EFiled: Feb 08 2023 10:01AM EST
Filing ID 69097615
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, 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-Below/ Appellees, and **SOLARWINDS CORPORATION**, Nominal Defendant-Below/ Appellee.	C.A. No. 411, 2022 APPEAL FROM THE COURT OF CHANCERY OF THE STATE OF DELAWARE, C.A. NO. 2021-0940-SG [redacted] REDACTED PUBLIC VERSION FILED: February 8, 2023

APPELLEES' ANSWERING BRIEF

OF COUNSEL:

Paul R. Bessette
Michael J. Biles
Tyler W. Highful
KING & SPALDING LLP
500 W. 2nd Street, Suite 1800
Austin, TX 78701

Benjamin Lee
Benjamin B. Watson
KING & SPALDING LLP
1180 Peachtree Street, NE
Atlanta, GA 30309

John L. Reed (I.D. No. 3023)
Ronald N. Brown, III (I.D. No. 4831)
Peter H. Kyle (I.D. No. 5918)
Kelly L. Freund (I.D. No. 6280)
DLA PIPER LLP (US)
1201 North Market Street, Suite 2100
Wilmington, DE 19801
(302) 468-5700
(302) 394-3241 (Fax)
john.reed@dlapiper.com
ronald.brown@dlapiper.com
peter.kyle@dlapiper.com
kelly.freund@dlapiper.com

Attorneys for Nominal Defendant-Below/Appellee SolarWinds Corporation

OF COUNSEL:

Sandra C. Goldstein, P.C.
Stefan Atkinson, P.C.
Byron Pacheco
KIRKLAND & ELLIS LLP
601 Lexington Avenue
New York, New York 10022
(212) 728-8000

Raymond J. DiCamillo (#3188)
Kevin M. Gallagher (#5337)
Alexander M. Krischik (#6233)
Christian C. F. Roberts (#6694)
RICHARDS, LAYTON & FINGER, P.A.
920 North King Street
Wilmington, Delaware 19801
(302) 651-7700

Attorneys for Defendants-Below/Appellees William Bock, Seth Boro, Paul J. Cormier, Michael Hoffman, Dennis Howard, Catherine R. Kinney, James Lines, and Easwaran Sundaram

OF COUNSEL:

Sameer Advani
Wesley R. Powell
Patricia O. Haynes
WILLKIE FARR & GALLAGHER LLP
787 Seventh Avenue
New York, New York 10019
(212) 728-8000

William M. Lafferty (#2755)
Ryan D. Stottmann (#5237)
Alexandra M. Cumings (#6146)
MORRIS NICHOLS ARSHT & TUNNELL LLP
1201 North Market Street
Wilmington, Delaware 19801
(302) 658-9200

Attorneys for Defendants-Below/Appellees Mike Bingle, Kenneth Hao, Jason White, and Michael Widmann

OF COUNSEL:

Peter L. Welsh
C. Thomas Brown
Patrick T. Roath
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
(617) 951-7865

Edward R. McNicholas
ROPES & GRAY LLP
2099 Pennsylvania Avenue, N.W.
Washington, DC 20006
(202) 508-4600

Stephen C. Childs (#6711)
ABRAMS & BAYLISS LLP
20 Montchanin Road, Suite 200
Wilmington, DE 19807
(302) 778-1150
childs@abramsbayliss.com

Counsel for Defendant-Below/ Appellee Kevin B. Thompson

DATED: January 19, 2023

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES **PAGE(S)**

OTHER AUTHORITIES

NATURE OF PROCEEDINGS

The Court of Chancery correctly dismissed the Complaint below under Rule 23.1 because Appellants/Plaintiffs-Below ("Plaintiffs") failed to plead that a majority of the Demand Board of Appellee/Nominal Defendant-Below SolarWinds Corporation ("SolarWinds" or "the Company") faced "a substantial likelihood" of personal liability for failure to oversee cybersecurity risks at SolarWinds. Plaintiffs' allegations and information incorporated by reference or subject to judicial notice showed that the SolarWinds Board of Directors: (1) implemented board-level monitoring and reporting on cybersecurity risks; and (2) did not willfully ignore any "red flags" of cybersecurity threats sufficient to show a conscious disregard of a known duty. Plaintiffs also failed to plead that SolarWinds violated any existing law or regulation concerning information security. On this record, the Court of Chancery appropriately ruled that Plaintiffs' Complaint fell short of the demanding standards necessary for imposing personal director liability under *In re Caremark Int'l Inc., Deriv Litig*., 698 A.2d 959 (Del. Ch. 1996). Respectfully, this Court should affirm.

Plaintiffs' arguments on appeal are factually and legally flawed. The main thrust of Plaintiffs' appeal is that the SolarWinds Board only "nominally" delegated oversight of cybersecurity risks to the Company's Nominating and Corporate Governance Committee ("NCG Committee") and Audit Committee. But Plaintiffs' own allegations contradict that assertion. As the Complaint alleges, the NCG

Committee received a detailed presentation from SolarWinds executives on February 19, 2019 that [redacted] In April 2020, SolarWinds' Chief Information Officer also made a presentation to the Audit Committee [redacted] The Company made each of these reports for the specific purpose of apprising the Board of ongoing cybersecurity risks.

