EFiled: Feb 23 2023 09:42AM EST
Filing ID 69200597
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 PUBLIC VERSION FILED FEBRUARY 23, 2023**

APPELLANTS' REPLY 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

TABLE OF AUTHORITIES

Page(s)

Cases

PRELIMINARY STATEMENT

The pleading stage record and Plaintiffs' well-pled allegations establish that the SolarWinds Board never established a system to monitor the "mission critical" risk that cybersecurity posed to the Company.[1] Defendants do not and cannot dispute that cybersecurity was, in fact, a mission critical risk, yet an utter "dearth of any board-level effort at monitoring"[2] persisted for years on end, resulting in the SUNBURST catastrophe. Neither the Board as a whole nor the Audit Committee specifically charged with overseeing cybersecurity issues *ever* received a single report or held a single discussion regarding cybersecurity. The lone instance of director engagement was a different committee's receipt of a single management presentation two years prior to SUNBURST, which [redacted] Even then, the Board did nothing to establish an oversight system and *actually* monitor mission critical cybersecurity risks.

[1] Unless otherwise stated, defined terms have the same meaning ascribed to them as in Appellants' Opening Brief.

[2] *Marchand v. Barnhill*, 212 A.3d 805, 809 (Del. 2019).

Defendants' contrary narrative distills to a conclusory assertion that, under *Caremark*'s first prong, "the SolarWinds Board in fact had an effective board-level cybersecurity monitoring and reporting system in place."[3] Essentially, Defendants ask this Court to elevate form over substance and conclude that the mere *creation* of Board committees tasked with overseeing a mission critical risk, and the mere *recognition* by a Board committee that the risk is in fact mission critical, themselves establish sufficient oversight. In fact, having failed to establish the necessary system of oversight, the Board failed to actually monitor cybersecurity risk, whether acting as a whole or through committees, for two years. Defendants' assertions that the Committees did exercise some degree of oversight rely on defense-friendly inferences that are wholly improper at the pleading stage and are inconsistent with Plaintiffs' well-pled allegations and the evidence that supports them.

Defendants' further argument that *Caremark* liability is foreclosed because Plaintiffs have not alleged violations of positive law not only defies Delaware law, but also ignores that Plaintiffs' allegations would establish liability even under that imagined standard.

[3] Appellees' Answering Brief (Trans. ID 68935252) ("Answering Brief") at 2.

Finally, Defendants' argument for escaping liability under *Caremark*'s second prong requires the Court to ignore the red flags paraded before the Board. Worse, it requires the Court to instead find that the directors of this monoline software company that suffered the very catastrophic fate about which it was expressly warned—and yet which failed to respond in any way to those warnings—are entitled to pleading stage dismissal as a matter of law.

In short, Defendants' Answering Brief achieves nothing more than echoing the trial court's reversible error. The well-pled allegations establish that this Action is fundamentally indistinguishable from this Court's *Marchand* decision. Delaware law—and coherence with *Marchand*—mandate reversal.

ARGUMENT

I. A MAJORITY OF SOLARWINDS' BOARD FACED A SUBSTANTIAL LIKELIHOOD OF LIABILITY UNDER *CAREMARK*'S FIRST PRONG

A. SolarWinds Had No Board-Level System to Monitor Mission Critical Cybersecurity Risk

Plaintiffs' well-pled allegations show that SolarWinds lacked any board-level cybersecurity monitoring or oversight system. From its inception as a public company: (i) SolarWinds' full Board never conducted any cybersecurity-related meetings or discussions; (ii) the Nominating and Governance Committee held a single meeting in February 2019 during which [redacted] (iii) no other committee conducted any cybersecurity oversight; (iv) there was no mandatory requirement that management report to the Board or any committee concerning cybersecurity; (v) there was no schedule for the Board or any committee to address cybersecurity, and no other requirement for Board or committee meetings to regularly focus on cybersecurity; and (vi) there were no other steps to ensure that Board members were performing cybersecurity oversight on a regular basis, and no such regular oversight occurred.

