing tools for future cyberattacks.

107. In the days following the Company's initial public disclosure of SUNBURST in December 2020, SolarWinds' stock lost nearly 40% of its value. As of today, the stock trades at more than a 30% discount to its pre-revelation trading price. For the six months ended June 30, 2021, the Company incurred $34 million in direct expenses related to SUNBURST, stemming from, *inter alia*, costs to investigate and remediate the cyberattack; legal, consulting, and other professional service expenses; and public relations costs.

108. In the first six months ended June 30, 2021, the Company also experienced a 27% decline in its license revenue relative to the previous year. SolarWinds explained that this decline was "primarily due to decreased sales of our licensed products as a result of the Cyber Incident [*i.e.*, SUNBURST]" (among other factors). The Company's net increase in cash and cash equivalents for the same period was down over 74% relative to the previous year, which the Company also attributed, in part, to SUNBURST.

109. The Company is also under investigation from numerous domestic and foreign law enforcement agencies and other governmental authorities, including the DOJ, SEC, and state Attorneys General, and is subject to several private class action lawsuits. SolarWinds has stated that it "expect[s] to continue to incur additional legal and other professional services costs and expenses associated with the Cyber Incident in future periods," including increased expenses related to "insurance, finance, compliance activities, and to meet increased legal and regulatory requirements." The Company forecasts that additional costs to "enhance [the] security measures across [its] systems and [its] software development and build environments" will be "approximately $20 million on an annual basis." Defendants failure to fulfill their obligations as described herein made it foreseeable, if not likely, that the Company would suffer these many significant harms.

110. The Company's current directors inflicted even further damage on SolarWinds by granting Defendant Thompson a liability release and (adding insult to injury) agreeing to hire him as a paid purported "Consultant" to help remedy the damage he helped cause.

111. On December 7, 2020, prior to discovering SUNBURST, the Board hired a new CEO to replace Defendant Thompson starting on January 4, 2021. That same day the Board also approved an amendment to Defendant Thompson's

employment agreement which confirmed that December 31, 2020 would be his termination date. Defendant Thompson's employment agreement with the Company required him to serve as a consultant to SolarWinds – without any further compensation – until March 31, 2021, even if his termination occurred prior to March 31, 2021. Nonetheless, after discovering SUNBURST, the Board overrode that provision and allowed the Company to enter into a "Transition Agreement" with Defendant Thompson (which became effective January 1, 2021) pursuant to which SolarWinds rehired Defendant Thompson as a purported "Consultant" with a monthly retainer of $62,500 for five months, or a total of $312,500. The Transition Agreement also purported to provide a release to Defendant Thompson "with respect to actions taken (or omitted to be taken) by the Consultant in his former capacity as Chief Executive Officer of the Company or as a member of the Board of which the Board (excluding the Consultant) has actual knowledge on the date hereof." These additional costs to SolarWinds were a foreseeable result of the Board's total failure to monitor the Company's cybersecurity.

DERIVATIVE & DEMAND ALLEGATIONS

112. Plaintiffs bring this action derivatively on behalf and for the benefit of SolarWinds, and in order to redress the Defendants' breaches of their fiduciary duties.

113. Plaintiffs have not made any demand on SolarWinds' current Board (the "Demand Board") to commence this action against Defendants because it would be futile. As detailed *supra*, eight of the eleven members who comprise the Demand Board – *i.e.*, Defendants Bock, Boro, Hao, Hoffmann, Kinney, Lines, Sundaram, and Widmann – could not impartially evaluate a demand because they face a substantial likelihood of personal liability for utterly failing to implement or oversee any reasonable system of monitoring over mission critical aspects of SolarWinds' business during the relevant time. Six of these directors – Defendants Bock, Boro, Hao, Hoffmann, Kinney, and Lines – have served on the Board at all times from the October 2018 IPO until the present. The other two directors – Defendants Sundaram and Widmann – joined the Board in February 2020 and therefore served on the Board for a substantial part of the relevant time and are likewise liable as a result.

[redacted]

114. Defendant Widmann is also currently a director at Silver Lake and has been employed there since 2011. He is thus conflicted with respect to: Defendant Bingle, who served as a managing director at Silver Lake during the relevant time;

Defendant Hao, who served as a managing partner at Silver Lake during the relevant time; and Defendant White, who served as a director at Silver Lake during the relevant time. Defendant Hao is likewise conflicted with respect to Defendants Bingle, Widmann, and White because of his ties to Silver Lake.

115. Another member of the Demand Board – Doug Smith – is also disabled from considering Plaintiff's demand because he was a senior advisor to Silver Lake from 2016 until 2019 and therefore has strong ties to Silver Lake. He is thus conflicted with respect to Defendants Bingle, Hao, Widmann, and White.

116. A majority of the Demand Board is also incapable of impartially evaluating a demand because by January 1, 2021, those directors had already determined to release Defendant Thompson for all of his conduct in connection with his role as the Company's CEO and as a fellow director during his entire tenure at SolarWinds. In addition, a majority of the Demand Board rewarded Defendant Thompson with more than $25.5 million in compensation in 2020 and a total of $37 million in compensation since 2017, and those directors have taken no action to claw back any of that compensation and have instead granted Defendant Thompson a liability release and excessive additional compensation as a purported "Consultant" to SolarWinds. Defendant Thompson, however, like the majority of the Demand

Board, utterly failed in his oversight duties related to the Company's cybersecurity risks for many years prior to SUNBURST.