These presentations demonstrate that, contrary to Plaintiffs' theory, the SolarWinds Board in fact had an effective board-level cybersecurity monitoring and reporting system in place. The Company designed this system in recognition of the cybersecurity threats it faced and with the explicit purpose of keeping the Board apprised of steps the Company implemented (and planned to take) to combat the threat, notwithstanding that SolarWinds had not encountered a material

cybersecurity incident to date. This is the opposite of the type of sustained and utter failure to implement reporting systems or conscious disregard of red flags required to state a claim under *Caremark*.

As the Court of Chancery's decision properly recognized, Plaintiffs' allegations here come nowhere close to the kinds of facts alleged in cases that have survived a motion to dismiss. In those cases, plaintiffs have alleged what amounts to a complete abandonment of risk oversight by the board. Bad faith has been presumed where boards fail to impose *any* systems for reporting risks or violations, and where that failure led the company to violate laws or regulations. Bad faith has also been presumed based on allegations that boards ignored numerous red flags that should have pointed them to the existence of risks that later materialized.

No such abandonment of oversight is present here. To the contrary, the SolarWinds Board placed such importance on cybersecurity that it tasked two different committees with responsibility to oversee cybersecurity risks. Those committees engaged in substantive oversight. The primary "red flag" Plaintiffs have identified was a single weak password—unrelated to Sunburst and used only in a testing environment—that was promptly fixed when discovered and which Plaintiffs do not causally connect to the incident giving rise to this litigation: Sunburst.

While Plaintiffs chastise the SolarWinds Board for not holding additional meetings to discuss cybersecurity issues, 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.

In sum, Plaintiffs' theory radically departs from the typical circumstances in which *Caremark* liability has been recognized in Delaware, and it should be rejected here. It is one thing for directors to face oversight liability for failing to navigate and comply with known affirmative legal obligations in highly regulated industries, but it would be an unwarranted expansion of *Caremark* to effectively put directors at personal risk of liability for the alleged failure to adequately implement and monitor measures if those measures do not prevent a sophisticated and determined attack by a nation-state actor. Plaintiffs essentially seek to make SolarWinds' directors guarantors against cyberattacks by sophisticated criminal actors. That is not, and should not be, Delaware law.

The Court of Chancery's Order Dismissing Plaintiffs' Derivative Complaint with Prejudice should be affirmed.

SUMMARY OF ARGUMENT

1. DENIED. Dismissal under Court of Chancery Rule 23.1 was warranted because Plaintiffs have not adequately pleaded that demand is excused on the basis that a majority of the Demand Board faces a substantial likelihood of liability for failing to fulfill their oversight duties under the standards set forth in *In re Caremark Int'l Inc. Deriv. Litig.*, 698 A.2d 959 (Del. Ch. 1996) and *Stone v. Ritter*, 911 A.2d 362 (Del. 2006).

COUNTER-STATEMENT OF FACTS

SolarWinds avoids repeating background allegations recited by Plaintiffs where possible, Sup. Ct. R. 14(b)(v), and incorporates the summary of alleged facts set forth in the Court of Chancery's Opinion. (*See* Op. at 5–12.)

A. The Parties

Nominal Defendant SolarWinds is a Delaware corporation and the world's leading provider of information technology ("IT") infrastructure management software. (Op. at 5, A30 ¶ 2.) Contrary to Plaintiffs' allegation that SolarWinds is a "monoline" company (Op. Br. at 1), SolarWinds offers more than 90 software products that help IT professionals solve numerous system problems. (B16.) Over 300,000 customers use SolarWinds software, including many Fortune 500 companies and United States government agencies. (*Id.*) The company's flagship product is the Orion Platform ("Orion"). (*Id.*)

Defendants William Bock, Seth Boro, Kenneth Hao, Michael Hoffman, Dennis Howard, Catherine Kinney, James Lines, Easwaran Sundaram, and Michael Widmann served as members of the SolarWinds Board of Directors at the time the Plaintiffs filed their Complaint on November 1, 2021. (Op. at 6–7; A94 ¶ 113.) Sudhakar Ramakrishna and Doug Smith also served on the SolarWinds Board at the time Plaintiffs initiated this litigation but were not named as defendants. (*Id.*)

Collectively, the eleven directors serving on the SolarWinds Board of Directors on November 1, 2021, are the "Demand Board." (*Id.*)

Defendants Mike Bingle, Paul J. Cormier, Kevin B. Thompson, and Jason White are former members of the SolarWinds Board of Directors. (Op. at 6–7, A38 ¶ 20, A39–40 ¶ 23, A43–44 ¶¶ 30–31.) Mr. Thompson served as SolarWinds' President and Chief Executive Officer from March 2020 to December 2020, resigning as planned before SolarWinds' discovery of the Sunburst attack. (Op. at 7, A43–44 ¶ 30.)

