IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

CONSTRUCTION INDUSTRY LABORERS PENSION FUND, CENTRAL LABORERS' PENSION FUND, LAWRENCE MILES, and BRIAN SEAVITT, derivatively on behalf of SOLARWINDS CORPORATION, Plaintiffs, v. MIKE BINGLE, WILLIAM BOCK, SETH BORO, PAUL J. CORMIER, KENNETH Y. HAO, MICHAEL HOFFMANN, DENNIS HOWARD, CATHERINE R. KINNEY, JAMES LINES, EASWARAN SUNDARAM, KEVIN B. THOMPSON, JASON WHITE, MICHAEL WIDMANN, Defendants, and SOLARWINDS CORPORATION, Nominal Defendant	)	C.A. No. 2021-0940-SG

MEMORANDUM OPINION

Date Submitted: May 13, 2022
Date Decided: September 6, 2022

Michael J. Barry and Vivek Upadhya, of GRANT & EISENHOFER, P.A., Wilmington, Delaware; Thomas Curry and Tayler D. Bolton, of SAXENA WHITE P.A., Wilmington, Delaware; OF COUNSEL: Chad Johnson, Noam Mandel, Desiree Cummings, Jonathan Zweig, and Sarah Delaney, of ROBBINS GELLER RUDMAN & DOWD LLP, New York, New York; Jeremy S. Friedman and David Tejtel, of FRIEDMAN OSTER & TEJTEL PLLC, Bedford Hills, New York; D. Seamus Kaskela, of KASKELA LAW LLC, Newton Square, Pennsylvania; Julia Goldsmith Reiser, of COHEN MILSTEIN SELLERS & TOLL PLLC, Washington, DC; Richard A. Speirs and Amy Miller, of COHEN MILSTEIN SELLERS & TOLL PLLC, New York, New York, *Attorneys for Plaintiffs.*

Raymond J. DiCamillo, Kevin M. Gallagher, and Alexander M. Krischik, of RICHARDS, LAYTON & FINGER, P.A., Wilmington, Delaware; OF COUNSEL: Sandra C. Goldstein, Stefan Atkinson, and Byron Pacheco, of KIRKLAND & ELLIS LLP, New York, New York, *Attorneys for Defendants William Bock, Seth Boto, Paul Cormier, Michael Hoffman, Dennis Howard, Catherine Kinney, James Lines, and Easwaran Sundaram.*

William M. Lafferty, Ryan D. Stottmann, and Alexandra M. Cumings, of MORRIS NICHOLS ARSHT & TUNNELL LLP, Wilmington, Delaware; OF COUNSEL: Sameer Advani, Wesley R. Powell, and Patricia O. Haynes, of WILLKIE FARR & GALLAGHER LLP, New York, New York, *Attorneys for Defendants Mike Bingle, Kenneth Hao, Jason White, and Michael Widmann*.

A. Thompson Bayliss and Stephen C. Childs, of ABRAMS & BAYLISS LLP, Wilmington, Delaware; OF COUNSEL: Peter L. Welsh, C. Thomas Brown, and Patrick T. Roath, of ROPES & GRAY LLP, Boston, Massachusetts; Edward R. McNicholas, of ROPES & GRAY LLP, Washington, D.C., *Attorneys for Defendant Kevin Thompson.*

John L. Reed, Ronald N. Brown, Peter H. Kyle, and Kelly L. Freund, of DLA PIPER LLP, Wilmington, Delaware; OF COUNSEL: Paul R. Bessette, Michael J. Biles, and Daniel M. Wodnicki of KING & SPALDING LLP, Austin, Texas; Benjamin Lee and Benjamin B. Watson, of KING & SPALDING LLP, Atlanta, Georgia, *Attorneys for Nominal Defendant SolarWinds Corporation.*

GLASSCOCK, Vice Chancellor

Nominal Defendant SolarWinds Corporation (the "Company") was in the business of providing management software to its customers. Sometime in 2020, SolarWinds became the victim of a major crime. Per the complaint, Russian hackers were able to penetrate SolarWinds systems and insert malware, to the detriment of SolarWinds customers, ultimately damaging the value of the company itself. The Plaintiffs here, SolarWinds stockholders at the time of the trauma, allege that the Defendant corporate directors, a majority of whom were on the board at all times pertinent, failed to adequately oversee the risk to cybersecurity of criminal attack. They seek to hold the Defendants liable in damages.

Derivative claims against corporate directors for failure to oversee operations—so-called *Caremark* claims, once relative rarities—have in recent years bloomed like dandelions after a warm spring rain, largely following the Delaware Supreme Court's opinion in *Marchand v. Barnhill*.[1] The cases, superficially at least, seem easy to conjure up: find a corporate trauma; allege the truism that the board of directors failed to avert that trauma; and *hey, presto!* an oversight liability claim is born. They remain, however, one of the most difficult claims to cause to clear a motion to dismiss. That is also easy to understand. Directors are not liable under our corporate law for the most likely cause of operational loss, simple negligence. Nor, given the ubiquity of exculpation clauses, are the directors even liable for gross

[1] 212 A.3d 805, 822 (Del. 2019).

negligence in violation of their duty of care. And, of course, most corporate trauma, to the extent it represents a breach of duty at the board level, implicates the exculpated duty of care. To plead potential liability sufficient to cause directors to be unable to consider a demand and thus justify a derivative claim under Rule 23.1, therefore, the lack of oversight pled must be so extreme that it represents a breach of the duty of loyalty. This in turn requires a pleading of scienter, demonstrating bad faith—in then-Chief Justice Strine's piquant formulation, a failure to fulfill the duty of care *in good faith*.[2] In other words, an oversight claim is a flavor of breach of the duty of loyalty, which itself requires an action (or omission) that a director knows is contrary to the corporate weal.[3] Historically, only utter failures by directors to impose a system for reporting risk, or failure to act in the face of "red flags" disclosed to them so vibrant that lack of action implicates bad faith, *in connection with the corporation's violation of positive law*, have led to viable claims under Caremark.

This matter is before me on the Defendants' Motions to Dismiss. Here, there is no credible allegation that the Company violated positive law. Instead, the Directors are accused of failing to monitor corporate effort in way that prevented cybercrime. Of course, absent statutory or regulatory obligations, how much effort

[2] *Id.* at 824.
[3] Or self-dealing, which is not typically implicated in allegations of oversight liability.

to expend to prevent criminal activities by third parties against the corporate interest requires an evaluation of business risk, the quintessential board function. Judicial post-hoc intrusion into the appropriate consideration of business risk, pre-trauma, is problematic, particularly where the demand is for damages and the directors are exculpated for gross negligence. Accordingly, this should be an easy action to resolve in favor of the Defendants. Many corporate decisions have implications for customers, no doubt. Nonetheless, I note that before me is a peculiar kind of business risk. Online software companies are dependent on their customers sharing access to the customer's information. The resulting relationship is essential to the business of these companies. In light of the ubiquity of attempts by evildoers to breach the security of tech companies and their customers, disclosure obligations have been imposed by the SEC regarding board efforts to oversee cybersecurity, and at least one major stock exchange has promulgated cybersecurity guidelines. To use the shibboleth arising from *Marchand*, cybersecurity, for online service providers, is mission critical.