117. A majority of the Demand Board, therefore, is incapable of impartially considering whether to enforce the claims alleged herein for breaches of fiduciary duty, rendering any demand Plaintiffs could make on the Demand Board futile.

118. As alleged herein, the Director Defendants breached their fiduciary duties of loyalty, due care, and good faith to the Company and its shareholders by failing to establish or oversee a system of oversight over SolarWinds' cybersecurity. The Director Defendants' failure to set up a system of oversight concerning cybersecurity also defied express SEC guidance, namely the SEC's 2018 Cybersecurity Release. Because these actions (or more aptly, inactions) were contrary to both Defendants' fiduciary duties to the Company and positive law, the actions cannot be deemed a valid exercise of the business judgment rule.

COUNT I

Breach of Fiduciary Duties of Loyalty and Care through a Bad Faith Failure to Oversee SolarWinds' Cybersecurity

(Derivatively Against All Defendants)

119. Plaintiffs incorporate by reference and restate each and every allegation set forth above, as if though fully set forth herein.

120. The Board was a fiduciary of the Company and its stockholders. As such, each Director Defendant owed the Company and its stockholders the highest duties of loyalty, due care, and good faith.

121. Consistent with its fiduciary duties, the Board was required to implement and monitor a system of corporate controls and reporting mechanisms concerning the Company's cybersecurity, a leading operational and financial risk to SolarWinds' business operations.

122. The Board utterly failed to implement any Board-level system of oversight concerning the Company's cybersecurity, including, *inter alia*, failing to (i) implement protocols requiring management to keep the Board apprised of cybersecurity compliance practices, risks, and reports, on an ongoing basis (quarterly or biannually, at a minimum); (ii) discuss key cybersecurity issues on a regular basis (quarterly or biannually, at a minimum); (iii) take remedial action when apprised of cybersecurity deficiencies; and (iv) implement and monitor any reporting

policies and systems in compliance with SEC disclosure and oversight laws concerning cybersecurity.

123. By failing to make a good faith effort to implement an oversight system concerning SolarWinds' cybersecurity, each Director Defendant individually and the Board collectively failed to exercise their duties of due care and loyalty to the Company and its stockholders. Such a severe lack of attentiveness to a mission critical operation of SolarWinds' business constitutes a bad faith breach of the Director Defendants' duties of loyalty and due care.

124. As a direct and proximate result of the Board's bad faith failure to carry out its fiduciary duties, SolarWinds has sustained, and will continue to sustain, significant damages – both financially and to its corporate profile and goodwill, among others. These damages may include, *inter alia*, substantial penalties, fines, damages awards, and expenses, and increased regulatory scrutiny.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for relief and judgment as follows:

A. Declaring that Plaintiffs may maintain this derivative action on behalf of SolarWinds and that Plaintiffs are proper and adequate representatives of the Company;

B. Declaring that Defendants have breached their fiduciary duties to SolarWinds;

C. Determining and awarding to SolarWinds the damages it has sustained as a result of the breaches of fiduciary duties set forth above from each of the Defendants, jointly and severally, together with interest thereon;

D. Directing SolarWinds to implement policies and procedures and to maintain adequate operational controls and Board governance of management concerning the Company's cybersecurity;

E. Awarding to Plaintiffs the costs and disbursements of the action, including reasonable attorneys' fees, costs, and expenses;

F. Awarding pre- and post-judgment interest; and

G. Granting such other and further relief as this Court deems just and equitable.

Of Counsel:

ROBBINS GELLER RUDMAN
& DOWD LLP
Chad Johnson
Noam Mandel
Desiree Cummings
Jonathan Zweig
Sarah Delaney
420 Lexington Avenue, Suite 1832
New York, NY 10170
chadj@rgrdlaw.com
noam@rgrdlaw.com
dcummings@rgrdlaw.com
jzweig@rgrdlaw.com
sdelaney@rgrdlaw.com

Counsel for Plaintiff Construction Industry Laborers Pension Fund

FRIEDMAN OSTER
& TEJTEL PLLC
Jeremy S. Friedman
David Tejtel
493 Bedford Center Road, Suite 2D
Bedford Hills, NY 10507
jfriedman@fotpllc.com
dtejtel@fotpllc.com

KASKELA LAW LLC
D. Seamus Kaskela
18 Campus Blvd., Suite 100
Newton Square, PA 19073
skaskela@kaskelalaw.com

Counsel for Plaintiff Lawrence Miles

SAXENA WHITE P.A.

/s/ Thomas Curry
Thomas Curry (#5877)
Tayler D. Bolton (#6640)
1000 N. West Street, Suite 1200
Wilmington, DE 19801
(302) 485-0480
tcurry@saxenawhite.com
tbolton@saxenawhite.com

GRANT & EISENHOFER P.A.

/s/ Michael J. Barry
Michael J. Barry (#4368)
Vivek Upadhya (#6241)
123 Justison Street, 7th Floor
Wilmington, DE 19801
(302) 622-7000
mbarry@gelaw.com
vupadhya@gelaw.com

Counsel for Plaintiffs

COHEN MILSTEIN SELLERS
& TOLL PLLC
Julie Goldsmith Reiser
1100 New York Avenue N.W.
Fifth Floor
Washington, DC 20005
(202) 408-4699
jreiser@cohenmilstein.com

COHEN MILSTEIN SELLERS
& TOLL PLLC
Richard A. Speirs
Amy Miller
88 Pine Street, 14th Floor
New York, NY 10005
(212) 838-7797
rspeirs@cohenmilstein.com
amiller@cohenmilstein.com

Counsel for Plaintiff Brian Seavitt

Dated: November 1, 2021