Plaintiffs allege that they are current SolarWinds stockholders who purport to have purchased shares of SolarWinds during the "relevant period" and have held the shares since that time. (Op. at 5, A37 ¶ 18.)

B. SolarWinds' Board-Level Oversight of Cybersecurity

Following an initial public offering ("IPO") in 2018, SolarWinds created an Audit Committee and a Nominating and Corporate Governance Committee ("NCG Committee"). (Op. at 7.) The Board of Directors assigned the NCG Committee oversight of corporate risks. In April 2019, SolarWinds amended that Committee's charter to require its members to discuss SolarWinds' major risk exposures with management, specifically including cyber- and data security. (Op. at 8, A72 ¶ 75.)

In February 2019, the NCG Committee met for a detailed briefing on cybersecurity from SolarWinds executives. (Op. at 9, A70–71 ¶ 73.) The presentation included the following information:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

- [redacted]

Following this presentation, the minutes of the meeting show [redacted] (Op. at 9.)

SolarWinds' Corporate Governance Guidelines charged a different committee—the Audit Committee—with oversight of data-security risks. (*Id.*, A70 ¶ 72.) As with the NCG Committee's amended charter, the Audit Committee charter mandated that the Committee's members discuss SolarWinds' major areas of potential financial risk exposures, including cyber- and data security, with management. (*Id.*) Consistent with its charter, in April 2020 the Audit Committee received an update from SolarWinds' Chief Information Officer ("CIO") on [redacted] The minutes for the April 13, 2020 meeting show [redacted] (B108-110.)

C. The Russian Foreign Intelligence Service's "Sunburst" Attack

In December 2020, SolarWinds announced that hackers—now understood to be operatives of the Russian Foreign Intelligence Service—had compromised the SolarWinds Orion software and infected certain Orion releases with a malicious code known as "Sunburst." (A87–89, ¶¶ 99–103.) Investigation into the attack

revealed that the hackers were highly sophisticated and among the most skilled in the world. (B92-93, B96.) Moreover, it is estimated that at least a thousand engineers were required to execute the attack. (B18.) In other words, Sunburst was a highly sophisticated cyberespionage operation led by state-backed actors—not a garden variety cybercrime. (B55.)

ARGUMENT

I. THE COURT OF CHANCERY CORRECTLY RULED THAT PLAINTIFFS FAILED TO PLEAD WITH PARTICULARITY THAT A MAJORITY OF THE DEMAND BOARD FACES A SUBSTANTIAL LIKELIHOOD OF LIABILITY UNDER *CAREMARK*

A. Question Presented

Did Plaintiffs adequately plead that a majority of the directors of the Demand Board face a substantial likelihood of liability for failing to fulfill their duty to oversee cybersecurity risks under *Caremark*, 698 A.2d 959, as applied in *Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019), where SolarWinds' Board specifically delegated the oversight of cybersecurity risks to the NCG Committee and Audit Committee, and both committees received substantive presentations by management on cybersecurity risks during the relevant period? (Preserved at A161-212.)

B. Standard And Scope Of Review

This Court's "review of decisions of the Court of Chancery applying Rule 23.1 is *de novo* and plenary." *United Food and Commercial Workers Union v. Zuckerberg*, 262 A.3d 1034, 1047 (Del. 2021). The Court "may affirm on the basis of a different rationale than that which was articulated by the trial court." *Unitrin, Inc. v. Am. Gen. Corp.*, 651 A.2d 1361, 1390 (Del. 1995). And while the Court rules on "issue[s] fairly presented to the trial court," *id.*, the "merits of any argument that

is not raised in the body of the opening brief shall be deemed waived and will not be considered by the Court on appeal," Sup. Ct. R. 14(b)(vi)(A)(3).

C. Merits Of The Argument

1. Plaintiffs Failed To Allege That A Majority Of The Demand Board Faces A Substantial Likelihood Of Liability Under *Caremark*'s First Prong

Plaintiffs here sought to plead the futility of a pre-suit demand under Rule 23.1 by alleging that a majority of the Demand Board faces a "substantial likelihood" of personal liability under *Caremark*, 698 A.2d at 970. Under the first prong of *Caremark*, directors may be liable only if they have utterly failed to create a system of oversight to ensure their company's compliance with the law. *Id.* at 971.

Importantly, this prong does not allow second-guessing board decisions to implement a system of oversight or probe the sufficiency of such oversight, only its existence. *See, e.g.*, *Firemen's Ret. Sys. of St. Louis ex rel. Marriott Int'l, Inc. v. Sorenson*, 2021 WL 4593777, at *12 (Del. Ch. Oct. 5, 2021) ("plaintiff must show that the director made no good faith effort to ensure the company had in place *any* system of controls") (internal citations and quotations omitted) (emphasis added); *In re Gen. Motors Co. Deriv. Litig.*, 2015 WL 3958724, at **14–15 (Del. Ch. June 26, 2015) (allegations that risk reporting system "should have been [] better" failed to plead a claim under prong one of *Caremark*), *aff'd*, 133 A.3d 971 (Del. 2016); *City of Detroit Police & Fire Ret. Sys. v. Hamrock*, 2022 WL 2387653, at *12 (Del. Ch.