To what extent are the decisions or omissions of Directors reviewable under Caremark in such a scenario? I need not address that issue here, because, as pled, the director defendants here (1) are not credibly alleged to have allowed the company itself to violate law, (2) did ensure that the company had at least a minimal reporting system about corporate risk, including cybersecurity, and (3) are not alleged to have

ignored sufficient "red flags" of cyber threats to imply a conscious disregard of a known duty, indicative of scienter.[4] In other words, the directors failed to prevent a large corporate trauma, but the Plaintiffs have failed to plead specific facts from which I may infer bad faith liability on the part of a majority of the directors regarding that trauma. The defendants have moved to dismiss, and I conclude Rule 23.1 is unsatisfied. The motions to dismiss must be granted accordingly.

My reasoning follows.

I. BACKGROUND

Before me are three motions to dismiss the sole count in this action, a derivative claim brought against all defendants for a breach of the "Fiduciary Duties of Loyalty and Care through a Bad Faith Failure to Oversee SolarWinds's Cybersecurity."[5] SolarWinds Corporation, the nominal defendant in this action ("SolarWinds" or the "Company"), suffered a major cyberattack in December 2020.[6] That cyberattack is referred to herein as the "Sunburst Attack." The purported breaches of fiduciary duty relate to the Sunburst Attack.

[4] I discuss supposed "red flags," *infra.*
[5] *See* Verified Stockholder Derivative Compl. 70, Dkt. No. 1 [hereinafter "Compl."].
[6] *See id.* ¶ 4. To be more precise, the Complaint pleads that SolarWinds learned of the cyberattack in December 2020. *Id.* Based on the pleadings, it is not clear that the Sunburst Attack can be tied to a singular date of occurrence.

A. Factual Background[7]

1. The Parties

Per the complaint (the "Complaint"), the Plaintiffs are current SolarWinds stockholders who "purchased SolarWinds shares during the relevant period" and have held shares since.[8]

Nominal Defendant SolarWinds, a Delaware corporation, provides information technology infrastructure management software.[9] Its software is used by a proliferation of clients ranging from the Fortune 500 to United States government agencies, and the Company's revenue is entirely dependent on the sale of its software.[10] The Company's main product, Orion Platform ("Orion"), is the software that was targeted in the Sunburst Attack.[11] Use of Orion requires the software to have access to clients' information technology systems.[12]

[7] Unless otherwise specified, the facts in this section are drawn from the Complaint. *See* Compl. This section is reflective of the Complaint, and I consider the facts to be true as pled in the Complaint, in accordance with the applicable standard on a motion to dismiss. This section therefore does not constitute formal findings of fact.
[8] *Id.* ¶ 18. It is unclear that this statement is sufficient to confer standing to bring a derivative claim on behalf of the Company, given its lack of anchor in time. No party has disputed the Plaintiffs' standing to date, so I do not address the question further here.
[9] *Id.* ¶ 2.
[10] *Id.* ¶¶ 2, 33.
[11] *Id.* ¶¶ 4, 34.
[12] *Id.* ¶¶ 3, 34–35.

SolarWinds was a private company prior to October 2018,[13] when it went public via an initial public offering ("IPO").[14] The Plaintiffs refer throughout the Complaint to the time period between the IPO and the Sunburst Attack in a manner that suggests they view this time period as the relevant one for purposes of their claim here.[15] I assume this is the case due to the timing of the various Plaintiffs' stock purchases in SolarWinds, though that information has not been provided in the Complaint.[16]

SolarWinds's charter contains a provision reflective of Delaware General Corporation Law Section 102(b)(7), exculpating its directors from liability for duty of care violations commensurate with the statute.[17]

The named Defendants in this action are Mike Bingle, William Bock, Seth Boro, Paul Cormier, Kenneth Hao, Michael Hoffmann, Dennis Howard, Catherine Kinney, James Lines, Easwaran Sundaram, Kevin Thompson, Jason White, and Michael Widmann, each of whom currently serves or previously served as a director

---

[13] More precisely, SolarWinds was founded in 1999, went public in 2009, and was taken private in 2016, prior to its second "initial" public offering. *See id.* ¶ 36. The take-private transaction in 2016 was undertaken by two private equity firms named Silver Lake and Thoma Bravo. *Id.* A number of directors on the SolarWinds board of directors have connections to Thoma Bravo and Silver Lake. *See id.* ¶ 37.

[14] *Id.* ¶ 36.

[15] *See, e.g., id.* ¶¶ 8, 71, 78, 80.

[16] I am assuming that events to which liability may attach here are limited to post-IPO. Nothing in the Complaint indicates that the Plaintiffs were stockholders prior to the take-private transaction in 2016, and in any event, laches issues would likely inhere in any attempt to raise events from that time period now.

[17] Transmittal Decl. of John L. Reed, Esq., Supp. Nominal Def. SolarWinds Corporation's Mot. to Dismiss Pls.' Derivative Compl., Ex. 11, Art. VII [hereinafter "Reed Decl."].

on SolarWinds's board of directors (the "Board").[18] The current Board is composed of eleven directors.[19] The Complaint alleges that a majority of the current (demand) directors were in service during/prior to the Sunburst Attack.[20]

Kevin Thompson stands in a somewhat different factual posture than the remainder of the Defendants, so additional facts are helpful. Thompson was, prior to his resignation in December 2020, both a director and the Chief Executive Officer ("CEO") of SolarWinds.[21] Following the Sunburst Attack, the Company rehired Thompson in a role as a consultant under a Transition Agreement.[22] Thompson's compensation for five months of transition services exceeds $300,000 under the Transition Agreement.[23] The Transition Agreement also provided him with a release related to any of his actions or omissions during his service as the CEO and a director of SolarWinds.[24]

2. SolarWinds's Board and Cybersecurity at the Relevant Time[25]

The Company created at least two Board subcommittees following its IPO: an Audit Committee and a Nominating and Corporate Governance Committee (the

[18] *See* Compl. ¶¶ 20–32.
[19] *See id.* ¶ 113.
[20] *Id.*
[21] *Id.* ¶ 30.
[22] *Id.* ¶¶ 30, 111.
[23] *Id.* ¶ 111.
[24] *Id.* ¶ 30.
[25] The Plaintiffs, having seemingly narrowed the pertinent timeframe to post-October 2018, also reference multiple events that took place at least in part in 2017. Most prominently, they point to

"NCG Committee"). Throughout this Memorandum Opinion, the two subcommittees are occasionally referred to as the "Committees."