In short, the pleading stage record and well-pled allegations based thereon show that SolarWinds had no processes or procedures to ensure consistent, regular

reporting concerning cybersecurity to the Board, or to otherwise enable the Board to fulfill its oversight duties.

Despite these facts, Defendants insist counterfactually that SolarWinds had "an effective board-level cybersecurity monitoring and reporting system." (Answering Brief at 2). This assertion is so divorced from Plaintiffs' well-pled allegations that it strains credulity; there simply was *no "system" of board-level oversight at all*. This is not a case based on allegations that the Company could have had a better or more effective board-level oversight system for cybersecurity. Rather, this is case in which Defendants never created—and never even tried to create—*any* system for the Board to conduct oversight regarding mission critical cybersecurity.

Corporate directors have a duty to create an "information and reporting system" that is "in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility." *Stone ex rel. AmSouth Bancorporation v. Ritter*, 911 A.2d 362, 368 (Del. 2006). The mere creation of Board committees with nominal responsibilities pertaining to a mission-critical risk to corporate interests does not constitute an oversight system that satisfies *Caremark* or *Marchand.* And this is particularly true if those committees fail to *actually* engage

in meaningful oversight. In *Marchand,* this Court identified several prerequisites for such a "system." Defendants satisfied none of them.

First, an oversight "system" must be mandatory. In *Marchand*, the Court held that plaintiffs had pleaded that the defendant board "had made no effort at all to implement a board-level system of mandatory reporting of any kind," including because the board "did not have a protocol requiring or have any expectation that management would deliver … reports or summaries of these reports to the board on a consistent and mandatory basis," and "no regular process or protocols that required management to keep the board apprised of food safety compliance practices, risks, or reports existed." *Marchand,* 212 A.3d at 813, 822. The same is true here. Defendants' Section 220 production revealed [redacted]

Second, an oversight "system" requires Board-level oversight on a regular basis. In *Marchand*, the Court held that the "complaint support[ed] an inference that no system of board-level compliance monitoring and reporting existed," including because there existed "no schedule for the board to consider on a regular basis, such as quarterly or biannually, any key food safety risks," and "the board meetings

[were] devoid of any suggestion that there was any regular discussion of food safety issues." *Marchand*, 212 A.3d at 822.[4] Likewise here, Defendants' Section 220 production revealed [redacted] In fact, the Section 220 production shows that [redacted]

Absent any system of Board-level cybersecurity monitoring and reporting, Defendants are left to argue, in effect, that a single committee meeting in which [redacted]

[4] *Cf. Firemen's Ret. Sys. Of St. Louis on behalf of Marriott Int'l, Inc. v. Sorenson*, 2021 WL 4593777, at *13 (Del. Ch. Oct. 5, 2021) (holding that "the Complaint itself shows that the Board has systems in place to assess cybersecurity risks" because the Complaint, for example, describes how the Board and Audit Committee were 'routinely apprised' on cybersecurity risks and mitigation [and] provided with annual reports on the Company's Enterprise Risk Assessment that specifically evaluated cyber risks."); *City of Detroit Police & Fire Ret. Sys. v. Hamrock*, 2022 WL 2387653, at *15 (Del. Ch. June 30, 2022) (dismissing prong one claim where "the Committee tried to fulfill its charge—meeting five times a year, receiving extensive reports from senior executives, and regularly reporting on safety risks to the full Board.").

[redacted] somehow permanently inoculates them from oversight liability. In fact, the opposite is true. The recognition of a risk as mission critical *triggers*—rather than extinguishes—the obligation of board-level oversight. The SolarWinds Board's utter failure to conduct any monitoring of cybersecurity in the two years after that single NGC meeting dramatically illustrates why Delaware law requires an oversight "system" for mission critical risks consisting of mandatory reporting on a regular basis.

