EFiled: Jan 04 2023 05:18PM EST
Filing ID 68797303
Case Number 411,2022

IN THE SUPREME COURT 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-Below/Appellants, 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-Below/Appellees, – and – SOLARWINDS CORPORATION, Nominal Defendant-Below/Appellee	NO. 411, 2022 CASE BELOW: COURT OF CHANCERY OF THE STATE OF DELAWARE C.A. No. 2021-0940-SG REDACTED VERSION FILED JANUARY 4, 2023

APPELLANTS' OPENING BRIEF

GRANT & EISENHOFER P.A.
Michael J. Barry (#4368)
Vivek Upadhya (#6241)
123 Justison Street, 7th Floor
Wilmington, DE 19801
(302) 622-7000

Counsel for Plaintiffs

SAXENA WHITE P.A.
Thomas Curry (#5877)
Tayler D. Bolton (#6640)
824 N. Market Street, Suite 1003
Wilmington, DE 19801
(302) 485-0483

Counsel for Plaintiffs

Of Counsel:

ROBBINS GELLER RUDMAN
& DOWD LLP
Chad Johnson
Noam Mandel
Desiree Cummings
Jonathan Zweig
420 Lexington Avenue, Suite 1832
New York, NY 10170
(212) 432-5100

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
(888) 529-1108

KASKELA LAW LLC
D. Seamus Kaskela
18 Campus Blvd., Suite 100
Newton Square, PA 19073
(888) 715-1740

Counsel for Plaintiff Lawrence Miles

COHEN MILSTEIN SELLERS
& TOLL PLLC
Julie Goldsmith Reiser
1100 New York Avenue, N.W.
Fifth Floor
Washington, DC 20005-3964
(202) 408-4600

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

Counsel for Plaintiff Brian Seavitt

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

NATURE OF THE PROCEEDINGS

This appeal raises a simple question: would *Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019), have been decided differently if Blue Bell's board had nominally delegated oversight of "food safety" to two committees, but those two committees—like the board as a whole—never engaged in any actual oversight concerning this mission-critical risk?

SolarWinds Corporation ("SolarWinds" or the "Company"), like Blue Bell, is a "monoline" company. Rather than sell ice cream, SolarWinds sells network management software—including a flagship product that requires customers to provide SolarWinds with full administrative privileges to their IT systems. This is a serious responsibility, as SolarWinds' customers include the highest-value hacking targets in the world: a majority of the Fortune 500 companies and numerous national security agencies. Thus, for SolarWinds, like Blue Bell, customer safety was of the utmost importance. For Blue Bell, this meant food safety. For SolarWinds, cybersecurity.

But SolarWinds, like Blue Bell, experienced a customer-safety disaster of epic proportions. Blue Bell's customers were poisoned by listeria infecting its ice cream due to Blue Bell's serious food safety deficiencies. SolarWinds' customers had troves of sensitive data compromised by malware infecting its software due to

SolarWinds' serious cybersecurity deficiencies (the "SUNBURST" incident).

Just as food safety deficiencies persisted unaddressed for years at Blue Bell prior to the moment of crisis, so too did cybersecurity deficiencies at SolarWinds. In 2017, for example, SolarWinds's "Global Cybersecurity Strategist" blew the whistle on SolarWinds' "*lack of security*"—which he believed was threatening the very "*survival of the company*"—then resigned in protest when senior executives were "unwilling to make the corrections" necessary. In 2019, as another example, SolarWinds management was notified by an external researcher that an important company password standing between hackers and SolarWinds' products was publicly accessible on the internet. The password? "s*olarwinds123*."

Plaintiffs here, like the plaintiff in *Marchand*, pursued books-and-records demands, obtaining SolarWinds board of directors (the "Board") materials spanning the 26-month period between SolarWinds's October 2018 IPO and the December 2020 revelation of SUNBURST (the "220 Production"). Like the plaintiff in *Marchand*, Plaintiffs here found an utter "dearth of any board-level effort at monitoring." *Marchand*, 212 A.3d at 809. Indeed, the Board as a whole *never* received a single report or held a single discussion regarding cybersecurity. Nothing. The Board's Audit Committee, specifically charged with overseeing cybersecurity issues, likewise *never* received a single report or held a single discussion regarding

cybersecurity. Nothing.

In fact, the only time any directors engaged in any substantive cybersecurity discussion was in connection with a single, one-off management presentation to the Nominating and Governance Committee ("NGC") in February 2019—nearly two years before SUNBURST. This presentation warned in striking language that cyberattacks were increasing, that SolarWinds was a particularly attractive target given its "trusted access" to its high-profile customers' networks, and that as a result, cybersecurity was "***mission critical*** to SolarWinds' business operations." (Emphasis in original). In the wake of the February 2019 briefing, in apparent newfound recognition of the importance of monitoring cybersecurity risk, the NGC amended its own Charter to include a requirement to "discuss with management the Company's major risk exposures, including … cyber and data security." *But it never did*. In the nearly two years between the February 2019 briefing and the December 2020 revelation of SUNBURST, the NGC never received a single report or held a single discussion concerning cybersecurity. Like the Audit Committee and the Board as a whole, it did absolutely nothing to monitor or ensure reporting on cybersecurity issues—even after being expressly informed such issues were "***mission critical*** to SolarWinds' business operations."

Thus, the SolarWinds Board—at the very least—is indistinguishable from the

Blue Bell Board in *Marchand and, by all appearances,* compares unfavorably, given the express warning received by the NGC in the February 2019 briefing. Yet, while this Court sustained oversight claims against Blue Bell's directors in *Marchand*, the trial court dismissed Plaintiffs' oversight claims below. To do so, the trial court found that the mere existence of two committees nominally charged with cybersecurity oversight constituted a sufficient "reporting system"—even though the NGC never received information concerning cybersecurity or discussed cybersecurity issues *on any occasion in the nearly two years* between the February 2019 briefing and the December 2020 revelation of SUNBURST, and the Audit Committee did nothing to monitor cybersecurity whatsoever. (Memorandum Opinion ("Op.") 31–36).

The trial court erred. The nominal delegation to Board committees of oversight concerning a "mission critical" risk does not constitute a "reporting system" if neither of those committees actually do anything for years on end. If *Marchand* means what it says, the decision below must be reversed.

SUMMARY OF THE ARGUMENT

1. Dismissal under Court of Chancery Rule 23.1 was not warranted because Plaintiffs have adequately pled that demand is excused on the basis that a majority of the Demand Board faces a substantial likelihood of liability for failing to fulfill their oversight duties under the standards set forth in *In re Caremark Int'l Inc. Deriv. Litig.*, 698 A.2d 959 (Del. Ch. 1996), as applied by this Court in *Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019).