At the time of the Company's IPO, the NCG Committee was charged with general oversight responsibility as pertained to corporate governance risks, though responsibility for cybersecurity was not specifically mandated.[26] In April 2019, the NCG Committee's charter was amended to require members to discuss SolarWinds's major risk exposures, explicitly including cyber and data security, with management.[27]

The Complaint indicates that "[f]ollowing the Company's IPO," the Board delegated cybersecurity oversight to the Audit Committee.[28] It is otherwise unclear when this delegation occurred relative to other pertinent facts. The Audit Committee charter states that members must discuss major financial risk exposures, such as cyber and data security, with members of management.[29]

---

an elementary-level password, 'solarwinds123,' that was used at the Company as early as 2017. *See, e.g.*, *id.* ¶ 82. This password was discovered by an outside party, who informed SolarWinds's information technology team of the issue in November 2019. *See id.* The Plaintiffs also reference a presentation describing perceived cybersecurity failures that a former employee, previously the Global Cybersecurity Strategist, had given to management in April 2017, to bolster their position that SolarWinds's approach to cybersecurity was lackadaisical. *See id.* ¶ 97. That same officer later left the Company in 2017 via resignation email to the Chief Marketing Officer. *Id.*

[26] *Id.* ¶ 10. The Complaint does not specify what document supports this assertion, though context suggests it may be the NCG Committee charter.

[27] *Id.* ¶ 75.

[28] *Id.* ¶ 72.

[29] *Id.*

In February 2019—before its charter was amended to specifically reference cybersecurity—the NCG Committee heard a briefing on the subject of cybersecurity, presented by the Company's executives (the "Cybersecurity Briefing").[30] That presentation emphasized the seriousness of cybersecurity risks for SolarWinds given its wide customer base and access to client software, but confirmed that the Company had only been a "target of opportunity" to date.[31] The presentation also specified that SolarWinds's "[i]ncident response process" was employed 94 times in 2018—indicating 94 issues had been detected and "tested" the process.[32] The minutes from the meeting indicate the NCG Committee held a discussion on the topic of cybersecurity following management's presentation.[33]

The Cybersecurity Briefing slides also contained a reference to the NCG Committee's upcoming events, including a listing for "January"—presumably January 2020—that read: "Discussion of risk management topic (e.g. cybersecurity)[.]"[34] No such meeting was ever scheduled.[35]

Besides the Cybersecurity Briefing in February 2019, the Committees did not receive any further presentations from management regarding SolarWinds's

[30] *Id.* ¶ 39. The Complaint pleads that the Cybersecurity Briefing was heard by defendant directors Kinney, Bingle, Bock, and Widmann. *Id.*
[31] *See, e.g., id.* ¶¶ 39–40.
[32] *Id.* ¶¶ 41–42.
[33] Reed Decl., Ex. 12, at SW_SEAVITT 220_000000806.
[34] Compl. ¶ 74.
[35] *Id.*

cybersecurity in the time period between the 2018 IPO and the Sunburst Attack in 2020.[36]

The full Board did not conduct any meetings or hold any discussions concerning cybersecurity at the Company from October 2018 until the Sunburst Attack occurred in December 2020.[37] Neither the NCG Committee nor the Audit Committee made any presentation to the full Board regarding cybersecurity during this time period, either.[38]

The Complaint contains a plethora of background facts about the increasing need for technology companies, in general, to address cybersecurity, including agency and private sector reports.[39] The most salient facts are those pertaining to certain guidance issued by the Securities and Exchange Commission (the "SEC") in 2018.[40] The guidance states in part: "This interpretive release outlines the Commission's views with respect to cybersecurity disclosure requirements under the federal securities laws as they apply to public operating companies."[41] The guidance reflects the SEC's belief that "the development of effective disclosure controls and

[36] *Id.* ¶¶ 8–10; *id.* ¶ 75.
[37] *Id.* ¶ 8.
[38] *Id.* ¶ 9; *id.* ¶ 75.
[39] *Id.* ¶¶ 44–56.
[40] *Id.* ¶ 59.
[41] *Id.*

procedures is best achieved" when directors are informed about cybersecurity risks and incidents pertaining to their company.[42]

The New York Stock Exchange ("NYSE"), where SolarWinds trades, also provides cybersecurity guidelines for directors and officers.[43]

3. The 2020 Sunburst Attack

The Sunburst Attack was discovered in December 2020.[44] The Complaint describes the attack as follows: "Russian hackers used SolarWinds' software as a 'Trojan Horse' to attack the Company's clients by hiding malicious code in SolarWinds' Orion software and exploiting its trusted access to gain entry to the Company's clients' systems."[45] The Plaintiffs allege that as early as January 2019, the hackers were able to infect the Orion "software build environment,"[46] theoretically through password deficiencies exploited by the hackers.[47] Once the hackers had accessed that software build environment, they inserted malicious code into Orion's software updates.[48] When SolarWinds's clients engaged in routine software updates, the malicious code was downloaded along with the Orion software.[49] The Complaint describes the hackers as accessing and stealing

[42] *Id.*
[43] *Id.* ¶ 64.
[44] *Id.* ¶ 4.
[45] *Id.*
[46] *Id.* ¶ 100.
[47] *Id.* ¶¶ 100–02.
[48] *Id.* ¶ 103.
[49] *Id.*

"extensive proprietary information, confidential emails, and intellectual property" from both private sector and government clients.[50]

Per SolarWinds, the Sunburst Attack affected up to 18,000 of its clients, both in the private and governmental sectors.[51] Upon public disclosure of the Sunburst Attack, SolarWinds's stock suffered significant losses, with its value ultimately discounted by almost 40%.[52] The stock continued to trade at a more than 30% discount to its pre-attack value as of the filing of the Complaint.[53] License revenues and other financial metrics were likewise negatively affected at least in part due to the Sunburst Attack.[54]

Following the attack, multiple class action lawsuits were filed, and investigations were opened by "numerous domestic and foreign law enforcement agencies."[55]

[50] *Id.* ¶ 104. Among the affected government entities were the Department of Homeland Security, the Pentagon, and numerous U.S. Attorney's Offices. *Id.* ¶ 105.
[51] *Id.* ¶ 4.
[52] *Id.* ¶ 107.
[53] *Id.*
[54] *Id.* ¶ 108.
[55] *Id.* ¶ 109.

B. Procedural History

The Complaint in this action was filed on November 1, 2021,[56] and three motions to dismiss followed soon after in January 2022.[57] Oral argument followed briefing on the motions to dismiss, and I took the matter under advisement in May 2022.[58]

II. ANALYSIS[59]

Litigation assets, like other corporate assets, are under the control of the board of directors. Only when a majority of directors are disabled from bringing their business judgment to bear regarding a litigation asset may a stockholder proceed to exploit it derivatively on behalf of the corporation. Accordingly, Court of Chancery Rule 23.1 requires that stockholders seeking exploitation of a corporate litigation asset make a demand for directors to so act; where, as here, no demand was made, demand is excused only where the putative derivative plaintiff pleads with specificity facts from which a court may infer that a demand would be futile. Otherwise, the derivative action will be dismissed.[60]

---

[56] *See generally* Compl.
[57] Nominal Def., SolarWinds Corporation's Mot. to Dismiss Pls.' Derivative Compl., Dkt. No.18; Def. Kevin B. Thompson's Mot. to Dismiss Pls.' Verified Shareholder Derivative Compl., Dkt. No. 19; Director Defs.' Mot. to Dismiss Pls.' Derivative Compl., Dkt. No. 20.
[58] *See* Tr. of 5-13-22 Oral Arg. on Defs.' Mots. to Dismiss, Dkt. No. 53 [hereinafter "Oral Arg."].
[59] As a preliminary matter, though the Complaint's count indicates that the claim includes a breach of the fiduciary duty of care (among others), I do not address duty of care here because SolarWinds's charter contains an exculpatory provision insulating directors from liability for duty of care breaches. It is the directors whose business judgment must be discredited here for the matter to proceed derivatively, obviously.
[60] *See United Food & Comm. Workers Union v. Zuckerberg*, 262 A.3d 1034, 1058 (Del. 2021).