Defendants also mischaracterize the February 2019 Cybersecurity Briefing in an attempt to argue that, even though the briefing accurately characterized [redacted] it somehow rendered oversight unnecessary. For example, Defendants urge the Court to make the defense-friendly inference that this single presentation "covered all of the necessary topics for the members of the [NGC] to feel comfortable with the Company's ongoing efforts to manage cybersecurity risk and confident that the Committee members were overseeing such risk in good faith." (Answering Brief at 21). Nothing in the Section 220 Production or the Complaint supports this sweeping assertion.

Defendants further assert that "[w]hat matters" is that, in the February 2019 briefing, [redacted]

[redacted] (Answering Brief at 22). Defendants completely ignore that the same presentation [redacted] (A50, A52.) This is because, according to the briefing, [redacted] *Id.* Such warnings flatly contradict Defendants' insistence that a major cybersecurity incident like SUNBURST was completely "unpredictable." (Answering Brief at 22). Yet in the face of those warnings, the NGC and the Board as a whole completely ignored the topic of cybersecurity until after the SUNBURST attack. A board cannot wait for "signs of trouble" to grow into a "severe problem" before establishing a system for oversight of mission critical risks. *Marchand*, 212 A.3d at 811, 813.

With respect to the NGC's failure to [redacted] Defendants again seek a favorable inference. Defendants do not dispute that this cybersecurity discussion by the NGC never occurred; instead, they argue: "A more reasonable inference is that

there was nothing material for management to report to the NCG Committee in the months following the February 2019 Cybersecurity Briefing." (Answering Brief at 24). This requested defense-friendly inference, unsupported by the Section 220 Production or the well-pled allegations, is contrary to Delaware law and should be rejected. *See Hughes v. Xiaoming Hu*, 2020 WL 1987029, at *2 (Del. Ch. Apr. 27, 2020) ("the *plaintiff* receives the benefit of all reasonable inferences, including inferences drawn from the documents") (emphasis added).[5]

Moreover, by claiming that reporting on cybersecurity issues was unnecessary because "there was nothing material for management to report," Defendants

[5] Defendants also once again reference the Audit Committee's *ad hoc* meeting after the COVID-19 pandemic's onset that made passing reference to cybersecurity. (Answering Brief at 23). As discussed in Plaintiffs' Opening Brief, the Court should not consider this meeting. (Opening Brief at 27-28 n.5). This meeting is not cited in the Complaint because the Company produced the subject document days before Defendants filed their motion to dismiss, well after SolarWinds had certified a complete production and Plaintiffs had filed the Complaint. Although Defendants argue that no harm or prejudice resulted from their improper delay in producing this document, the prejudice is self-evident given that Defendants relied on this document in their motion to dismiss. Even if the Court were to consider this document—and it should not—[redacted] clearly does not demonstrate any sort of systematic cybersecurity oversight by the Board. Defendants are not entitled to a pleading-stage inference that this discussion extended beyond [redacted] Indeed, the fact that Defendants certified completion of production without producing any documents regarding this *ad hoc* meeting shows that Defendants themselves understood that the meeting is irrelevant.

acknowledge that whether to report to the Board or any of its committees regarding cybersecurity was left to management's discretion, and was therefore neither mandatory nor regular, as *Marchand* requires. Indeed, Defendants' argument demonstrates the same disregard for risk monitoring that was criticized in *Boeing*:

> The nature and content of management's *ad hoc* reports to the Board indicate that the Board had no regular process or protocols requiring management to apprise the Board of airplane safety. Nothing in the Amended Complaint supports the inference that the Board requested those reports or expected those reports to contain safety information.

In re Boeing Co. Deriv. Litig., 2021 WL 4059934, *31 (Del. Ch. Sept. 7, 2021). In short, a Board cannot fulfill its oversight duties by sitting back and waiting for management to issue reports as management deems necessary. A system of reporting that relies on such *ad hoc* reports from management amounts to no system at all.