STATEMENT OF FACTS

I. SolarWinds' Mission-Critical Cybersecurity Risk

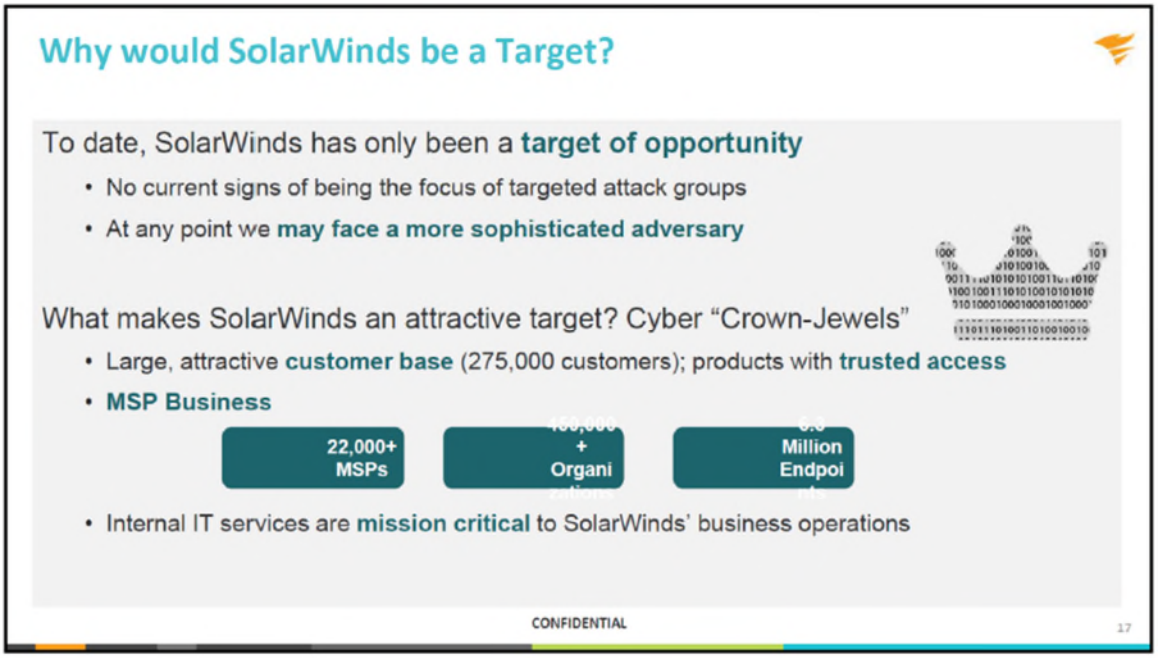
Cybersecurity is a "mission critical" concern for SolarWinds. Defendants do not, and cannot, deny this.

SolarWinds is a leading information technology ("IT") management company whose clients include vital U.S. government agencies and major corporations. The Company's flagship software, the Orion Platform ("Orion"), is a network management software suite that provides "centralized monitoring and management." (A46 ¶34).

To perform its core functions, Orion requires unhindered access with full administrative privileges to users' IT systems. (A222 ¶35). This means that Orion enters highly privileged accounts and locations on users' computer networks, and anyone who accesses Orion can alter, delete, or steal vital files and applications, reboot or disable connected IT, and engage in "lateral movement" across the network. *Id.* Trusted and limitless access to SolarWinds' clients' networks was thus a fundamental aspect of the Company's core business, subjecting the Company to unique and well-known cybersecurity risks. (A30 ¶3).

SolarWinds' own documents acknowledge that cybersecurity is "***mission critical***" to the Company, because SolarWinds' "***trusted access***" to a "large,

attractive ***customer base***" constituted "Cyber Crown-Jewels" and made SolarWinds an "attractive target" that could "[a]t any point … ***face a more sophisticated adversary***." (A263-264 ¶39) (all emphasis in original). The severity of this risk was reported to the NGC in February 2019, when that committee received a "Cybersecurity Briefing" from company management. (A33 ¶7, A48-A53 ¶¶39–43): The presentation speaks for itself:



(A48-A50 ¶39).[1]

The Cybersecurity Briefing demonstrates, explicitly, what Defendants and the trial court cannot dispute: cybersecurity was "mission critical" for SolarWinds, as

[1] The February 2019 Cybersecurity Briefing was attended by Defendant Directors Kinney, Bingle, Bock, and Widmann. (A224 ¶39).

companies like SolarWinds, with trusted access to valuable third parties' networks, were subject to a significant and increasing risk from malicious actors seeking to access those networks (*i.e.*, "supply chain" cyberattacks, like SUNBURST). And SolarWinds was perhaps the most attractive target of all, given its "Cyber Crown-Jewels" of unfettered access to the internal networks of the most attractive hacking-targets in the world. (A249 ¶38).

These risks, moreover, were well-known in SolarWinds' field. As detailed in the Complaint, U.S. government agencies and leading cybersecurity firms issued stark public warnings about the significant and increasing threat of supply chain cyberattacks. (A53-A59 ¶¶44–53). Any fiduciary reasonably familiar with SolarWinds' business must have known that supply chain cyberattacks posed a catastrophic and surging risk to SolarWinds. (A61 ¶57). SolarWinds' core network management business, and its high-value customer base, made it self-evident that cybersecurity required affirmative Board-level oversight.

SolarWinds' own SEC filings acknowledge the growing, mission critical nature of the Company's cybersecurity risks and the Board's obligation to monitor and oversee these risks. (A64 ¶62). The Company's annual proxy filings for 2019 and 2020 attempted to reassure stockholders by stating falsely that the "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[.]" (A65 ¶63).

These cybersecurity-related SEC filings were not voluntary disclosures, but express requirements of the federal securities laws. In February 2018, the SEC unanimously approved and issued new interpretive guidance ("2018 Cybersecurity Release") which interpreted *binding law* to require public companies to "maintain appropriate and effective disclosure controls[,] including those related to cybersecurity," and obligating directors to be informed "about the cybersecurity risks and incidents that the company has faced or is likely to face." (A63 ¶59). For companies like SolarWinds, where cybersecurity risks are "material to [the] company's business," the SEC requires 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 cybersecurity issues"; and (iii) the "company's cybersecurity risk management program." (A64 ¶60).[2]

Defendants thus knew that SolarWinds faced mission critical cybersecurity risks that they were required to oversee. Yet, they utterly failed to do so.

---

[2] Likewise, the New York Stock Exchange, where SolarWinds traded, issued a detailed "Cybersecurity Guide" emphasizing the critical role of corporate directors in cybersecurity oversight: "Active, hands-on engagement by … the board is required. The risk is ***existential***. Nothing is more important." (A67 ¶65)

II. Defendants' Utter Failure to Conduct Good Faith Oversight

Defendants' own documents show that they did not conduct—or even attempt in good faith to conduct—any reasonable oversight of this fundamental risk to the Company's only line of business. (A69 ¶¶70–71).

SolarWinds' 220 Production shows that SolarWinds' Board as a whole did not hold a single meeting or engage in a single substantive discussion about the Company's cybersecurity risks for more than two years from the time of the Company's IPO in October 2018 until learning of SUNBURST in December 2020. (A34 ¶8, A69 ¶71).

SolarWinds' 220 Production also shows that the Audit Committee conducted no cybersecurity oversight during the same two-year period even though it held formal responsibility for oversight concerning cybersecurity pursuant to its Charter, which specifically identified "cyber and data security" as one of "the Company's major financial risk exposures." *Id.* Despite this express oversight obligation, the Audit Committee never held a meeting or discussion concerning any aspect of the Company's cybersecurity, engaged in no oversight regarding cybersecurity, and never reported to the Board about cybersecurity risks. *Id.*

SolarWinds' 220 Production shows further that the NGC also utterly failed to carry out this responsibility. Not long after the IPO, the NGC received the February

2019 Cybersecurity Briefing warning of the "***mission critical***" cybersecurity risks facing SolarWinds. (A48 ¶39). The NGC Charter was then amended, in April 2019, to formally include cybersecurity among the NGC's oversight responsibilities. (A72 ¶75). Yet, despite its explicit recognition of the need for such oversight, the NGC never actually did anything. After that Charter amendment, the NGC—like the Audit Committee—never held a meeting or discussion concerning any aspect of the Company's cybersecurity, engaged in no oversight regarding cybersecurity, and never reported to the Board about cybersecurity risks. (A70-A72 ¶¶73–75).

Ultimately, the Cybersecurity Briefing—which expressly warned of the mission critical cybersecurity risks facing the Company—was the ***only*** meeting prior to SUNBURST in which any of SolarWinds Board members even received a report concerning the Company's cybersecurity. (A34-35 ¶10).