The Complaint in this action pleads that demand is futile solely on the basis that SolarWinds's Board could not impartially evaluate a demand for suit because eight of the eleven Board members face a substantial likelihood of liability in the action.[61] The Plaintiffs' primary theory alleging liability is founded in *Caremark* and its progeny.[62] The Plaintiffs must demonstrate that at least half of the members of the demand Board are substantially likely to be liable under their *Caremark* theory (or some other theory) to have satisfied demand futility.[63] The motions to dismiss seek dismissal under Rule 23.1 for failure to allege with particularity that demand is in fact futile due to a substantial likelihood of *Caremark* liability.[64]

The standard of review applicable to assess demand futility under Rule 23.1 is more demanding than the standard of review applicable to a motion to dismiss brought under Rule 12(b)(6). In short, the reason for this higher standard is that by bringing suit on behalf of a corporation without first making a demand upon the board of directors, a plaintiff supplants the board of directors' decision-making role

[61] Compl. ¶ 113; *see also Zuckerberg*, 262 A.3d at 1058.
[62] Compl. ¶ 113 ("[A majority of the Demand Board] could not impartially evaluate a demand because they face a substantial likelihood of personal liability for utterly failing to implement or oversee any reasonable system of monitoring over mission critical aspects of SolarWinds' business during the relevant time.").
[63] *See Firemen's Ret. Sys. of St. Louis ex rel. Marriott Int'l, Inc. v. Sorenson*, 2021 WL 4593777, at *7 (Del. Ch. Oct. 5, 2021) (citation omitted).
[64] *See, e.g.*, Opening Br. of Nominal Def., SolarWinds Corporation Supp. Its Mot. to Dismiss Pls.' Derivative Compl. 16, Dkt. No. 18. Though there are three motions pending, I need only treat the nominal defendant's motion under Rule 23.1 to dispose of the action. The other two motions also reference a failure to state a claim under Rule 12(b)(6) as a separate argument in favor of dismissal.

with respect to whether to bring said suit.[65] Given this subversion of default roles, Court of Chancery Rule 23.1 requires derivative complaints to allege demand futility with particularity, which "differ[s] substantially" from notice pleading.[66]

Despite the requirement that the Plaintiffs plead their case with particularity, they are still entitled to the benefit of all reasonable inferences and the Court must accept as true all particularized and well-pled allegations contained in the Complaint.[67] The reasonable inferences "must logically flow from particularized facts alleged by the plaintiff."[68]

A. Assessing the Caremark Theory of Demand Futility

The Plaintiffs have argued that a substantial likelihood of liability attaches to a majority of the demand Board based on either or both of what are colloquially referred to as prongs one and two of *Caremark*.[69] That is, the Plaintiffs allege both that a majority of the demand Board utterly failed "to implement and monitor a system of corporate controls and reporting mechanisms" regarding cybersecurity,[70] and that even if a monitoring system was in place, the directors failed to "oversee"

---

[65] *See, e.g.*, *United Food & Comm. Workers Union v. Zuckerberg*, 250 A.3d 862, 875–77 (Del. Ch. 2020), *aff'd*, 262 A.3d 1034.
[66] *Zuckerberg*, 262 A.3d at 1048 (internal quotations omitted) (quoting *Brehm v. Eisner*, 746 A.2d 244, 254 (Del. 2000)).
[67] *Id.* at 1048.
[68] *Wood v. Baum*, 953 A.2d 136, 140 (Del. 2008).
[69] *See, e.g.*, Compl. ¶ 113; Pls.' Omnibus Answering Br. Opp'n Defs.' Mots. to Dismiss 33–52, Dkt. No. 28 [hereinafter "AB"].
[70] Compl. ¶ 121.

such system of oversight in breach of their fiduciary duties because they overlooked "red flags" signaling corporate risk.[71]

Plaintiffs in *Caremark* cases must "plead with particularity 'a sufficient connection between the corporate trauma and the [actions or inactions of] the board.'"[72] "A stockholder cannot displace the board's authority simply by describing the calamity and alleging that it occurred on the directors' watch."[73] The requirement of a connection between the Board and the corporate trauma at issue is at least one plausible reason that *Caremark* cases are generally brought in the context of violations of applicable *laws*.[74] For example, in *Marchand v. Barnhill*, the corporate trauma suffered as a result of a listeria outbreak was—at least theoretically—within the company's (and the directors') control. That is, the board's failure to institute a reporting and monitoring system allowing it to oversee the company's compliance with positive-law regulation of food safety led to a pleading-stage inference of bad faith.[75] Similarly, in *Boeing*, the Boeing board of

---

[71] *Id.* ¶ 118. The "prong two" argument that directors of SolarWinds ignored red flags was made without enthusiasm in the complaint, but advanced more strongly in the answering brief. *See* AB 44–52.

[72] *In re Boeing Co. Deriv. Litig.*, 2021 WL 4059934, at *24 (Del. Ch. Sept. 7, 2021) (citing *La. Mun. Police Emps.' Ret. Sys. v. Pyott*, 46 A.3d 313, 340 (Del. Ch. 2012), *rev'd on other grounds*, 74 A.3d 612 (Del. 2013)).

[73] *Pyott*, 46 A.3d at 340.

[74] *Cf. id.*, 46 A.3d at 340–41 (citations omitted) ("To plead a sufficient connection between the corporate trauma and the board, the plaintiff's first and most direct option is to allege with particularity actual board involvement in a decision that violated positive law . . . . [T]he next alternative is to plead that the board consciously failed to act after learning about evidence of illegality—the proverbial 'red flag.'"); s*ee Sorenson*, 2021 WL 4593777, at *11–12.

[75] *Marchand*, 212 A.3d at 822.

directors, in their duties as overseers of corporate performance, failed to monitor compliance with airplane safety regulations at the board level, even after two fatal crashes.[76]

The Plaintiffs plead that despite this juridical history of applying *Caremark* primarily to cases involving violations of positive law, oversight liability may be established even in the absence of such a violation.[77] Here, the Plaintiffs ask me to find that oversight liability may attach to the Company's alleged failure to sufficiently oversee risks related to efforts to avoid cybercrime by third parties—that is, business risk. Many Delaware cases have cautioned that whether *Caremark* should be applied to business risk remains an open question.[78]

The Plaintiffs cite *Firemen's Retirement System of St. Louis on behalf of Marriott International, Inc. v. Sorenson* in support of their argument. *Sorenson* is a recent Court of Chancery case that found *Caremark* to apply, at least hypothetically, to failure to monitor cybersecurity risks, reasoning that "corporate governance must