Though Defendants maintain that a one-time discussion of a mission critical risk suffices under *Marchand*, Defendants badly mischaracterize the only case on which they rely, *Hamrock,* 2022 WL 2387653. In *Hamrock*, the plaintiff argued that the relevant board committee's oversight of pipeline safety was limited to a "one-time discussion," but the Court held that the Section 220 production was "replete" with information suggesting the board and the relevant committee monitored and reported on those specific safety issues. *Id.* at *16. Criticizing the plaintiff's cherry-

picking, the Court cited *14* additional instances when the committee reviewed or discussed pipeline safety risks. *Id.* at *16-17. No such facts exist here.

In sum, Defendants come nowhere close to showing that the Board, whether as a whole or via committees, had a "regular process or protocols that required management to keep the board apprised" of mission critical cybersecurity risks. *Marchand*, 212 A. 3d at 822.

B. *Caremark* Liability Does Not Require a Violation of Positive Law, but Plaintiffs' Allegations Are Sufficient to Establish Liability Even if it Did

Defendants also contend that liability under *Caremark* is precluded because Plaintiffs have not alleged that SolarWinds violated positive law. (Answering Brief at 15-19.) This argument fails for at least three reasons. *First, Caremark* liability is not—and should not be—contingent on a violation of positive law, and the Court should reject Defendants' attempt to manufacture a new and unduly narrow version of *Caremark*'s vital regime. *Second*, Defendants' strawman argument that *Caremark* does not encompass the generic monitoring of "business risk" misses the point entirely, as cybersecurity was far from a routine business risk for SolarWinds. Rather, as the Board was expressly warned, cybersecurity was inextricable from—and thus "mission critical" to—the monoline Company's core function. *Third*, Defendants' misconduct *did* lead to SolarWinds violating positive law.

First, Defendants ask this Court to make new law. No Delaware case has ever held that *Caremark* liability can only attach where there has been a violation of positive law. It is thus unsurprising that Defendants cannot cite any precedent purportedly supporting their novel proposition. (*See* Answering Brief at 15-19.) Instead, Defendants merely observe that *Caremark* and *Marchand* happened to involve conduct that violated positive law. (Answering Brief at 15). This is again unsurprising: it stands to reason that a corporation whose board of directors has abdicated its oversight responsibility will often also end up violating positive law. Indeed, while Delaware courts have observed that successful *Caremark* claims often accompany violations of positive law, they have *never* predicated the former on the latter. *See, e.g.*, *In re Facebook, Inc. Section 220 Litig.*, 2019 WL 2320842, at *14 (Del. Ch. May 30, 2019), *as revised* (May 31, 2019), *judgment entered sub nom. In re Facebook, Inc.* (Del. Ch. 2019) ("Delaware courts are *more inclined* to find *Caremark* oversight liability at the board level when the company operates in the midst of obligations imposed upon it by positive law yet fails to implement compliance systems") (emphasis added); *Sorenson*, 2021 WL 4593777, at *12 ("Oversight violations are *typically* found where companies—particularly those operating within a highly-regulated industry—violate the law or run afoul of regulatory mandates.") (emphasis added).

By disclaiming liability on the basis that SolarWinds purportedly did not violate positive law, Defendants ask this Court to sharply limit *Caremark*'s scope. The Court should decline that invitation. As a starting point, "[i]f *Caremark* means anything, it is that a corporate board must make a good faith effort to exercise its duty of care." *Marchand*, 212 A.3d at 824. Defendants' proposed reinterpretation of *Caremark* would set a dangerously low bar for Delaware directors' discharge of this duty of care: just avoid affirmatively breaking the law. This cannot be the law. *Marchand* itself made clear that legal compliance is only one component of directors' oversight responsibility, alongside "operational viability" and "financial performance." *Marchand*, 212 A.3d at 809. There is no reason in law or logic for *Caremark* to be limited to the self-evident proposition that directors should ensure their company does not affirmatively violate the law.[6]

Second, Defendants also contend that monitoring a mere "business risk" falls outside *Caremark*'s purview. (Answering Brief at 15-16). But this litigation is not