III. SolarWinds' Grossly Deficient Cybersecurity Practices

As a result of the Board's complete failure to oversee known mission critical cybersecurity risks, serious deficiencies in SolarWinds' cybersecurity developed and persisted between 2018 and 2020, culminating in SUNBURST. (A75 ¶80, A87 ¶99). From the Company's IPO in October 2018 until its disclosure of SUNBURST in December 2020, SolarWinds: (i) used ludicrously ineffective passwords to protect key elements of its software; (ii) failed to 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 as a virtual menu for cybercriminals. (A75 ¶80).

In November 2019, cybersecurity expert and prominent "malware hunter" Vinoth Kumar emailed SolarWinds' Information Security team warning that file transfer protocol ("FTP") credentials—*i.e.*, usernames and passwords—for SolarWinds' software download website were publicly available on the internet. (A 75 at ¶81). Remarkably, the Company's FTP password was "*solarwinds123*." This incident clearly foreshadowed the eventual SUNBURST catastrophe: the Company would eventually admit that the SUNBURST hackers accessed the Company's "software development environment" by way of "compromised credentials" (*i.e.*, usernames and passwords). (A49 ¶82; Op. 23). Mr. Kumar's email to the Company alerting it to the breach of the "*solarwinds123*" password warned that, as a result of SolarWinds' compromised credentials, "any hacker could upload malicious exe [*i.e.*, malware] and update it with release [of] SolarWinds product." (A72 ¶81). In other words, Mr. Kumar specifically warned that the Company's software download website was readily accessible to hackers who could infect SolarWinds software updates—precisely what happened in SUNBURST.

In testimony before the House Oversight and Homeland Security Committee

and Senate Intelligence Committee hearings on SUNBURST, SolarWinds' former and current CEOs both attempted to downplay this glaring failure of basic cybersecurity as "a mistake that an intern made." (A77 ¶83). But neither could explain why SolarWinds granted an intern the authority to set critical login credentials for a company that counts the Pentagon, the National Security Agency, the White House, and nearly the entire Fortune 500 amongst its clients. *Id.*

SolarWinds also did not implement proper "network segmentation," the practice of dividing computer networks into smaller sub-networks to "prevent[] attackers or threats from spreading or moving laterally, or 'east-west,'" which is "one of the best mitigations against data breaches, ransomware infections, and other types of cybersecurity threats." (A78 ¶¶85–86). FireEye (the company that first discovered SUNBURST) noted in a detailed report on SUNBURST that "[o]nce the attacker gained access to [SolarWinds'] network with compromised credentials, they moved laterally," revealing SolarWinds' poor or non-existent network segmentation. (A79 ¶87). SolarWinds also directed Orion software users to "exclude certain files, directories and ports from anti-virus protection and GPO restrictions [*i.e.*, firewall protection]" on "[a]ll Orion Platform products" in order to "run SolarWinds products more efficiently[.]" (A79 ¶88). That was another major failure in basic cybersecurity, as adequate firewalls could have significantly limited

the SUNBURST malware. *Id.*

Defendants' years-long neglect of cybersecurity is also evident from SolarWinds' diminishing investment in this mission-critical area. At the direction of its Thoma Bravo and Silver Lake directors (who together comprised a majority of the Board), SolarWinds slashed investments in cybersecurity from 2018 until December 2020. (A81-A83 ¶¶91–94). That strategy resulted in the offshoring of SolarWinds' software development to foreign-owned firms in Belarus, Poland, Romania, and the Czech Republic, which presented a heightened risk from Russian operatives known to be active in those areas. (A83 ¶95).

To make matters worse, SolarWinds included a detailed list of its high-profile clients on its online marketing website, including the Pentagon, State Department, NSA, DOJ, and the White House, among others. (A84 ¶96). Cybersecurity analysts have described this catalog of high-value targets as "like a shopping list for adversaries." *Id.* After the revelation of SUNBURST, SolarWinds removed this list from its website as a supposed "courtesy to [its] customers." *Id.*

This litany of major deficiencies in SolarWinds' cybersecurity is not a retroactive judgment in light of SUNBURST. Rather, the most scathing criticism of SolarWinds' cybersecurity came from within the Company—years before SUNBURST. In April 2017, Ian Thornton-Trump, a Global Cybersecurity Strategist

employed by the Company before the IPO, delivered a 23-page presentation to the Company's top technology and marketing executives, detailing SolarWinds' cybersecurity failures. (A86 ¶97). 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." *Id*. 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. *Id.* 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" necessary to rectify its major cybersecurity lapses. *Id.*

Significantly, none of those critical cybersecurity issues—each of which would independently constitute a major red flag—are ever discussed or even referenced in the 220 Production, further demonstrating Defendants' failure to perform any reasonable or systematic oversight concerning mission-critical cybersecurity risks.

IV. The Resulting SUNBURST Catastrophe

Defendants' oversight failures allowed SolarWinds' severe cybersecurity

deficiencies to persist and grow without remediation, resulting in SUNBURST, a massive cybersecurity incident that SolarWinds announced in December 2020. SUNBURST was a supply chain cyberattack in which hackers used SolarWinds' trusted access to its clients' IT systems to infiltrate those systems in what is regarded as the most devastating cyberattack against the United States in history. (A31 ¶4; Op. 11). In simple terms, hackers used SolarWinds' Orion software as a "Trojan horse" to attack the Company's clients, hiding malware within software updates that SolarWinds' clients downloaded into their IT systems. (A31 ¶4; Op. 11). Hackers gained entry to the Orion software "build environment"—a collection of hardware and software tools used to develop and update the software—due to the Company's password deficiencies. (A88 ¶100; Op. 11). Once inside the build environment, the hackers inserted the SUNBURST malware into software updates for Orion. (A89 ¶103; Op. 11). When SolarWinds' clients conducted routine software updates, they unknowingly brought this malware into their systems. (A31 ¶4). According to the Company, SUNBURST impacted up to 18,000 clients, including numerous U.S. national security agencies and leading technology companies. (*Id.*; Op. 12).

The full extent of the SUNBURST hackers' access is not publicly known, but it is clear that they were able to steal extensive proprietary information, confidential emails, and intellectual property from some of America's most sensitive government

agencies and private businesses. (A90 ¶104; Op. 12). These compromised entities include corporations such as Microsoft and Cisco; and U.S. government entities including the Defense, Commerce, State, Treasury, Justice, Homeland Security, and Energy Departments, as well as the National Nuclear Security Administration. (A90 ¶105; Op. 12 n.50). The SUNBURST hackers accessed the private emails of the former secretary of the DHS and other high-level officials in that department, as well as the email accounts of employees in at least 27 U.S. Attorney's Offices, including all emails and attachments of at least 80% of the employees in all four of New York's U.S. Attorney's Offices. *Id.* The fallout from SUNBURST has caused catastrophic reputational and financial harm to SolarWinds.

ARGUMENT

I. THE TRIAL COURT ERRED IN DISMISSING THE COMPLAINT FOR FAILURE TO PLEAD DEMAND FUTILITY

A. Question Presented

Did Plaintiffs adequately plead that demand is excused because a majority of the directors on the Demand Board face a substantial likelihood of liability for failing to fulfill their oversight duties under the standards set forth in *Caremark*, 698 A.2d 959, as applied by this Court in *Marchand*, 212 A.3d 805? This question was raised below (A141-A146, A183-A211, A245-A270) and considered by the trial court (Op. 1–37).

B. Scope of Review

This Court "review[s] a motion to dismiss for failure to plead demand futility *de novo*." *Marchand*, 212 A.3d at 817.