[76] *Boeing*, 2021 WL 4059934, at *25–33.
[77] *See* Oral Arg. 59:5–62:3; *see also Sorenson*, 2021 WL 4593777, at *11–12.
[78] *See In re Facebook, Inc. Section 220 Deriv. Litig*., 2019 WL 2320842, at *14 n.150 (Del. Ch. May 30, 2019) (collecting cites); *see also In re Clovis Oncology, Inc. Deriv. Litig*., 2019 WL 4850188, at *12 (Del. Ch. Oct. 1, 2019) ("[A]s relates to *Caremark* liability, it is appropriate to distinguish the board's oversight of the company's *management of business risk* that is inherent in its business plan from the board's oversight of the company's *compliance with positive law*—including regulatory mandates."); *In re Goldman Sachs Grp., Inc. S'holder Litig.*, 2011 WL 4826104, at *21 (Del. Ch. Oct. 12, 2011) ("As a preliminary matter, this Court has not definitively stated whether a board's *Caremark* duties include a duty to monitor business risk.").

evolve" as "legal and regulatory frameworks" do.[79] But *Sorenson* did not address the question of whether an appropriate nexus existed between the corporate trauma—a cybersecurity breach—and the Board. And *Sorenson* specifically found that there was

> no known illegal conduct, lawbreaking, or violation[] of a regulatory mandate alleged in the Complaint that could support a finding that the [] Board faces a substantial likelihood of liability for failed oversight . . . . The plaintiff in this action has not pleaded particularized facts that the [] Board knowingly permitted Marriott to violate the law.[80]

Thus, despite the *Sorenson* court's discussion of the increasing importance of cybersecurity, echoed in this decision, *supra.*, *Sorenson* expressly looked to affirmative corporate illegality in assessing the substance of the *Caremark* claims. *Sorenson* ultimately suggests that even if lack of cybersecurity oversight might be an appropriate subject for a *Caremark* claim, a violation of law or regulation is still likely a necessary underpinning to a successful pleading. Unable to find one applicable to its facts, the court dismissed the complaint.

While no case in this jurisdiction has imposed oversight liability based solely on failure to monitor business risk, it is possible, I think, to envision an extreme hypothetical involving liability for bad faith actions of directors leading to such

[79] *Sorenson*, 2021 WL 4593777, at *11–12.
[80] *Id.* at *15.

liability.[81] 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. Oversight liability caselaw focusing on the "connection" element is comparatively thin, with virtually all of the discussion centered around illegal acts by the company stemming from company (board or management) action or inaction.[82] As the court in *Sorenson* aptly noted at the end of its analysis, the corporate trauma "that came to fruition was at the hands of a hacker. Marriott was the victim of an illegal act rather than the perpetrator."[83] So too with SolarWinds here. The pertinent question is not whether the Board was able to prevent a corporate trauma, here a third-party criminal attack. Instead, the question is whether the Board undertook its monitoring duties (to the extent applicable) *in bad faith*.

[81] *But see In re Citigroup Inc. S'holder Deriv. Litig.*, 964 A.2d 106, 126 (Del. Ch. 2009) ("To the extent the Court allows shareholder plaintiffs to succeed on a theory that a director is liable for a failure to monitor business risk, the Court risks undermining the well settled policy of Delaware law by inviting Courts to perform a hindsight evaluation of the reasonableness or prudence of directors' business decisions.").

[82] *See, e.g.*, *South v. Baker*, 62 A.3d 1, 14–15 (Del. Ch. 2012); *Pyott*, 46 A.3d at 340–41; *Okla. Firefighters Pension & Ret. Sys. v. Corbat*, 2017 WL 6452240, at *15 (Del. Ch. Dec. 18, 2017); *Horman v. Abney*, 2017 WL 242571, at *7 (Del. Ch. Jan. 19, 2017); *Reiter ex rel. Cap. One Fin. Corp. v. Fairbank*, 2016 WL 6081823, at *8 (Del. Ch. Oct. 18, 2016); *Pettry ex rel. FedEx Corp. v. Smith*, 2021 WL 2644475, at *7 (Del. Ch. June 28, 2021).

[83] *Sorenson*, 2021 WL 4593777, at *18.

I need not resolve these open questions in order to address the pending motions, which can be adequately resolved via a traditional "two prong" *Caremark* analysis, in any event. I turn now to that analysis.

1. Caremark's Doctrinal Underpinnings

At bottom, a meritorious *Caremark* claim demonstrates a breach of the duty of loyalty, by way of a failure by the directors to act in good faith. As Chancellor Allen wrote in *Caremark* itself,[84] and as has been reaffirmed by our Supreme Court in *Stone v. Ritter* and *Marchand v. Barnhill*, a lack of good faith is a "necessary condition" to a finding of nonexculpated oversight liability.[85] In *Stone*, the Delaware Supreme Court indicated that imposing oversight liability "requires a showing that the directors knew that they were not discharging their fiduciary obligations."[86]

Shortly thereafter, in *Desimone v. Barrows*, the Court of Chancery commented upon *Stone*, reading *Stone* to "ensure[] that the protections that exculpatory charter provisions afford to independent directors against damage claims would not be eroded" by expansion of the *Caremark* doctrine.[87] Stated differently, *Stone* stood for the proposition that despite the potential for oversight

[84] *In re Caremark Int'l Inc. Deriv. Litig.*, 698 A.2d 959, 971 (Del. Ch. 1996).
[85] *Stone ex rel. AmSouth Bancorporation v. Ritter*, 911 A.2d 362, at 370–71 (Del. 2006); *Marchand*, 212 A.3d at 820–21 (quoting *Desimone v. Barrows*, 924 A.2d 905, 935 (Del. Ch. 2007)) ("In other words, for a plaintiff to prevail on a *Caremark* claim, the plaintiff must show that a fiduciary acted in bad faith—'the state of mind traditionally used to define the mindset of a disloyal director.'").
[86] *Stone*, 911 A.2d at 370.
[87] *Desimone*, 924 A.2d at 935.

liability to attach to director judgments under *Caremark*, exculpatory charter provisions preventing a director from being held liable for a breach of the *duty of care* were to continue in force. Directors of a corporation with exculpatory charter provisions could continue to wield their business judgment—including "evaluation of risk"—under the umbrella protection of exculpation clauses, despite the *Caremark* specter.[88] In *Citigroup*, another *Caremark* case, the Court noted that "[i]t is almost impossible for a court, in hindsight, to determine whether the directors of a company properly evaluated risk and thus made the 'right' business decision."[89]

This state's courts, then, have acknowledged the importance of retaining the statutory safe harbor that Delaware General Corporation Law Section 102(b)(7) provides for director conduct that might otherwise give rise to a reasonably conceivable claim of a breach of the duty of care.[90] In other words, director gross negligence with respect to a corporate trauma is insufficient to establish director liability; such liability may only attach where a director acts in bad faith.