June 30, 2022) (noting that the "utter failure" standard for liability under prong one of *Caremark* is "a linguistically extreme formulation intended to set a high bar when articulating the standard to hold directors personally liable for a failure of oversight") (internal quotation marks omitted).

The standard of liability is extremely high because determination of the level of resources devoted to business risk management is a classic discretionary exercise that is properly within the business judgment of the Board of Directors. *See Marchand*, 212 A.3d at 821. Courts should not usurp the Board's role and substitute their own judgment. *Id*. ("we are not examining the effectiveness of a board-level compliance and reporting system after the fact"). Instead, the question is simply whether the Board demonstrated good faith by engaging with the issue and attempting to establish a system of oversight. *Id*. ("the board must make a good faith effort—*i.e.*, try—to put in place a reasonable board-level system of monitoring and reporting."); *accord Fisher v. Sanborn*, 2021 WL 1197577, at *11 (Del. Ch. Mar. 30, 2021) (dismissing *Caremark* prong-one claim where "[p]laintiff's own brief concedes" the existence of a board-level monitoring system thus foreclosing a prong-one claim); *In re LendingClub Corp. Deriv. Litig*., 2019 WL 5678578, at *9–10 & n.59 (Del. Ch. Oct. 31, 2019) (same); *Gen. Motors*, 2015 WL 3958724, at *14–15 (same).

Here, the SolarWinds Directors engaged in good faith with the important topic of cybersecurity, designating the NCG and Audit Committees of the Board to have joint responsibility for oversight of this issue. (Op. at 7; A70 ¶ 72.) It is well-settled law that a board may delegate important functions, including oversight, to its committees. *See Hamrock*, 2022 WL 2387653, at *1 (dismissing *Caremark* claim where board designated oversight of safety issues to a committee.)

The Company amended the charter of the NCG Committee in April 2019 to include a requirement to "discuss with management the Company's major risk exposures, including cyber and data security." (Op. at 30; A72 ¶ 75.) Likewise, the Audit Committee was tasked with specific oversight of data security. (Op. at 30.) And both the NCG Committee and the Audit Committee received detailed cybersecurity briefings during the relevant time period that satisfied the directors' good-faith duty to attempt to ensure that a system of oversight was in place to manage cybersecurity risks. (*See generally* B61-89 & B108-110.)

Plaintiffs cite several *Caremark* cases in support of the proposition that the SolarWinds Directors should face a substantial likelihood of liability under *Caremark's* first prong, including *Marchand* and *Boeing*. But those cases are distinguishable. These distinctions clarify that the actions of the SolarWinds Directors fall far outside the "bad-faith" realm required by the first prong of *Caremark*.

a. Unlike In *Caremark* And Its Progeny, Plaintiffs Have Not Alleged Any Violation Of Positive Law Governing SolarWinds' Cybersecurity Practices

The first major distinction between this case and the *Caremark* line of cases is that there is no allegation that SolarWinds' Board failed to ensure the Company's compliance with regulatory or statutory requirements. In *Caremark*, the underlying issue was whether the Board failed to provide oversight when its executives authorized the company's entrance into illegal kickback arrangements with healthcare providers to prescribe Caremark products and services that resulted in fines and penalties amounting to over $250 million. *Caremark*, 698 A.2d at 961. Likewise, both *Marchand* and *Boeing* concerned compliance with important safety laws and regulations governing the areas of food safety and air transportation respectively. *See Marchand*, 212 A.3d at 821-22; *In re Boeing Co. Deriv. Litig.*, 2021 WL 4059934, at *5 (Del. Ch. Sept. 7, 2021).

Here, Plaintiffs have not cited any violation by SolarWinds of positive law or any applicable regulation requiring SolarWinds to implement specific cybersecurity measures. To be sure, Plaintiffs' own allegations and documents incorporated by reference confirm that SolarWinds chose to adopt robust cybersecurity protections. But the Company's decision to do so reflects an exercise of quintessential business judgment—a balancing of trade-offs, where the variety of threats is nearly infinite, and each new countermeasure carries a cost. Accordingly, "Delaware courts have

not broadened a board's *Caremark* duties to include monitoring risk in the context of business decisions." *Sorenson*, 2021 WL 4593777, at *12; *see also, In re Citigroup Inc. S'holder Deriv. Litig.*, 964 A.2d 106, 131 (Del. Ch. 2009) ("There are significant differences between failing to oversee employee fraudulent or criminal conduct and failing to recognize the extent of a Company's business risk."); *Reiter on Behalf of Capital One Fin. Corp. v. Fairbank*, 2016 WL 6081823, at *8 (Del. Ch. Oct. 18, 2016) ("In applying the *Caremark* theory of liability, even in the face of alleged red flags, this Court has been careful to distinguish between failing to fulfill one's oversight obligations with respect to fraudulent or criminal conduct as opposed to monitoring the business risk of the enterprise.").