C. Merits of the Argument

Plaintiffs argued below that demand was futile under Court of Chancery Rule 23.1 because a clear majority of the Demand Board faces a substantial likelihood of liability for failing to fulfill their oversight duties in good faith under *Caremark*, as applied by this Court in *Marchand*. In *Marchand*, the Court explained:

> Bad faith is established . . . when the directors completely fail to implement any reporting or information system or controls, or having implemented such a system or controls, consciously fail to monitor or

> oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention. In short, to satisfy their duty of loyalty, directors must make a good faith effort to implement an oversight system and then monitor it.

Marchand, 212 A.3d at 821 (internal quotation and footnote omitted) (applying *Caremark*, 698 A.2d 959)). *Marchand* further "mandate[s]" that boards "rigorously exercise [their] oversight function with respect to mission critical aspects of [their] company's business." *In re The Boeing Company Deriv. Litig.*, 2021 WL 4059934 at *26 (Del. Ch. Sept. 7, 2021); *see also City of Detroit P&F Ret. Sys. v. Hamrock*, 2022 WL 2387653, at *13 (Del. Ch.June 30, 2022) (recognizing that "[t]he Delaware Supreme Court clarified in *Marchand* that a reasonably designed monitoring and reporting system, at a minimum, addresses 'mission critical' risks.").

Stockholders may assert a *Caremark* claim under two "prongs." A "prong one" claim involves a board's utter failure to implement an oversight system. *See, e.g.*, *Boeing*, 2021 WL 4059934, at *24. A "prong two" claim involves a board that has implemented an oversight system, but has failed to adequately monitor it—typically evidenced by the board's disregard of "red flags." *Id.* at *33.

Plaintiffs alleged that eight of the eleven members of the Demand Board face a substantial likelihood of personal liability for failing to satisfy their oversight duties under *Caremark* "prong one" (or, alternatively, "prong two") with respect to

the Company's known "mission critical" cybersecurity risks—ultimately culminating in the SUNBURST catastrophe. (A94 ¶113).[3] The trial court, however, found such allegations insufficiently pled and dismissed the action pursuant to Court of Chancery Rule 23.1. The Court of Chancery's decision was in error. Straightforward application of *Caremark* and *Marchand* demonstrate the sufficiency of Plaintiffs' allegations and mandate reversal.

1. The trial court erred in finding Plaintiffs failed to plead bad faith under *Caremark* prong one.

(a) Plaintiffs' allegations satisfy *Marchand*.

Marchand holds that a reasonable inference of a bad faith failure to satisfy the duty of oversight follows from: (i) the existence of a mission critical risk to corporate interests; and (ii) the lack of any Board-level system of monitoring or reporting on that issue. Where a plaintiff pleads such facts, it is entitled to a pleading-stage inference of bad faith. *See Marchand*, 212 A.3d at 822 ("When a plaintiff can plead an inference that a board has undertaken no efforts to make sure it is informed of a

[3] Six of those directors—Defendants Bock, Boro, Hao, Hoffmann, Kinney, and Lines—served on the Board continuously from the Company's October 2018 IPO until the commencement of this action, and these individuals alone constitute a majority of the Demand Board. *Id.* The two others—Defendants Sundaram and Widmann—joined the Board in February 2020 and served for a substantial part of the relevant time period. *Id.* In addition, Defendant Widmann also personally attended the February 2019 Cybersecurity Briefing. *Id.*

compliance issue intrinsically critical to the company's business operation, then that supports an inference that the board has not made the good faith effort that *Caremark* requires."); *id.* at 824 ("In Blue Bell's case, food safety was essential and mission critical. The complaint pled facts supporting a fair inference that no board-level system of monitoring or reporting on food safety existed.").[4]

Here, Plaintiffs have met the standard set forth in *Marchand*. Plaintiffs have adequately pled that cybersecurity threats constituted *the* "mission critical" risk to SolarWinds in the years leading to the SUNBURST catastrophe. This is not hindsight bias or, as the trial court put it below, Plaintiffs' counsel reciting a "shibboleth arising from *Marchand*" (Op. 3). SolarWinds' leaders on the Board and in management were expressly put on notice of the unique and existential importance of cybersecurity to the Company. The February 2019 Cybersecurity Briefing to the NGC expressly identified cybersecurity threats as "***mission critical to SolarWinds' business***" (A21-A53 ¶¶39–43), and the Company's own Global Cybersecurity

[4] Throughout the Opinion below, the trial court emphasized its views concerning the importance of "scienter" in pleading bad faith. *Marchand*, however, stands for the proposition that all of the prerequisites for bad faith are demonstrated, at least at the pleading stage, where a plaintiff can plead the two essential elements: (i) the existence of a mission critical risk to corporate interests; and (ii) the lack of any Board-level system of monitoring or reporting on that issue. As detailed herein, Plaintiffs have met this standard.

Strategist resigned under protest after expressing to management that the Company's "***lack of security***" was threatening the very "***survival of the company***" (A86 ¶97). These warnings came amid a chorus of outside voices—including the SEC, NYSE, FBI, White House, and other major organizations—sounding alarm bells about the critical importance of cybersecurity for companies generally. (A61 ¶56, A66 ¶64, A68 ¶68).

The importance of cybersecurity for SolarWinds in particular, given its status as the holder of "Cyber Crown-Jewels" most coveted by hackers (A49 ¶39), was paramount. Just as "food safety was essential and mission critical" for an ice cream manufacturer, *Marchand*, 212 A.3d at 824, and "airplane safety was essential and mission critical" for an airplane manufacturer, *Boeing*, 2021 WL 4059934 at *26, cybersecurity was unquestionably essential and mission critical for SolarWinds—a monoline provider of software granted trusted access with full privileges to the IT systems of its customers, including the principal United States national security agencies and a majority of the Fortune 500 companies. (A44-A61 ¶¶33–57). Accordingly, Plaintiffs have unquestionably pled that cybersecurity constituted the type of "mission critical" risk requiring systematic Board-level oversight under *Marchand*.

Plaintiffs likewise have adequately "pled facts supporting a fair inference that

no board-level system of monitoring or reporting on [cybersecurity] existed." *Marchand*, 212 A.3d at 824. Armed with the 220 Production, Plaintiffs have alleged an utter "dearth of any board-level effort at monitoring," *Marchand*, 212 A.3d at 809, that is effectively on all-fours with *Marchand* and the Court of Chancery's subsequent decision sustaining oversight claims in *Boeing*. In *Marchand*, the Supreme Court found that the following alleged facts supported a reasonable inference that the defendant directors failed to make a good faith effort to ensure that there was a system of board-level monitoring and reporting concerning food safety:

> (i) No board committee addressed food safety;
>
> (ii) No regular process or protocols existed requiring management to keep the board apprised of food safety compliance practices, risks or reports;
>
> (iii) No schedule existed for the board to consider food safety risks on a regular basis;
>
> (iv) During a key period, management received reports containing red or yellow flags, but there was no evidence of their disclosure to the board;
>
> (v) The board was given certain favorable information, but was not given important reports presenting a much different picture; and
>
> (vi) Food safety issues were not regularly discussed at board meetings.

212 A.3d at 822. In *Boeing*, where the plaintiffs brought "remarkably similar factual allegations" to those in *Marchand*, similar deficiencies supported the same inference. *Boeing*, 2021 WL 4059934, at *26. The same is true here.