Marchand v. Barnhill is the latest word in Delaware Supreme Court cases that substantively treat the *Caremark* doctrine.[91] *Marchand* emphasizes again the requirement that directors act in a manner lacking good faith before a *Caremark*

---

[88] *Corbat*, 2017 WL 6452240, at *18 (citations omitted).
[89] *Citigroup*, 964 A.2d at 126 (citation omitted).
[90] 8 *Del. C.* § 102(b)(7). Section 102(b)(7) also indicates that charters cannot eliminate or limit director liability for breaches of the duty of loyalty or "for acts or omissions not in good faith or which involve intentional misconduct or a knowing violation of law." *See id.*
[91] *Marchand*, 212 A.3d 805.

claim can be considered viable.[92] That opinion notes that "[b]ad faith is established, under *Caremark*," by way of either prong one, "when the directors completely fail to implement any reporting or information system or controls," or via prong two, when directors, "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."[93] Per the Supreme Court in *Marchand*, "[u]nder *Caremark*, a director may be held liable if she acts in bad faith in the sense that she made no good faith effort to ensure that the company had in place any 'system of controls.'"[94] As I understand *Marchand*, the lack of a system of controls with respect to a *particular* incarnation of risk does not itself demonstrate bad faith; the lack of such system must be the result of action or inaction taken in bad faith. This distinction is heightened, I believe, in consideration of risk outside the realm of positive law.

Marchand does not undertake an analysis of bad faith under *Disney* or its progeny,[95] despite the concept's prominence in the opinion. As I read *Marchand*, directors must make a good faith effort to satisfy prongs one and two of *Caremark*. This interpretation is, I believe, bolstered by the opinion's further statement that "[i]f

[92] *Id.* at 820–24.
[93] *Id.* at 821 (cleaned up and emphasis added).
[94] *Marchand*, 212 A.3d at 821 (citations omitted).
[95] *See generally In re Walt Disney Co. Deriv. Litig.*, 906 A.2d 27 (Del. 2006).

Caremark means anything, it is that a corporate board must make a good faith effort to exercise its duty of care."[96] That is, directors cannot intentionally disregard their duties to be "informed of risks or problems requiring their attention,"[97] because such intentional disregard would constitute bad faith supporting a *Caremark* claim.

Marchand and the other caselaw discussed above thus demonstrate that it is necessary to assess a director's good or bad faith in connection with a plaintiff's allegations before an oversight liability claim can be deemed viable.

2. Considering the SolarWinds's Directors Bad Faith

Disney remains the preeminent word on good faith in Delaware caselaw.[98] In *Disney*, the Delaware Supreme Court adopted the following definitions of bad faith:

> [(i) w]here the fiduciary intentionally acts with a purpose other than that of advancing the best interests of the corporation, [(ii)] where the fiduciary acts with the intent to violate applicable positive law, or [(iii)] where the fiduciary intentionally fails to act in the face of a known duty to act, demonstrating a conscious disregard for his duties.[99]

Notably common among all three formulations here is an element of *intent*. That is, to act in bad faith, the directors must have acted with scienter, in that the directors had "actual or constructive knowledge that their conduct was legally improper."[100]

---

[96] *Id.* at 824.
[97] *Id.* at 821.
[98] 906 A.2d 27.
[99] *Id.* at 67.
[100] *City of Birmingham Ret. & Relief Sys. v. Good*, 177 A.3d 47, 55 (Del. 2017); *see also Boeing*, 2021 WL 4059934, at *24–25 (quoting *Stone*, 911 A.2d at 370)).

And, as mentioned above, showing scienter in the context of a Rule 23.1 motion to dismiss requires a plaintiff to plead supporting facts with particularity, from which a plaintiff-friendly inference of bad faith may arise.[101]

The Plaintiffs allege that the directors behaved in a manner contrary to positive law,[102] but this is not supported by the Complaint. The Complaint cites a number of "warnings" by government agencies[103] and private companies.[104] Its strongest fact is that the SEC in 2018 issued "new interpretive guidance" about disclosures around cybersecurity risks, including a statement that "[c]ompanies are required to establish and maintain appropriate and effective disclosure controls and procedures[,] including those related to cybersecurity[.]"[105] While this guidance is certainly indicative of requirements regarding public company disclosures, it does not establish positive law with respect to required cybersecurity *procedures* or how to manage cybersecurity risks. NYSE—the stock exchange upon which SolarWinds is listed—has also promulgated a "guide" to cybersecurity, which the Complaint references, but this guide is also not positive law.[106] The Plaintiffs did not plead that this guide was binding. In other words, the Plaintiffs have not alleged that "legal

[101] *See, e.g.*, *Wood*, 953 A.2d at 141.
[102] Compl. ¶ 118.
[103] *Id.* ¶¶ 6, 44–56.
[104] *Id.* ¶¶ 7, 44–56.
[105] *Id.* ¶ 59.
[106] *Id.* ¶¶ 64–67.

and regulatory frameworks" have "evolve[d]" with respect to cybersecurity, such that SolarWinds's corporate governance practices must have followed.[107]

The Complaint also does not plead with particularity that the SolarWinds directors intentionally acted with a purpose inimical to the corporation's best interests and, so far as I can tell, the Plaintiffs do not attempt to put that argument forward here.

The last, best argument available to the Plaintiffs in this action is that the directors demonstrated a conscious disregard for their duties by intentionally failing to act in the face of a known duty to act,[108] either by ignoring red flags so vibrant that scienter is implied, or by utterly failing to put into place a mechanism for monitoring or reporting risk. The Complaint discusses in considerable detail the actions and inactions of the SolarWinds Board and various Board committees with respect to cybersecurity, and I take all of the allegations in the Complaint as true, given the procedural posture here. Again, the Plaintiffs are also entitled to the benefits of all reasonable inferences at this stage.

But even with this plaintiff-friendly tailwind, the Complaint does not clear the high hurdle of pleading scienter with particularity. To establish that the directors acted in bad faith, a predicate to oversight liability, the Plaintiffs must make out a

[107] *Sorenson*, 2021 WL 4593777, at *12.
[108] Assuming, without finding, that directors have a "known duty" to act with respect to cybersecurity.

particularized allegation of facts from which I may infer scienter on the part of the directors.[109] To the extent the Plaintiffs argue that I should infer scienter exists due to a "sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists,"[110] or lack of action in the face of "red flags" manifesting a duty to act, I find that such an inference would not be reasonable here.

I first address the red flags, indifference to which, per Plaintiffs, implies bad faith. The positive facts pled that support the Plaintiffs' position are: a reference in the Complaint to the Company's NCG Committee "effectively ignor[ing]" cybersecurity warnings it received at a presentation in 2019;[111] a description of a *2017* cybersecurity presentation given to management by the Company's former Global Cybersecurity Strategist and a later resignation email complaining that changes he requested prior to his departure were not implemented;[112] and a vestigial and patently insecure password used by the Company that was created in 2017 but survived at least until November 2019.[113]

---

[109] *See, e.g.*, *Boeing*, 2021 WL 4059934, at *25.
[110] *South*, 62 A.3d at 15–16 (quoting *Caremark*, 698 A.2d at 970)).
[111] Compl. ¶ 78.
[112] *Id.* ¶ 97.
[113] *Id.* ¶¶ 81–84. The Complaint also pleads a number of business practices, described as "gross deficiencies," seemingly in support of a red-flags type argument. These include the allegations that SolarWinds did not properly "segment" its information technology networks, that it directed clients to disable antivirus scanning and firewall protection in order to use Orion, that it cut investments in cybersecurity, and that it listed high-value clients on their website. *See id.* ¶ 80.