As the Court of Chancery explained, "[h]ere there is no credible allegation that the Company violated positive law." (Op. at 2.) Although the Court of Chancery's decision did not hinge on a finding that there was no alleged violation of positive law, it was nevertheless an important distinction separating this case from *Caremark*, *Marchand*, and *Boeing*. (*Id.*)

Plaintiffs contend that the SEC's guidance on cybersecurity-event disclosures, issued in February 2018, imposed a specific disclosure requirement for cybersecurity and thus constitutes positive law that SolarWinds violated. (Op. Br. at 9.) But this argument has two fatal flaws.

First, the SEC's guidance is not an affirmative disclosure obligation, but merely interpretative guidance meant to assist companies in making the decision of when and how to report material cybersecurity issues. *See Perez v. Mortg. Bankers Ass'n*, 575 U.S. 92, 97 (2015) (holding interpretive agency rules do not require notice-and-comment rulemaking, and "do not have the force and effect of law"). Plaintiffs do not—and could not—allege that SolarWinds failed to disclose the risk of cyberattacks or knowingly failed to report a material cyber breach.

Second, there is a vast conceptual difference between positive law such as food or airline safety regulations and the SEC's disclosure guidance—a difference that renders the SEC guidance largely irrelevant to the analysis here. The former mandates certain minimum actions an entity must take to limit the likelihood that a known, prospective risk will materialize. The latter, by contrast, constitutes only a recommendation that an entity *disclose* that a risk exists or that a material event has occurred in the past. Indeed, the SEC has proposed specific cybersecurity rules that create clear mandates, but these were proposed only after the SolarWinds incident, and are not even final now. *See* SEC, Proposed rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, March 9, 2022, *available at* https://www.sec.gov/rules/proposed/2022/33-11038.pdf. The SEC disclosure guidance does not impose any minimum duty to adopt particular cybersecurity risk-management practices.

Plaintiffs attempt to paint over this important distinction in a footnote. Citing no authority, they contend that "this distinction … means little." (Op. Br. at 45, n. 10.) Plaintiffs are wrong. The existence of specific legal violations in *Caremark* cases sets a floor against which courts may assess the actions of the Board. Directors act in bad faith when they do not institute oversight systems capable of reasonably assuring compliance with positive law. (*See* Op. at 2 (recognizing that "historically" *Caremark* claims have only been stated "in connection with the corporation's violation of positive law").)

Plaintiffs also argue that the settlement of a related securities class action and the existence of an SEC investigation is proof that SolarWinds violated the federal securities laws. (Op. at 45.) This is simply irrelevant. Neither a class action settlement nor the fact of an SEC investigation is evidence of a violation of the law, and in any event, as noted above, the federal securities laws do not currently mandate that companies implement specific cybersecurity measures. If accepted, Plaintiffs' argument would preclude the dismissal of any *Caremark* derivative claim where a related securities class action complaint survives a motion to dismiss or where there is a related SEC investigation.

Oversight of business risk is inherently a balancing act properly left to the board's judgment, so long as the board engages meaningfully in the consideration of those risks. (Op. at 2-3 ("[H]ow much effort to expend to prevent criminal activities

by third parties against the corporate interest requires an evaluation of business risk, the quintessential board function.").) As discussed in the next section, the Demand Board did just that.

b. The Demand Board's Thoughtful Engagement With SolarWinds' Cybersecurity Risk Shows Good Faith Balancing Of The Need For Oversight Of This Business Risk

Plaintiffs cannot deny that the Demand Board assigned responsibility for oversight of cybersecurity risk to the NCG and Audit Committees. (Op. at 8.) That fact alone distinguishes *Marchand*, where the Court noted specifically that no board committee had been tasked with oversight of food safety. *See Marchand*, 212 A.3d at 822. Instead, Plaintiffs quibble that the NCG Committee's oversight was insufficient because the Committee did not have additional cybersecurity briefings between the February 2019 briefing and the December 2020 discovery of the Sunburst attack, conveniently ignoring that the responsibilities for cybersecurity oversight were delegated across two committees, the second of which received a thorough briefing in April 2020. (*See* Op. Br. at 3.)

Plaintiffs attempt to spin the Court of Chancery's decision as having erroneously held that the SolarWinds Board satisfied its oversight responsibility merely through "nominal delegation" of oversight responsibility to the NCG and Audit Committees. (*See* Op. Br. at 25–36.) This is a gross mischaracterization of

the Court of Chancery's opinion and reasoning. The Court of Chancery correctly observed that "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." (Op. at 31.) But the Court never characterized oversight by the SolarWinds Board as "nominal." Instead, the Court of Chancery based its decision on the fact that the committees did carry out substantive oversight. (*Id*. at 31-32.)

Plaintiffs incorrectly contend that the oversight that was indisputably exercised by the Board Committees here was insufficient to constitute good faith. This argument ignores three important facts: the briefing the NCG Committee received [redacted] and the Audit Committee also received briefing on cybersecurity issues during the same period. And most importantly, the presentations [redacted]

First, the NCG Committee reviewed and considered [redacted] The 2019 briefing received by the NCG Committee was not perfunctory, ad hoc or one-sided. It described, *inter alia*, [redacted]

[redacted] (B76-83.)