[6] Beyond these troubling legal and policy implications, Defendants' preferred reimagining of *Caremark* would also be difficult to administer as a practical matter. Must stockholders await final resolution of civil and/or criminal charges before bringing viable *Caremark* claims, even if this process stretches beyond Delaware's statute of limitations? Would a company's entry into a settlement with the government to resolve charges without admitting any wrongdoing represent a violation of positive law sufficient to allow a *Caremark* claim?

about any ordinary "business risk." Rather, as the Complaint and Opening Brief explain at length, this litigation is about the [redacted] cybersecurity risk that SolarWinds faced in its capacity as a network management company asking some of the world's largest companies and agencies to entrust it with managing their entire IT infrastructure. Cybersecurity risk undoubtedly was more significant to SolarWinds than, for example, the risk of violating a county ordinance about how frequently it cuts the grass in front of its corporate headquarters. It is the mission critical nature of the risk that counts, not the technical question of whether some positive law was violated.

The undisputed fact that cybersecurity was a mission critical risk to SolarWinds sets this case apart from the precedents upon which Defendants rely. (Answering Brief at 15-16). This includes *Sorenson*, where cybersecurity could reasonably be viewed as an ordinary "business risk" for a hotel management company. *Sorenson*, 2021 WL 4593777, at *13 (Del. Ch. Oct. 5, 2021). This also includes *Citigroup*, where exposure to the subprime mortgage lending market could reasonably be viewed as an ordinary "business risk" for a large financial institution. *In re Citigroup Inc. S'holder Derivative Litig.*, 964 A.2d 106, 123 (Del. Ch. 2009). Further, the *Reiter* court did not rely on a distinction between legal and business risk as a basis for its ruling. *Reiter on Behalf of Cap. One Fin. Corp. v. Fairbank*, 2016

WL 6081823, at *14 (Del. Ch. Oct. 18, 2016). Defendants' attempt to recast cybersecurity as a run-of-the-mill business risk for SolarWinds—without actually disputing that cybersecurity was mission critical—is plainly at odds with Plaintiffs' well-pled allegations and the underlying pleading stage evidence.

Third, even though *Caremark* does not require a violation of positive law, Defendants' fiduciary breaches *did* lead to one. Defendants argue that the SEC's interpretive 2018 Cybersecurity Release lacks the full force of law and did not impose any substantive requirements on SolarWinds. (Answering Brief at 17-18). Although the 2018 Cybersecurity Release might not unilaterally impose *new* legal obligations on companies like SolarWinds, the Company unquestionably remained subject to the laws and regulations that the 2018 Cybersecurity Release interpreted, and Defendants do not suggest that the SEC's interpretation of those laws and regulations was wrong in any way. In any event, the 2018 Cybersecurity Release is the SEC's own description of how it intends to apply and enforce existing laws and regulations.

Further, Defendants completely ignore the fact that the SEC is not just investigating SolarWinds, but has issued a "Wells Notice" stating that SEC staff has preliminarily determined to recommend that the SEC file an enforcement action against SolarWinds for violation of federal securities law with respect to its

cybersecurity disclosures. (Opening Brief at 45). Ultimately, any law is subject to interpretation, and there is no viable distinction, at least for present purposes, between violating the SEC's unchallenged interpretation of the law, and violating the law itself.

Finally, Defendants' claim that there is a relevant "conceptual difference" between disclosure requirements and, for example, airline safety regulations (Answering Brief at 17), is completely unsupported. Indeed, Defendants' apparent argument that some unknown set of positive laws, which they deem relatively unimportant, cannot form the basis of oversight liability undermines their argument that oversight liability requires a positive law violation in the first place. What matters for purposes of oversight liability is whether, as *Caremark* and *Marchand* require, there is a board-level system to monitor mission critical risks. Whether a company has technically violated positive law in the midst of corporate trauma is at most a secondary question, particularly in a case like this one in which there is no dispute that the risk at issue was mission critical. *See Marchand*, 212 A.3d at 823 (noting that "the fact that Blue Bell nominally complied with FDA regulations does not imply that the *board* implemented a system to monitor food safety *at the board level*") (emphases in original).