Taking these in turn: the NCG Committee's receipt of the Cybersecurity Briefing, itself, is not a red flag or a fact supportive of bad faith or scienter. It was, in fact, an instance of oversight. As presented in the Complaint, the Cybersecurity Briefing was not indicative of an imminent corporate trauma. It reflected the concept that the Company *might become* the subject of a cyberattack and described the manner in which the Company was successful in preventing any such trauma. The pleading that the NCG Committee effectively ignored the presentation is conclusory. It is not pled that the presentation made action by the Board necessary.

The facts regarding the Company's Global Cybersecurity Strategist are outside the relevant time period, and further, there is no pleading that the Board was aware of either the presentation he gave before departure or the complaints he made in his resignation email. The Complaint instead indicates that the Global Cybersecurity Strategist's presentation was made to "technology and marketing executives" in the non-public company, pre-IPO, and that he resigned in an email to the Chief Marketing Officer.[114] Given its lack of knowledge, the Board cannot have acted in bad faith in response (or a lack of response) thereto.

These decisions are business decisions rather than particularized incidents giving rise to red flags. The answering brief also alleges that generalized industry warnings constituted red flags. *See* AB 52–53. Failing to take industry warnings into account, I may presume, is bad *practice*, but is insufficient to plead bad faith failure *to oversee SolarWinds particularly*, as was the fiduciary duty of the Board.

[114] Compl. ¶ 97.

Finally, and most seriously, the Complaint pleads a failure of cybersecurity in that the Company had a jejune, even farcical, password—'solarwinds123'—in place in a manner that could have compromised Company security from as early as 2017 until November 2019.[115] In November 2019, an unaffiliated third party sent an email to SolarWinds's information technology team informing them of this security deficiency.[116] But again, it is not pled that the Committees were ever told that this incident had occurred. There is no indication that management knew of the solarwinds123 password being in place when the Cybersecurity Briefing was given in February 2019, and there is no indication that either the Committees or the full Board were ever apprised of the password deficiency. Without such knowledge, the Board again cannot have acted in bad faith relating to this incident.

The stronger argument is that the facts above are not themselves "red flags" but instead indicate the lack of an effective reporting system. The Plaintiffs note that the Board as a whole received no briefing about cybersecurity risk—indeed, the Plaintiffs plead that the "Board did not conduct a single meeting or have a single discussion about the Company's mission critical cybersecurity risks"[117] in its two-year pre-attack existence.

[115] *Id.* ¶ 81–82.
[116] *Id.* ¶ 81–84.
[117] *Id.* ¶ 71.

The Complaint notes that "[f]ollowing the Company's IPO," the Board had delegated cybersecurity oversight to the Audit Committee,[118] but also that the Audit Committee "never reported to the Board about cybersecurity risks."[119] The Audit Committee charter, per the Complaint, instructs the Audit Committee to discuss "with *management* the Company's major financial risk exposures, including . . . cyber and data security."[120]

The Complaint also acknowledges that the NCG Committee had oversight responsibility for cybersecurity, as the NCG Committee was responsible for "oversight responsibility for corporate governance risks" as of the time SolarWinds completed its IPO in October 2018.[121] The Company identified the NCG Committee in multiple proxy statements as "monitor[ing] and assess[ing] the effectiveness of our corporate governance guidelines *and our policies, plans and programs relating*

[118] This was apparently in addition to the NCG Committee, which retained general risk management oversight, although the documents supporting the delegation of authority are not available to me at this stage. The Complaint does not plead that the Audit Committee's receipt of oversight authority divested the NCG Committee of oversight authority, and as I understand the pleadings, the Committees' roles were essentially duplicative in this area.

[119] *Id.* ¶ 72. The Complaint also asserts that the Audit Committee never held any discussion regarding the Company's cybersecurity or risks. This the Defendants contest, pointing to a document not produced until after the filing of the Complaint; the document should have been included in the Section 220 production associated with this action, but was not. The challenged document is a set of Audit Committee meeting minutes indicating a discussion about cybersecurity risk did indeed take place in April 2020. I need not determine whether the minutes can be considered at this stage, given their exceedingly late production, because I find their consideration would not change the outcome here.

[120] *Id.* (emphasis added).

[121] *Id.* ¶ 10.

to cyber and data security."[122] That is, the NCG Committee was to oversee business risk. And the NCG Committee received a presentation in February 2019 entitled "Risk Management Topic: Cybersecurity Briefing."[123] The minutes from that NCG Committee meeting indicate that Joe Kim, Rani Johnson, and Tim Brown, each a member of Company management, presented on "the Company's risk management and mitigation policies and initiatives related to cybersecurity," and that a "discussion ensued."[124]

Two months later, in April 2019, the NCG Committee amended its charter to specify "cyber and data security" as a major risk exposure within the Committee's risk management.[125] Like the Audit Committee, the NCG Committee's charter specifically stated the Committee would "[d]iscuss with management the Company's major risk exposures, including [among other topics] cyber and data security."[126]

The Complaint also notes that the NCG Committee "apparently attempted to schedule a subsequent meeting to discuss the Company's cybersecurity" in January 2020, but that this meeting never occurred.[127] The Sunburst Attack occurred late that same year.

---

[122] *Id.* ¶ 63.
[123] *Id.* ¶ 39.
[124] Reed Decl., Ex. 12, at SW_SEAVITT 220_000000805–06.
[125] Compl. ¶ 10.
[126] *Id.* ¶ 75.
[127] *Id.* ¶ 74.

I read the Complaint as indicating that both of the Committees were charged with oversight responsibility for cybersecurity. The next question is whether I can infer that the Committees' failure to report to the Board regarding cybersecurity risk over a period of 26 months (from latest IPO to the Sunburst Attack) was reflective of bad faith, on the part of a majority of directors.

This inference I find unwarranted. To be sure, nominal acts of delegation, such as delegating oversight responsibility to a Board subcommittee that failed to meet, or that failed to investigate serious misconduct after being put on notice, are not preclusive of an oversight claim.[128] But the Complaint does not allege that the Audit Committee failed to meet; it alleges that the Audit Committee "did not hold one meeting or discussion concerning any aspect of the Company's cybersecurity" within a period of 26 months.[129] There is no indication in the complaint that the Audit Committee was simply a nominal, sham committee, and it would not be reasonable to infer such.

In the case of the NCG Committee, there are affirmative facts pled in the Complaint indicating that the committee not only met, but that it *met and discussed*

[128] *See, e.g.*, *David B. Shaev Profit Sharing Acct. v. Armstrong*, 2006 WL 391931, at *5 (Del. Ch. Feb. 13, 2006), *aff'd*, 911 A.2d 802 (Del. 2006); *Rich ex rel. Fuqi Int'l, Inc. v. Chong*, 66 A.3d 963, 980 (Del. Ch. 2013) (quoting *Stone*, 911 A.2d at 370) ("Examples of directors' 'disabling themselves from being informed' include a corporation's lacking an audit committee, or a corporation's not utilizing its audit committee.").