The presentation also provided the NCG Committee with detailed information about [redacted] (B76-83.) Thus, although the briefing the NCG Committee received was not repeated during the timeframe cited by Plaintiffs, it covered all of the necessary topics for the members of the NCG Committee 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. *See Hamrock*, 2022 WL 2387653, at *16 (rejecting plaintiff's argument that an alleged "one time discussion" of safety risk was "too infrequent to meet the standard of *Marchand*" and noting instead that "this argument diverges too dramatically from the high 'utter failure' standard, even as understood through the refined lens of *Marchand* and *Boeing*").

Second, the briefing stated that [redacted] (B76-83.) This stands in stark contrast to the doomsday scenario painted by Plaintiffs, who state that the briefing "warned in striking language that cyberattacks were increasing, [and] that SolarWinds was a particularly attractive

target." (Op. Br. at 3.) But this ignores the reality of cybersecurity, in which incidents occur regularly, the variety of threats is nearly infinite, and a similarly unlimited number of additional security steps could be taken if cost and operations were not a concern.

What matters is that the NCG Committee was informed that [redacted] a point which Plaintiffs have not disputed. The materiality of incidents and threats is the key factor in measuring risk. If it were otherwise—if, for example, as Plaintiffs' arguments seem to suggest, some threshold number of *immaterial* issues could trigger a legal duty to respond—boards would be incentivized to limit discovery and reporting of such issues. That SolarWinds tracked a large number of incidents that were nevertheless immaterial to the Company's safety and operations, and that the Board Committee members knew the Company was taking this thorough approach, reflects positively on the robustness of the monitoring systems both the Company and the Board had in place during the relevant period.

Here, in particular, Plaintiffs have not alleged—because they cannot—that [redacted] Such an argument would be preposterous, given the completely novel and unpredictable nature of that sophisticated operation by Russian government hackers.

Third and finally, Plaintiffs ignore the fact that the NCG Committee briefing was not the Board's only exercise of oversight. Highlighting the importance with which the Board regarded cybersecurity, the Board delegated additional responsibility for cybersecurity oversight to the Audit Committee, which received a briefing on [redacted] (B110.) Plaintiffs attempt to sweep this presentation under the rug because it was not produced until after they filed their Complaint. However, Plaintiffs received production of this document in advance of the motion-to-dismiss briefing to the trial court, and thus cannot point to any harm or prejudice that resulted from the supplemental production.

Although the Court need not rely on this presentation in order to conclude that the Demand Board exercised good faith, it is further proof of the Board's significant and ongoing oversight of cybersecurity. However, even if the Court were to disregard management's cybersecurity briefing to the Audit Committee and assumes that the Audit Committee failed to carry out its duty to oversee SolarWinds' cybersecurity risks, Plaintiffs would still fall short of their burden to establish that a majority of the Demand Board faced a risk of liability under *Caremark.* There are eleven directors on the Demand Board. Only three directors (Messrs. Brock, Sundaram, and Ms. Kinney) served on the Audit Committee in April 2020. (A38 ¶

21; A41 ¶ 27; A42 ¶ 29.) And, as noted, the NCG Committee also monitored cyber risks during the relevant period.

Indeed, the NCG Committee also continued to monitor cybersecurity after the February 2019 briefing. As Plaintiffs argued below, "the NGC [sic] appears to have recognized the imperative to follow up on the February 2019 Cybersecurity Briefing by attempting to schedule [redacted] (A232 (citing A71 ¶ 74).) Plaintiffs contend that the absence of documents in the 220 Production indicating [redacted] demonstrates that the NCG Committee was asleep at the wheel and willfully ignored its oversight obligations. (*Id*.) But such an inference is unreasonable and unwarranted. The fact that the NCG Committee [redacted] demonstrates that the Committee understood its oversight obligations and directed management to update the committee on material cybersecurity developments. 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. Plaintiffs cite no material cybersecurity incident at SolarWinds between the February 2019 Briefing and the Sunburst cyberattack in December 2020—the use of one insecure password for one third-party server that did not result in corporate harm was neither material nor alleged to have been reported at a board level.

c. The SolarWinds Board's Oversight Of Cybersecurity Risks Stands In Sharp Contrast To The Oversight Failures At Issue In *Caremark*, *Marchand*, And *Boeing*

Plaintiffs cite several cases where *Caremark* claims survived a motion to dismiss in support of their argument that the Demand Board faces a "substantial likelihood" of liability under the first prong of *Caremark.* However, each of these cases is easily distinguishable because all involved a complete lack of Board-level oversight of legal compliance.

Beginning with *Caremark* itself, first-prong liability has always been premised on an "utter failure to attempt to assure a reasonable information and reporting system exists." *Caremark*, 698 A.2d at 971.