II. A MAJORITY OF SOLARWINDS' BOARD FACED A LIKELIHOOD OF LIABILITY FOR IGNORING "RED FLAGS" UNDER *CAREMARK*'S SECOND PRONG

In their Answering Brief, Defendants rely on the trial court's flawed holding that they did not ignore red flags to establish demand futility under *Caremark*'s second prong. Plaintiffs' Complaint, however, states a claim under that prong by pleading 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 *7 (Del. Ch. Jan. 19, 2017).

Here, the Complaint identifies glaring "red flags" which establish that the Board failed to adequately oversee the Company's mission critical risk related to cybersecurity issues. Specifically, the February 2019 Cybersecurity Briefing [redacted] (A48-49, ¶¶39-40). The February 2019 Cybersecurity Briefing [redacted] (A50, ¶39). The Cybersecurity Briefing then [redacted]

[redacted] (A50, ¶39) (emphasis in original).

The Cybersecurity Briefing [redacted]

[redacted]" (A50-51 ¶¶40, 41) (emphasis in original). Given SolarWinds' limitless access to its customers' networks and the manifest risks, these warnings should have triggered Board action. As reflected in the pleading stage record and alleged in the Complaint, however, the NGC took no further actions in response to the express, specific and serious warnings identified in the Briefing—a clear violation of the directors' oversight duties.

Echoing the trial court, Defendants ignore these specific allegations to reach the improper defense-friendly inference that the February 2019 Cybersecurity Briefing was "an instance of oversight" of the NGC. (Answering Brief at 35). Not so. A single meeting [redacted] does not constitute adequate oversight.[7] *See, e.g.*, *Boeing*, 2021 WL 4059934, at *28 ("The Board and

[7] Defendants incorrectly seek an inference, which the trial court improperly granted,

management's passive invocations of quality and safety, and use of safety taglines, fall short of the rigorous oversight *Marchand* contemplates.").[8] Indeed, (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 Loc. 443 Health Services & Ins. Plan v. Chou*, 2020 WL 5028065, at *12 (Del. Ch. Aug. 24, 2020).

---

that the February 2019 Cybersecurity Briefing's disclosure of "the precise number of security incidents at the Company in 2017 and 2018—showing that management was tracking each incident," means that this Briefing does not constitute a "red flag." In fact, Plaintiffs more than sufficiently plead that this warning is a critical "red flag" because, *e.g.*, this tracking showed "94 incidents in 2018," which was a "124% increase over 2017," and yet the Board took no further action in response. (A51-53, ¶¶41-42).

[8] Defendants also note that *Boeing* involved a prior plane crash with the same safety issue, and that no prior large scale cyberattack had occurred at SolarWinds before SUNBURST. But there is no basis to contend that only the catastrophic materialization of the risk in question—as opposed to specific warnings, for example—can constitute a red flag. *See, e.g.*, *Marchand*, 212 A.3d at 811 (outbreak did not occur until after red flags were ignored).

Defendants' contention that *Sorenson* applies here is wrong. 2021 WL 4593777. *First*, as explained above, *Sorenson* involved a data breach at the Marriott hotel company, not a monoline IT network management company, like SolarWinds, whose Board knew [redacted][9] The Complaint's allegations concerning how cybersecurity is a "mission critical" risk to SolarWinds' business is a fundamental factual difference that makes *Sorenson*'s holding inapplicable here. 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 [redacted] by the Company's own admission. (Op. at *1).