[129] Compl. ¶ 72. The Plaintiffs' counsel, at oral argument, appeared to concede that the Audit Committee did in fact meet. *See* Oral Arg. 56:1–58:4. I do not rely on this concession, in any event.

the pertinent issue, cybersecurity, both via receipt of a management presentation and then again in discussion following the presentation.[130] Following the Cybersecurity Briefing, the NCG Committee in April 2019 amended its charter to expressly address cybersecurity,[131] indicating that the topic had arisen at a subsequent meeting. The Plaintiffs also point out that the NCG Committee had at least referenced a follow-up discussion about cybersecurity—possibly to take place in January 2020—though they note that no follow-up occurred.[132] The Plaintiffs' argument remains true, however, that there is nothing in the pleadings showing the NCG Committee ever spoke to the *Board as a whole* regarding cybersecurity concerns. The Complaint is silent as to what management told the NCG Committee that is sufficient to imply bad faith in the failure to communicate such information to the Board; what actions should have been recommended, if any; or what could have been done to prevent the Sunburst Attack.

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. Without a pleading about the

[130] *See* Reed Decl., Ex. 1. Management's presentation identified cybercriminal activity as a ubiquitous threat, but there is no allegation that recommendations for corporate action were communicated to the Committees or the Board, let alone ignored thereby.
[131] Compl. ¶ 10.
[132] *Id.* ¶ 74.

Committees' awareness of a particular threat, or understanding of actions the Board should take, the passage of time alone under these particular facts does not implicate bad faith.[133] 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.[134] 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. 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—and without a pleading of what information Committee members possessed which raised a good-faith duty to report, is simply unwarranted.

Certainly, the actions (or omissions) of the Committees in carrying out their oversight duties here appear in hindsight far from ideal. I agree fully with the *Sorenson* court that good corporate practice requires director consideration of potential risks to customers; particularly so, perhaps, regarding cybersecurity. That

[133] *Cf. Chong*, 66 A.3d at 980 ("I am conscious of the need to prevent hindsight from dictating the result of a *Caremark* action; a bad outcome, without more, does not equate to bad faith.").
[134] *South*, 62 A.3d at 18–19 (citation omitted) ("Directors who try to 'get this balance right[]' are protected by the business judgment rule, even if they fall short in the attempt.").

does not mean the actions of the Committees, as pled, imply scienter supporting bad faith. Even if the acts of the Committees did implicate bad faith, those actions would not necessarily implicate the directors not serving therein. Having delegated oversight of risk to two non-sham, functioning Committees, the failure of those Committees to make a Board presentation on a particular risk in a particular year, without more, does not to my mind give rise to an inference that the *Board* intentionally disregarded its oversight duties in bad faith.[135] The fact that the Board did not receive reports from the Committees with respect to cybersecurity over a 26-month period, I may infer, should have been, to a prudent director, of concern, but failure to demand a presentation, without facts pled implying that the directors were aware of a failure of Committee duties, does not implicate bad faith—instead, it goes to the duty of care, not loyalty.[136] It is not indicative of an utter failure of reporting and control for the Board to delegate risk assessment to the Committees, and then fail to demand an accounting of a particular business risk. As this Court noted in

---

[135] *But see Hughes v. Hu*, 2020 WL 1987029, at *15 (Del. Ch. Apr. 27, 2020) (emphasis added) ("These chronic 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.").

[136] The Complaint also alleges that the Company created a Technology and Cybersecurity Committee "at a special meeting of the board in early January 2021," and tasked it with helping the Board to fulfill its oversight responsibilities, including oversight of the Company's IT systems and cybersecurity generally. Compl. ¶ 76. Although the Plaintiffs frame the creation of this new committee as an admission that the Board had failed in its oversight responsibilities prior to the Sunburst Attack, "[t]hese actions do not bespeak faithless or imprudent fiduciaries." *Ash v. McCall*, 2000 WL 1370341, at *15 (Del. Ch. Sept. 15, 2000) (discussing defendant directors' "immediately" taking "decisive steps to disclose and cure" corporate trauma leading to a *Caremark* claim).

Boeing, the "'intentional dereliction of duty' or 'conscious disregard for one's responsibilities' . . . 'is more culpable than simple inattention or failure to be informed of all facts material to the decision,'" instead requiring that "directors have acted in bad faith and cannot avail themselves of defenses grounded in a presumption of good faith"[137] to raise the inference of liability. Here, inferences cannot take the Plaintiffs from inattention to intentional dereliction.

To recapitulate, a subpar reporting system between a Board subcommittee and the fuller Board is not equivalent to an "utter failure to attempt to assure" that a reporting system exists.[138] The short time period here between the IPO and the trauma suffered, together with the fact that the Board apparently did not request a report on cybersecurity in that period, is not sufficient for me to infer an *intentional* "sustained or systematic failure" of oversight,[139] particularly given directors are *presumed* to act in good faith.[140] And again, the Complaint is silent as to what the

[137] *Boeing*, 2021 WL 4059934, at *25 (citing *Disney*, 906 A.2d at 66; then citing *Citigroup*, 964 A.2d at 125).
[138] *See South*, 62 A.3d at 18 (citing *Caremark*, 698 A.2d at 971) ("These pled facts do not support an inference of an 'utter failure to attempt to assure a reasonable information and reporting system exists,' but rather the opposite: an evident effort to establish a reasonable system.").
[139] No facts are pled regarding the frequency of Board subcommittee meetings.
[140] *Cf. Citigroup*, 964 A.2d at 125 ("The presumption of the business judgment rule, the protection of an exculpatory Section 102(b)(7) provision, and the difficulty of proving a *Caremark* claim together function to place an extremely high burden on a plaintiff to state a claim for personal director liability for a failure to see the extent of a company's business risk."); *see id.* at 136 (internal quotations omitted) ("[T]he plaintiff must overcome the general presumption of good faith . . . .").

Committees should in good faith have reported, and how it could have mitigated corporate trauma.

Carelessness absent scienter is not bad faith. In sum, the Complaint has not pled sufficient particularized facts to support a reasonable inference of scienter and therefore actions taken in bad faith by the Board. Without a satisfactorily particularized pleading allowing reasonably conceivable inference of scienter, a bad faith claim cannot survive a motion to dismiss. Because the *Caremark* claim is not viable, there is no substantial likelihood of liability attaching to a majority of the directors on the demand Board. Therefore, demand on the Board would not have been futile.

B. The Plaintiffs' Second Theory of Demand Futility

The Plaintiffs make another argument as to a majority of the demand Board. They argue that the demand Board is incapable of impartially evaluating a demand because that majority granted Defendant Thompson a release for any actions taken as Company CEO or director.[141] The legal theory they seek to advance is, to me, unclear, and the release theory is not discussed in the single count of the Complaint. This demand futility argument fails for want of particularized pleading, as well.

[141] Compl. ¶ 116.

The Defendants' motions to dismiss must therefore be granted for failure to establish demand futility under any theory. Accordingly, I need not examine the Defendants' motions to dismiss under Rule 12(b)(6).

III. CONCLUSION

For the foregoing reasons, Defendants' motions to dismiss under Rule 23.1 are GRANTED. The parties should submit a form of order consistent with this Memorandum Opinion.