As in *Marchand* and *Boeing*, neither the SolarWinds' Board nor any committee thereof had any "regular process or protocols that required management to keep the board apprised of [cybersecurity] compliance practices, risks, or reports." *Marchand*, 212 A.3d at 822 (substituting "cybersecurity" for "food safety"). Nor did any "schedule for the board to consider on a regular basis … any key [cybersecurity] risks exist[]." *Id.* And, as in *Marchand* and *Boeing*, the records of SolarWinds' "board meetings are devoid of any suggestion that there was any regular discussion of [cybersecurity] issues." *Id.* Further, as in *Marchand* and *Boeing*, "during a key period … management received reports that contained what could be considered red, or at least yellow, flags,"—most notably the "solarwinds123" password incident reported to management approximately one year before SUNBURST—"and the board minutes of the relevant period revealed no evidence that these were disclosed to the board." *Id.* And while SolarWinds had Board committees that were nominally delegated the task of overseeing cybersecurity, in reality "no board committee [ ] addressed [cybersecurity]" (*id.*): (i) the Audit Committee *never once even discussed* cybersecurity; (ii) the NGC

utterly failed to monitor cybersecurity between the February 2019 Cybersecurity Briefing that highlighted the "mission critical" nature of cybersecurity risks to SolarWinds's business and the December 2020 revelation of SUNBURST; and (iii) neither the Audit Committee nor the NGC ever reported to the full Board on cybersecurity matters. These undisputed facts are on all fours with those supporting denial of Rule 23.1 motions by this Court in *Marchand* and by the Court of Chancery in *Boeing*.

(b) The trial court incorrectly held that the nominal delegation of oversight was sufficient to satisfy *Marchand*

Notwithstanding the remarkable similarity between Plaintiffs' allegations and those sustained in *Marchand* and *Boeing*, the trial court below dismissed Plaintiffs' claims. It found Plaintiffs had pled that SolarWinds had a "subpar reporting system," but a system nonetheless, and thus granted Defendants' motions to dismiss. (Op. 35). Specifically, the trial court found—based on improper defense-friendly inferences and a misinterpretation of Plaintiffs' claims—that the mere existence of two Board committees "charged with oversight responsibility for cybersecurity" (Op. 30), *i.e.* the Audit Committee and the NGC, ultimately constituted a sufficient system to preclude a finding of bad faith. This holding must be reversed. The nominal delegation of oversight to Board committees concerning a "mission critical"

risk does not constitute a "reporting system," particularly if those committees never actually provide any oversight.

(i) Plaintiffs allege, consistent with SolarWinds's books-and-records, that neither the Audit Committee nor the NGC ever exercised oversight concerning cybersecurity.

From the IPO until SUNBURST was discovered, the Audit Committee was responsible for overseeing data security risks and discussing with management the Company's major financial risk exposures, including cyber and data security. (A70 ¶39). However, the Audit Committee wholly failed to discharge these important responsibilities: it never once met with management to assess cybersecurity risks or convened any committee meeting to discuss cyber or data security. *Id*. Simply having a committee with certain responsibilities means nothing if the committee does not actually do anything to fulfill those responsibilities. *See Hughes v. Hu*, 2020 WL 1987029, at *14–16 (Del. Ch. Apr. 27, 2020) ("mere existence of an audit committee" insufficient to withstand *Caremark* claim where the committee (did not locate this cite) "utterly failed to actually meet its responsibilities"); *Rich v. Chong*, 66 A.3d 963, 983 (Del. Ch. 2013) (*Caremark* claim sustained, despite the existence of an audit committee and independent auditor, where company had no "meaningful controls in place").

The NGC, for its part, received the February 2019 Cybersecurity Briefing highlighting the "mission critical" risk to the Company posed by cybersecurity threats, and in April 2019 assumed its own responsibility for cybersecurity oversight. (A72 ¶75). However, like its sister Audit Committee, the NGC did not actually fulfill that responsibility. The NGC never reported to the full Board about the Cybersecurity Briefing (or about cybersecurity at all), and never held a single meeting or discussion about cybersecurity after the Cybersecurity Briefing. (A65 ¶63, A70-A72 ¶¶73–75).

There is absolutely nothing in the record or the 220 Production reflecting any actual exercise of oversight concerning cybersecurity by the Audit Committee or NGC in the nearly two years between the February 2019 Cybersecurity Briefing and the revelation of SUNBURST in December 2020. Plaintiffs' 220 demands requested all books and records reflecting all Board (and Board committee) oversight regarding cybersecurity, and the Company produced documents after a full and fair opportunity to search its own records. The Company certified that its production was complete (and even had an additional post-hoc opportunity to further supplement its production).[5] If exculpatory evidence existed, Defendants would

[5] Nearly six months after certifying that their production was complete, and just days

have produced it. At the pleading stage, the absence of any Board materials reflecting oversight by the Audit Committee or the NGC provides a strong inference that no such materials exist. *See Boeing*, 2021 WL 4059934, at *1 n.1 ("It is reasonable to infer that exculpatory information not reflected in the document production does not exist."); *In re Tyson Foods, Inc. Consol. S'holder Litig.*, 919 A.2d 563, 578 (Del. Ch. 2007) ("it is more reasonable to infer that exculpatory documents would be provided than to believe the opposite: that such documents existed and yet were inexplicably withheld."). Simply put, "[i]n order to rule in Defendants' favor, [the Court] would need to read words into [] Committee minutes that do not appear and take inferences in their favor." *H & N Mgmt. Grp., Inc. v. Couch*, 2017 WL 3500245, at *5 (Del. Ch. Aug. 1, 2017). But "[a]t this stage," the Court "must take all reasonable inferences in favor of the non-moving party." *Id.*

---

before they were due to respond to the Complaint, Defendants produced a handful of additional documents reflecting a *de minimus* reference to cybersecurity by the Audit Committee in April 2020 in relation to the outbreak of the Covid-19 pandemic. *See* A243-A244; *see also* Op. at 29 n.119. This passing mention of cybersecurity does nothing to diminish the inference that the Audit Committee failed to make a good faith effort to oversee cybersecurity at all, much less in the rigorous and systematic fashion *Marchand* requires. Indeed, Defendants' failure to produce these documents in the first place reflects their own understanding that this negligible allusion to cybersecurity has no bearing on this case. Regardless, Plaintiffs respectfully reiterate their argument that the Court should not consider these late-produced documents. *See* A243-A244.

(ii) The trial court improperly discounted Plaintiffs' allegations of Board and committee-level oversight failures.

The trial court effectively ignored Plaintiffs' well-pled allegations that the Audit Committee and NGC failed to exercise meaningful oversight. Instead, based on the fact that the Audit Committee and NGC were nominally "charged with oversight responsibility for cybersecurity" (Op. 30), the trial court misconstrued the Complaint as asserting *only* a failure by the committees to report to the full Board on cybersecurity. *See* Op. 32 ("In fact, as I understand the Plaintiffs' argument, they urge me to infer bad faith on the part of the Committees' members solely based on the fact that in the two years following the delegation of responsibility regarding cybersecurity, the Committees failed to report to the full Board on the subject."). Thus, the trial court construed the failure of the committees to report to the full Board as the sole basis for the alleged breach of duty. The trial court then dismissed this claim by holding that the business judgment rule applies to committees' decisions regarding what to report to the full Board. Specifically, the Court held:

> Board committees, as delegees of Board authority, must exercise their members' business judgment in determining what items are on the agenda for any given meeting. They must also exercise business judgment in determining what issues should be brought from the subcommittee to the full Board. Such exercises of business judgment

> are protected by exculpatory clauses such as the one SolarWinds had in place here.

Op. 33.

The trial court's analysis is erroneous for multiple reasons.

First, the utter failure of the Audit Committee or NGC to report to the full Board concerning cybersecurity is only one component of Plaintiffs' allegations. Plaintiffs have alleged a failure by SolarWinds' directors to perform *any* cybersecurity oversight at all, either at the Board or the committee level for nearly two years. *See Hughes*, 2020 WL 1987029, at *15 ("[C]hronic deficiencies support a reasonable inference that the Company's board of directors, acting through its Audit Committee, failed to provide meaningful oversight over the Company's financial statements and system of financial controls").