Marchand did not change that standard. In *Marchand,* Blue Bell Creameries "had no board committee charged with monitoring food safety." 212 A.3d at 813. Thus, Blue Bell's board "never received any information about *listeria*," or the prior outbreaks of *listeria* and multiple regulatory violations found by the FDA that would have put the board on notice of major food safety risks. *Id.* at 812. In the years leading up to the *listeria* outbreak in early 2015 that killed 8 people in two different states, there were 8 inspections by the FDA or state health department officials that noted issues with condensation, dirty facilities, open containers of ingredients, violations of food safety regulations, among other serious regulatory violations. *Id.*

at 811–12, 814. In 2014, the year before the deadly outbreak, there were 10 positive tests for listeria. *Id.* at 812. In February 2015 alone, there were at least 3 notifications of positive tests for *listeria* in Blue Bell samples. *Id.* at 813.

As the Court noted, there was "no effort at all to implement a board-level system of mandatory reporting of any kind." *Id.* at 813. The Court noted that Blue Bell was a "monoline" company producing only ice cream, and thus food safety was especially critical to its success. *Id*. at 809. Contrary to Plaintiffs' assertion, SolarWinds is not a monoline company—it produces a wide variety of software products, of which Orion (the software targeted in the Sunburst attack) is only one. (*See* Op. at 5.)

In *Marchand*, the Board had failed to carry out its obligations in good faith because it "had no committee overseeing food safety, no full board-level process to address food safety issues, and no protocol by which the board was expected to be advised of food safety reports and developments." *Marchand*, 212 A.3d at 809. Likewise, in *Boeing*, the court denied defendants' motion to dismiss because "[n]one of Boeing's Board committees were specifically tasked with overseeing airplane safety, and every committee charter was silent as to airplane safety" and because "the board [didn't] have any tools to oversee safety." *Boeing*, 2021 WL 4059934, at *5. This was so, despite that from 2000 to 2020, "the FAA flagged twenty airplane safety violations for poor quality control, poor maintenance, and noncompliant parts,

as well as the Company's failure to provide its airline clients with crucial safety information." *Id*. at *4. These led to fines of up to $13 million. *Id.*

Boeing also had "thirteen separate pending or potential civil enforcement cases relating to quality control, safety protocol violations, and manufacturing errors in production lines" that culminated in an "unprecedented settlement with the FAA" in 2015 whereby Boeing "agreed to pay historic fines of $12 million, with up to $24 million in additional fines deferred" pending an improvement in regulatory compliance. *Id.*

Then there were the crashes. In July 2013, "one of Boeing's 777 airplanes crashed, killing three and seriously injuring dozens." *Id.* On October 29, 2018, a Boeing 737 MAX crashed, killing all 189 people on board. *Id.* at *12. But Boeing's board failed to investigate the crash or implement any meaningful oversight of the company's regulatory compliance. The result was that the same faulty sensor that caused the prior, uninvestigated crash later resulted in a crash that killed 157 people. *Id.* at *16.

Here, Plaintiffs affirmatively allege that two committees were designated to jointly oversee cybersecurity (*see* A34-35 ¶¶ 9–10) and the briefings to those committees are evidence of a "protocol by which the board" would be advised of cybersecurity concerns (B61-89 & B108-110).

This case is also distinguishable from *Boeing* because in that case, reports from management were *ad hoc* and one-sided, made only in response to specific safety incidents, and did not provide a comprehensive risk overview to the board, instead only offering "favorable" information. 2021 WL 4059934, at *29. As Plaintiffs themselves note, the February 2019 presentation to the NCG Committee included [redacted] (Op. Br. at 38.) It was not "one-sided"—rather, it [redacted] This is a far cry from the sugarcoated reports that *Boeing*'s management gave its board. *See Boeing*, 2021 WL 4059934, at *29. Similarly, the 2020 presentation to the Audit Committee apprised the committee [redacted]

Plaintiffs argue that the delegation of oversight to a committee is not enough, suggesting that the *entire Board* must provide oversight. In support of this proposition, Plaintiffs cite *Hughes v. Xiaoming Hu*, where the Court denied a defendants' motion to dismiss because plaintiffs adequately alleged that the Board failed to put in place a system of oversight for their company's financial reports. 2020 WL 1987029, at *2 (Del. Ch. Apr. 27, 2020). But in *Hughes*, the Court's reasoning centered around a complete failure of the Board to serve as anything

beyond a rubber stamp for the company's management. *Id*. at *14 (also finding that the audit committee "had clear notice of irregularities" in company accounting). Indeed, in that case the Audit Committee met only perfunctorily, and certainly did not receive detailed briefings as in this case. Here, Plaintiffs may quibble with the frequency of oversight meetings but, as the Court of Chancery correctly held, Plaintiffs have not come close to alleging that the SolarWinds Board or either of its two Committees were shams, as was the finding in *Hughes*.

Instead, this case is much more like *Hamrock*, where the court granted defendants' motion to dismiss plaintiff's *Caremark* claim because "the plaintiff's own allegations, however, demonstrate that the [defendant's] board of directors did establish a system for monitoring and reporting on pipeline safety issues" that "included a committee tasked with overseeing safety issues." *Hamrock*, 2022 WL 2387653, at *1. As in *Hamrock*, the facts here establish that there were two Board Committees tasked with cybersecurity risk management that both received cybersecurity briefings during the relevant time.