Next, *Sorenson* is inapposite because, unlike here, the Marriott board actually took (and monitored) 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

[9] Defendants' contention that SolarWinds was not "monoline" because "it produces a wide variety of software products" (Answering Brief at 26) is (1) waived, because it was not raised in Defendants' briefing below; (2) irrelevant, because Defendants cannot and do not dispute that cybersecurity was a mission critical risk to the Company's only line of business—software; and (3) just as unconvincing as the notion that Blue Bell was not a monoline producer of ice cream because, as the Court acknowledged, it "does make a few other related products, such as frozen yogurt." *Marchand*, 212 A.3d at 822 n.107.

premier IT network manager. *See Sorenson*, 2021 WL 4593777, at *16-17. Given the Marriott board's knowledge and oversight of management's earnest efforts, the court deemed the plaintiffs' allegations insufficient to support an inference that the board members breached their oversight duty under *Caremark*. *Id.*

In contrast, the pleading stage record and Plaintiffs' allegations based thereon establish that the Board did nothing to respond to or follow up on the February 2019 presentation's warnings. (A70-71, ¶¶73–74). Defendants' Section 220 Production shows [redacted] (A72-73, ¶76). The total absence of any substantive Board response to [redacted] constitutes a textbook example of directors ignoring red flags and their duty of oversight.

Moreover, the red flags in the Cybersecurity Briefing do not stand alone. 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. (A53-61, ¶¶44–56). Defendants ignore these allegations, which the Court incorrectly characterized as a "plethora of background facts about the increasing need for technology companies, in general, to address cybersecurity."

(Op. at 4). Critically, SolarWinds is not a generic company facing run-of-the-mill cybersecurity risks. As the Court and the Company recognize, 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. *Chou*, 2020 WL 5028065, at *20 (although certain warnings "alone could serve as [] red flags 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.").

Defendants also contend that the Court properly rejected the Complaint's other allegations of red flags due to its finding that the Board was unaware of them. (Answering Brief at 31-36). For example, Defendants argue that the Complaint's allegations concerning the Company's password— "solarwinds123"—cannot serve as a red flag because the Board was oblivious to it.[10] Likewise, Defendants argue that the Complaint's allegations about the April 2017 presentation by Mr. Thornton-

[10] Defendants also contend that the "solarwinds123" password did not cause corporate harm or have a direct connection to SUNBURST, but those contentions are completely unproven at this stage, and the use of such an obviously insecure password is a critical red flag in any event because it should have raised fundamental questions about the Company's cybersecurity practices.

Trump, SolarWinds' "Global Cybersecurity Strategist," which 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 his related resignation in protest cannot serve as red flags for the same reasons (*i.e.*, the Board was unaware of them). (A86, ¶97).

Any reasonable system of cybersecurity oversight would have brought these glaring red flags to the Board's attention on an emergency basis. The fact that the Board never even learned of them confirms that Defendants did not actually "*monitor*" any reasonable oversight or reporting system regarding the Company's known mission critical cybersecurity risks. *In Re Clovis Oncology, Inc. Derivative Litig.*, 2019 WL 4850188, at *1 (Del. Ch. Oct. 1, 2019) (emphasis in original).

Lastly, Defendants contend that "Plaintiffs do not allege any facts about this unprecedented and highly sophisticated attack by a foreign state actor from which one could infer that any number of oversight meetings would have sufficed to prevent it." (Answering Brief at 4). In fact, Plaintiffs' complaint details basic cybersecurity steps—such as the use of secure passwords, firewalls, and network segmentation to prevent hackers from moving between different parts of the system—that SolarWinds failed to implement. (A75-81, ¶¶80-90.) This is akin to a bank that is expressly warned about the rising risks of bank robbery and the bank's

particular status as a prime target, yet leaves the door to its vault open, and then asserts that nothing could have prevented the robbery. Indeed, had the hypothetical bank bothered to lock the vault—or had SolarWinds adopted basic cybersecurity measures—the bad actors could well have been unsuccessful or decided to target a different company, or at least the damage could have been substantially limited. At the pleading stage, Plaintiffs are not required to prove to a certainty that adequate oversight would have led to remedial action and prevented the corporate harm in question, but only to plead facts that support a "fair inference" to that effect. *Marchand*, 212 A.3d at 824. Defendants do not seriously contest that Plaintiffs meet this pleading standard.

CONCLUSION

The judgment below should be reversed.

Dated: February 3, 2023

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