Second, the trial court improperly inferred good faith oversight by the full Board based solely on the Board's mere delegation of oversight responsibility to the committees. *See* Op. 34. This is contrary to *Marchand*, which repeatedly emphasized that oversight concerning "mission critical" areas is an obligation of the entire board. *See Marchand*, 212 A.3d at 823; *Boeing*, 2021 WL 4659934, at *26 (applying "*Marchand's* mandate that the board rigorously exercise its oversight function with respect to mission critical aspects of the company's business"). Thus,

the mere delegation of oversight responsibility without more does not and cannot support a finding of good faith under *Marchand* at the pleading stage.

Third, the trial court disregarded and failed to credit the Complaint's particularized allegations about the committees' wholesale failures to carry out their oversight duties. The Complaint clearly alleges—with particularity based on Defendants' 220 Production—that the directors on the Audit Committee and NGC breached their oversight duties by failing to carry out any oversight through those committees over a two-year period, even though those committees were expressly delegated responsibility for oversight of cybersecurity risks. As Plaintiffs alleged, neither the Audit Committee nor the NGC ever prepared any report regarding cybersecurity, and never even met to discuss that "mission critical" subject for nearly two years. (A34-A35 ¶10, A52-A53 ¶42, A69-A72 ¶¶71–75, A74 ¶78).

Fourth, the trial court appears to have drawn the unreasonable and unsupported inference that the committees in fact performed their oversight obligations, but merely failed to report their findings or actions regarding cybersecurity. In particular, the trial court speculated that another meeting concerning cybersecurity occurred after February 2019 because the NGC's charter was amended to expressly delegate that committee with responsibility for cybersecurity oversight. Op. 32 ("Following the Cybersecurity Briefing, the NGC

Committee in April 2019 amended its charter to expressly address cybersecurity, indicating that the topic had arisen at a subsequent meeting") (footnote omitted). Not only is this an unreasonable inference to draw in favor of Defendants, it is in fact untrue: as alleged based on Defendants' 220 Production, the NGC never met again to discuss cybersecurity after the Cybersecurity Briefing(A34-A35 ¶10, A70-A72 ¶¶73–75).

Fifth, the trial court observed that the Complaint does not allege that the Audit Committee or NGC were "shams" that utterly "failed to meet." (Op. 31, 34). Committee meetings on entirely unrelated topics, however, cannot constitute oversight of the mission-critical risk at issue, any more than completely unrelated Board meetings could do so. Whatever unrelated activities they may have engaged in, the Audit Committee's and NGC's purported oversight of cybersecurity risks was indeed a sham.

Sixth, the trial court criticizes Plaintiffs for failing to allege "what information Committee members possessed which raised a good-faith duty to report." Op. 33. That criticism is absurd. The committees had nothing to report because they failed to conduct any oversight or even discuss cybersecurity at all. That is, in fact, the basis of Plaintiffs' "prong one" *Caremark* claim. The notion that board committees must "exercise business judgment in determining what issues should be brought

from the subcommittee to the full Board" (Op. 33) has no relevance when those committees utterly fail to monitor a mission-critical risk for years on end.

Finally, the trial court held that it would be "unwarranted" to "hold members of Board committees liable for failure to discuss one particular business risk with the full Board over a period of 26 months—while contending with the transition to life as a public company and the novel coronavirus pandemic[.]" Op. 33. While the committees' failure to report to the full Board regarding cybersecurity for over two years (and the full Board's failure to demand such reports) is far from the only basis for *Caremark* liability in light of the committee failures discussed above, it is nonetheless highly relevant. Neither *Caremark* nor *Marchand* suggest SolarWinds' Board could place the mission-critical risk of cybersecurity on the back burner for over two years and completely ignore it just because it coincided with other risks. And unlike the cybersecurity risks, there is no record evidence that coronavirus or the "transition to life as a public company" posed *mission-critical risks to SolarWinds in particular*. Nor does any record evidence counterintuitively suggest that fast-moving cyber threats can reasonably be monitored less than once every two years, on no schedule whatsoever. Fundamentally, cybersecurity was not merely "one particular business risk" or "a *particular* incarnation of risk" for SolarWinds, as the trial court indicated. Op. 22, 33. Rather, cybersecurity was central and

mission-critical to SolarWinds' core business, yet SolarWinds' Board, including both the Board acting as a whole and the Board acting through committees, utterly failed to monitor it as such.

(iii) The trial court's erroneous interpretation of Plaintiffs' allegations regarding committee-level oversight failures caused the Court to perform a faulty demand futility analysis

The trial court also performed an erroneous demand futility analysis. That analysis was based on the trial court's erroneous misconstruction of the Complaint as asserting breaches by the full Board based "solely" on the full Board's failure to receive committee reports (or to inquire about any such reports). *See* Op. 32 (Plaintiffs allege "bad faith on the part of the Committees' members solely based on the fact that the Committees failed to report to the full Board the subject"), 34 ("The fact that the Board did not receive reports from the Committees with respect to cybersecurity … does not implicate bad faith—instead, it goes to the duty of care, not loyalty.") (footnote omitted). The trial court's misconstruction of Plaintiffs' claims thus undermined the trial court's entire demand futility analysis.

The Demand Board comprises eleven directors, six of whom served on the Board at all times from the October 2018 IPO to the present (Bock, Boro, Hao, Hoffman, Kinney and Lines). (A66 ¶113). Another two directors joined the Board

in February 2020 and therefore served on the Board for a substantial part of the relevant time and are likewise liable for their failure to implement or oversee any reasonable system of cybersecurity oversight (Sundaram and Widmann). *Id*. Thus, a clear majority of the Demand Board (six of eleven) served on the Board at all relevant times, and another two directors face liability for their service for a portion of the relevant time. These facts alone establish demand futility, but the trial court failed to apply this demand futility analysis.[6]

Every member of the Board had an oversight duty but none of them made any good faith effort to fulfill that duty. Merely delegating oversight responsibility to committees and forgetting about it does not satisfy the directors' fiduciary duties of oversight under *Marchand*.

Moreover, a clear majority of the Demand Board members served on the Audit Committee and/or the NGC or have conflicting ties to those who did. Bock,

[6] *See United Food & Com. Workers Union & Participating Food Indus. Employers Tri-State Pension Fund v. Zuckerberg*, 262 A.3d 1034, 1059 (Del. 2021) (demand futile where at least half of the board members (i) "face a substantial likelihood of liability on any of the claims that are the subject of the litigation demand" or (ii) lack independence from someone "who would face a substantial likelihood of liability on any of the claims that are the subject of the litigation demand") (citation omitted); *Hughes*, 2020 WL 1987029, at *17 (demand futile where "the defendants who face a substantial likelihood of [*Caremark*] liability constitute a majority of the Demand Board").

Cormier, Howard, Kinney, Lines, Sundaram, and White all served on Audit Committee (A38-40 ¶¶21, 23, A41-A44 ¶¶26–29, 31), and Bingle, Cormier, Kinney, Sundaram served on the NGC (A38 ¶20, A39-A40 ¶23, A41-A42 ¶27, A42-A43 ¶29), each for all or a substantial portion of the relevant time. Defendants Windmann and Smith are also disabled from considering Plaintiffs' demand due to their positions at Silver Lake, where other directors (Bingle, Hao and White) also held important positions (as managing partner, director or senior advisor). (A94-A95 ¶¶114–115). As a result of misconstruing Plaintiffs' allegations and failing to credit the alleged committee-level oversight failures, the trial court failed to consider the disabling conflicts confronting the committee members as an independent basis of demand futility, and thus the trial court failed to apply the proper demand futility analysis.

2. The trial court erred in finding Plaintiffs failed to plead bad faith under *Caremark* prong two.

Alternatively, the trial court erred in also holding that Defendants did not ignore red flags to establish demand futility under *Caremark's* prong two.

Caremark's second prong "is implicated when it is alleged the company implemented an oversight system but the board failed to monitor it." *In Re Clovis Oncology, Inc. Deriv. Litig.*, 2019 WL 4850188, at *13 (Del. Ch. Oct. 1, 2019)

(citing *Marchand*, 212 A.3d at 821) (internal punctuation omitted); *see also Boeing*, 2021 WL 4059934, at *33 ("A classic prong two claim acknowledges the board had a reporting system, but alleges that system brought information to the board that the board then ignored."). To state a claim under *Caremark*'s second prong, Plaintiffs must plead particularized facts that the Board knew of "proverbial 'red flag[s]'—yet acted in bad faith by consciously disregarding its duty[.]" *Horman v. Abney*, 2017 WL 242571, at *10 (Del. Ch. Jan. 19, 2017).

Here, Plaintiffs' Complaint identifies significant "red flags" concerning cybersecurity that went unheeded by SolarWinds' Board. For example, the February 2019 Cybersecurity Briefing constituted a glaring red flag warning that SolarWinds was an "*attractive target*" for rapidly increasing cyberattacks due to the Company's unique "Cyber 'Crown-Jewels.'" (A262 ¶¶39-40). Rather than taking steps to minimize the threat to the Company's core business, the NGC "ignored" that warning." (A70 ¶73). Despite these specific allegations, the trial court incorrectly concluded that pleading that the NGC effectively ignored the presentation is "conclusory." Op. 27. That is not so. There is no evidence in the record that the NGC took any steps in response to protect the Company's core business. Similarly, notwithstanding the Company's major unaddressed cybersecurity deficiencies, the trial court wrongly concluded the Complaint did "not ple[a]d that the presentation

made action by the Board necessary." *Id*.

Faced with these allegations, the trial court erred when it found that this presentation was not a red flag, but "an instance of oversight." (Op. 27). A single meeting with generic references to cybersecurity measures does not constitute adequate oversight. Nor does it satisfy Defendants' exacting oversight obligations, much less in the face of the stark warnings presented at the Cybersecurity Briefing. *See, e.g.*, *Boeing* at *28 ("The Board and management's passive invocations of quality and safety, and use of safety taglines, fall short of the rigorous oversight *Marchand* contemplates."). Further, (i) Defendants "did not follow up on whether management actually carried out" any measures mentioned in the Cybersecurity Briefing, (ii) there is no Board-level evidence that any "policies or procedures were implemented, revised, or updated in response" to the Cybersecurity Briefing, (iii) the Cybersecurity Briefing was "not presented to [SolarWinds'] full Board," and (iv) "neither the Board nor [any] Committee received subsequent reports" on the Cybersecurity Briefing or any other aspect of the Company's mission critical cybersecurity concerns. *Teamsters Local 443 Health Serv. & Ins. Plan v. Chou*, 2020 WL 5028065, at *12 (Del. Ch. Aug. 24, 2020).

Indeed, the trial court noted its confusion when comparing this case to *Firemen's Ret. Sys. of St. Louis v. Sorenson*, 2021 WL 4593777 (Del. Ch. Oct. 5,

2021): "What is not wholly clear to me is that cybersecurity incidents of the type suffered by SolarWinds and in *Sorenson*—involving crimes by malicious third parties—present a sufficient nexus between the corporate trauma suffered and the Board for liability to attach." (Op. 19). This case, however, is easily distinguishable from *Sorenson*, a case about a data breach at the Marriott hotel company, not a monoline IT network management company whose Board knew it was an attractive target for increasingly common cyberattacks. The Cybersecurity Briefing itself shows that SolarWinds' trusted access to its large customer base subjected the Company to specific and growing cybersecurity threats inherent to its core business that were "mission critical" by the Company's own admission, and to which the trial court also agreed. (Op. 1). In contrast, Marriott had only the generic cybersecurity concerns present at any corporation. By not taking any action, Defendants here provided an open door and easy access for those criminal activities in violation of their oversight duties.

Sorenson is also inapposite because, unlike here, the Marriott board actually took (and was made aware of) remedial action to address Marriott's cybersecurity issues. Indeed, if anything, *Sorenson* provides a real-world example of a hotel chain whose Board paid far greater attention to cybersecurity than SolarWinds, the world's premier IT network manager.

Unlike this case—in which Defendants expressly knew the Company was an "***attractive target***" that could "[a]t any point … ***face a more sophisticated adversary***" (¶39 (emphases in original)) but did nothing—Marriott's board took decisive steps in response to relatively anodyne warnings. These warnings included, for example, that Marriott's cybersecurity was rated as "needs improvement," that its incident response plan was "not up to date," and that certain of its data security standards allowed a "greater opportunity for deviation from the expected published standard." *Sorenson*, 2021 WL 4593777, at *16. In response, Marriott's board learned of "efforts made ***immediately*** to remedy" these issues, and that "management had enhanced monitoring, expanded enterprise security logging and event management, and expanded the use of third party monitoring among other numerous actions." *Id.* The Court of Chancery also found that, after Marriott's data breach occurred, "the Board continued to receive detailed updates on the ***incredible amount of work***" management did in response. *Id.* at *17 (internal punctuation omitted; emphasis added). Given the Marriott board's knowledge and oversight of management's earnest efforts, the Court of Chancery found that the plaintiffs' allegations were insufficient to support an inference that the board members breached their oversight duty under *Caremark*. *Id.*

The allegations here are a world apart. Rather than being warned that

SolarWinds' cybersecurity merely "need[ed] improvement" or had "out of date" protocols, the Cybersecurity Briefing explicitly warned the Board that SolarWinds was an "attractive target" because its products were "Cyber 'Crown-Jewels'" with "***trusted access***" to SolarWinds' "large, attractive ***customer base***" of over 275,000 high-value clients, which was "***mission critical*** to SolarWinds' business operations." (A48-A50 ¶39 (emphasis in original)). Consistent with industry-wide warnings, the Cybersecurity Briefing specifically warned further that the risk was increasing, with a "124% increase" in attacks against the Company over the previous year, and that "[a]t any point we ***may face a more sophisticated adversary***." (A48-A50 ¶39, A51 ¶41) (emphasis in original). Given SolarWinds' limitless access to its customers' networks, these warnings represented clear red flags that should have triggered Board action.

Yet, the Board here took no action, doing nothing to respond to or follow up on the February 2019 presentation. (A70-A72 ¶¶73–74). Nor did it receive detailed periodic updates from management. Defendants' 220 Production shows that following the Cybersecurity Briefing, the Board and its committees held no substantive discussions whatsoever until the Company learned of the SUNBURST catastrophe almost two years later. (A72 ¶76).

Moreover, the red flags in the Cybersecurity Briefing do not stand alone.

Rather, those warnings came in the context of other concrete security lapses at the Company, and amidst a drumbeat of warnings from industry participants that the risk of a supply chain cyberattack (like SUNBURST) was rapidly increasing. Although those warnings "alone could serve as [] red flag[s] sufficient to make it reasonably conceivable that the [] Defendants face a substantial likelihood of liability," those red flags also, at a minimum, "serve[] as a backdrop against which the other pled red flags must be viewed." *Chou*, 2020 WL 5028065, at *20.

The trial court rejected the Complaint's other allegations of red flags because it found that the Board was unaware of them.[7] For example, the trial court acknowledged that the Complaint alleges that the "Company had a jejune, even farcical, password—'solarwinds123'—in place in a manner that could have compromised the Company security from as early as 2017 until November 2019." Op. 28. The trial court, however, found that "there is no indication that either the Committees or the full Board were ever apprised of the password deficiency," and

[7] This, of course, is the point of Plaintiffs' "prong one" claim. Had the Board implemented and monitored a reasonable reporting system, that system would necessarily have brought these myriad significant red flags to the Board's attention. The fact that those red flags did not reach the Board proves that the Board did nothing to actually "*monitor*" the reporting system that it claims to have implemented, as Delaware law requires. *Clovis*, 2019 WL 4850188, at *1 (emphasis in original).

"[w]ithout such knowledge, the Board again cannot have acted in bad faith." *Id*. Any reasonable system of cybersecurity oversight would have brought that glaring red flag to the Board's attention on an emergency basis. The fact that the Board never even learned of it confirms that Defendants did not actually monitor any reasonable oversight or reporting system regarding the Company's known mission critical cybersecurity risks.

Likewise, Mr. Thornton-Trump, SolarWinds' "Global Cybersecurity Strategist," warned the Company's top management that, among other things, SolarWinds suffered from "minimal security leadership at the top" and from a lack of "internal commitment to security," and resigned in protest. (A86 ¶97). The Complaint further alleges a litany of dire government and industry warnings putting the Board on notice to take action with respect to the Company's mission critical cybersecurity risk. (A53-A61 ¶¶44–56). The trial court incorrectly characterized those allegations as a "plethora of background facts about the increasing need for technology companies, in general, to address cybersecurity." Op. 4. Again, SolarWinds is not a generic company facing run-of-the-mill cybersecurity risks. Cybersecurity was a mission critical risk area for SolarWinds, and the warnings detailed in the Complaint should have—at a minimum—prompted the Board to take action in response to the February 2019 Cybersecurity Briefing and other red flags.

3. The trial court erred in suggesting Plaintiffs failed to plead a violation of positive law, or that a violation of positive law is a necessary predicate to a *Caremark* claim

Throughout the Opinion below, the trial court expressed its skepticism that a *Caremark* claim can be pled without a showing that the alleged oversight failures resulted in a violation of positive law, apparently based on its view that the SUNBURST incident involved no violation of positive law. Though the trial court did not seek to resolve the question (Op. 20), the trial court's skepticism appears to have influenced its analysis. *See, e.g.*, Op. 22 (suggesting that greater scrutiny might be required for bad faith claims involving "risk outside the realm of positive law"). To the extent this distinction influenced the trial court's analysis, the trial court's skepticism rested on faulty premises.

As an initial matter, the Complaint *does* support the existence of violations of positive law by SolarWinds in connection with the SUNBURST incident. Specifically, it supports that SolarWinds's cybersecurity deficiencies that proliferated in the years prior to SUNBURST caused SolarWinds to breach its federal disclosure obligations. (A62 ¶59). Though the trial court dismissed the SEC's interpretative guidance concerning cybersecurity-related disclosures as nonbinding (Op. 24), this ignores that the SEC's guidance interpreted unquestionably binding federal securities laws. Indeed, a federal district court has

sustained allegations that the Company violated those laws, holding that "the cybersecurity measures at the company were not as they were portrayed, such as the "'solarwinds123'" password incident, the statements of former employees, and Thornton-Trump's presentation." *In re SolarWinds Corp. Sec. Litig.*, 595 F. Supp. 3d 573, 588 (W.D. Tex. 2022), *opinion clarified*, 2022 WL 3699429 (W.D. Tex. Aug. 19, 2022).[8] Moreover, the Company has since announced that the SEC has issued it a "Wells Notice" stating "that the SEC staff has made a preliminary determination to recommend that the SEC file an enforcement action against the Company alleging violations of certain provisions of the U.S. federal securities laws with respect to its cybersecurity disclosures and public statements[.]"[9] Accordingly, the trial court's conclusion that Plaintiffs' claims do not involve violations of positive law is wrong.[10]

---

[8] After losing on its motion to dismiss, the Company has agreed to settle that securities class action for $26 million.

[9] *See* Form 8-K filed 11/3/22, available at: https://www.sec.gov/ix?doc=/Archives/edgar/data/0001739942/000173994222000091/swi-20221028.htm

[10] The trial court further dismissed the relevance of securities laws and related guidance on the basis that they pertain to cybersecurity-related disclosures rather than actual cybersecurity procedures. (Op. 25). This distinction, however, means little. Either way, it is fairly pled that the Board's failure to inform itself of the Company's cybersecurity practices, and the glaring inadequacies proliferating therein, caused the Company to violate positive law—in addition to incurring

But even if the Complaint did not support the existence of a violation of positive law (it does), that would not end the inquiry. Though compliance issues are important to all companies and it is compliance failures that most typically lead to *Caremark* litigation, legal compliance is only one facet of directors' duty to exercise oversight: "[u]nder *Caremark* and this Court's opinion in *Stone v. Ritter*, directors have a duty 'to exercise oversight' and to monitor the corporation's ***operational viability, legal compliance, and financial performance.***" *Marchand*, 212 A.3d at 809 (citing *Stone v. Ritter*, 911 A.2d 362 (Del 2006) and *Caremark*, 698 A.3d 959) (emphasis added).

Issues of the "mission critical" nature described in *Marchand* are issues that implicate operational viability and are of overwhelming significance to a company's financial performance, regardless of whether a company manages to nominally comply with positive law. Indeed, *Marchand* itself explains that, in the sphere of mission critical activities, a company's *mere compliance* with positive law is insufficient to absolve its directors for failures to implement an appropriate oversight system. *Id.* at 823 ("But the fact that Blue Bell nominally complied with FDA regulations does not imply that the *board* implemented a system to monitor food

---

catastrophic reputational and financial harm by failing in a core and critical aspect of its business operations.

safety at the *board level*."); *see also Boeing*, 2021 WL 4059934, at *28 ("As *Marchand* made plain, the fact that the company's product facially satisfies regulatory requirements does not mean that the board has fulfilled its oversight obligations to prevent corporate trauma.").

Moreover, given directors' obligation to monitor not only their corporation's "legal compliance," but also its "operational viability … and financial performance," *Marchand*, 212 A.3d at 809, there is no principled basis on which to conclude that directors should only be held liable for a failure to monitor mission critical risks when that failure results in violations of positive law, but not when it results in other forms of catastrophic harm to the corporate weal. Where a board carefully considers mission critical risks and makes a reasoned judgment to pursue a dubious but legal course of action, such a decision may not give rise to a claim under *Caremark* or *Marchand*. But where, as here, a Board utterly fails to exercise any oversight whatsoever concerning mission critical risks and that failure of oversight allows glaring deficiencies threatening the very "*survival of the company*" (A86 ¶97) to persist, that Board cannot escape liability for the catastrophic results of such inaction.

CONCLUSION

The judgment below should be reversed.

Dated: December 20, 2022

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

SAXENA WHITE P.A.

/s/ Thomas Curry
Thomas Curry (#5877)
Tayler D. Bolton (#6640)
824 N. Market Street, Suite 1003
Wilmington, DE 19801
(302) 485-0480

Counsel for Plaintiffs

Of Counsel:

ROBBINS GELLER RUDMAN
& DOWD LLP
Chad Johnson
Noam Mandel
Desiree Cummings
Jonathan Zweig
420 Lexington Avenue, Suite 1832
New York, NY 10170
(212) 432-5100

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
(888) 529-1108

KASKELA LAW LLC
D. Seamus Kaskela
18 Campus Blvd., Suite 100
Newton Square, PA 19073
(888) 715-1740

Counsel for Plaintiff Lawrence Miles

COHEN MILSTEIN SELLERS
& TOLL PLLC
Julie Goldsmith Reiser
1100 New York Avenue, N.W.,
Fifth Floor
Washington, DC 20005-3964
(202) 408-4600

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

Counsel for Plaintiff Brian Seavitt