This case is also very similar to *Sorenson*, in which the court granted defendants' motion to dismiss plaintiff's *Caremark* claim against directors of Marriott. *Sorenson*, 2021 WL 4593777, at *12. There, plaintiffs alleged that the Marriott board had failed to implement a system of oversight related to cybersecurity risk. *Id*. In dismissing the claim, the court stated, *inter alia*, that "the plaintiff has

not shown that the directors completely failed to undertake their oversight responsibilities." *Id*. at *1. As the court explained, the extent of a Board's involvement in managing cybersecurity risk is a decision of "disinterested business judgment" and "directors have great discretion to design context- and industry-specific approaches tailored to their companies' businesses and resources." *Id*. at *12 (internal citations and quotations omitted). Thus, where, as here, a Board puts in place "any system of controls," it has fulfilled its obligations under *Caremark*'s first prong. *Id*. Consequently, the record in this case firmly establishes that the Demand Board faces no substantial likelihood of personal responsibility for failure to implement a system of controls over cybersecurity.

2. Plaintiffs Have Failed To Allege That A Majority Of The Demand Board Faces A Substantial Likelihood Of Liability Under *Caremark*'s Second Prong For Ignoring Cybersecurity "Red Flags"

Plaintiffs argue in the alternative that the Court of Chancery erred in ruling that Plaintiffs failed to adequately plead that a majority of the Demand Board ignored cybersecurity "red flags" to allege liability under *Caremark*'s second prong. The Court of Chancery's holding on this issue was both legally and factually correct and should be affirmed. (*See* Op. at 26–28.)

Caremark's second prong requires Plaintiffs to plead that the directors consciously failed to monitor or oversee the company's operations by disregarding "red flags" and had culpable knowledge that they were not discharging their fiduciary obligations—*i.e.*, they acted in bad faith and with scienter. *See Stone*, 911 A.2d at 370. The Court of Chancery correctly held that Plaintiffs' Complaint failed to meet this standard. None of these "red flag" allegations show bad faith or scienter by the Board, because Plaintiffs do not allege that the Board received information that would have put the directors on notice of the risk of the Sunburst attack.

Plaintiffs point to the following "red flag" allegations to satisfy *Caremark*'s second prong: (1) the "Solarwinds123" password assigned to a single server that was maintained by a third-party; (2) the Thornton-Trump PowerPoint presentation; and (3) the February 2019 cybersecurity briefing. (Op. Br. at 36–43.) None of these allegations are sufficient to allege that a majority of the Demand Board faces a substantial likelihood of liability.

First, Plaintiffs reference a November 11, 2019 e-mail to a SolarWinds employee disclosing the existence of an insecure password ("Solarwinds123") for a third-party test download server used by SolarWinds, and argue that it was a red flag of potential cybersecurity deficiencies. But nowhere in the Complaint do Plaintiffs allege that any director was made aware of this issue, or that any member of management even knew about the weak password at the time of the February 2019

cybersecurity briefing—a briefing that occurred months before the password issue was brought to anyone's attention at SolarWinds.

That is why the Court of Chancery correctly rejected the argument that these allegations satisfy *Caremark*'s second prong: "Without such knowledge, the Board … cannot have acted in bad faith relating to this incident." (Op. at 28.) Plaintiffs cite no authority that would lead to a contrary conclusion, and this Court should affirm the Court of Chancery's ruling on this point. *See Reiter*, 2016 WL 6081823, at *8 (explaining that a *Caremark* red-flag theory of liability depends on allegations that "the board *knew of* evidence of corporate misconduct") (emphasis added). To take this argument to its logical conclusion, if directors were required to be alerted to every employee's use of a weak password, directors would have little time to focus on much else.

Moreover, there is no indication that the "Solarwinds123" password resulted in any corporate harm, much less that it had any connection to the Sunburst attack. The use of this password does not implicate any systemic or internal controls issue—instead, it is an example of a single user's erroneous use of a weak password. Plaintiffs do not allege that the Sunburst hackers even exploited that password to access the Orion platform—nor could they, as the password was used on a server for third-party downloads, an IT process wholly unrelated to Orion. Thus, even if, for the sake of argument, the directors should have been aware of a single user's weak

password, it is still irrelevant to Plaintiffs' burden to show bad faith under the second prong of *Caremark* because the password issue was not a "red flag" of any cybersecurity deficiency implicated by the Sunburst attack. *See Melbourne Mun. Firefighters' Pension Tr. Fund v. Jacobs*, 2016 Del. Ch. LEXIS 114, at *22 (Del. Ch. Aug. 1, 2016) (explaining that a "subsequent complained-of corporate trauma … must be sufficiently similar to the misconduct implied by the red flags such that the board's bad faith, conscious inaction proximately caused that trauma") (cleaned up); *see also Oklahoma Firefighters Pension & Ret. Sys. v. Corbat*, 2017 WL 6452240, at *19 (Del. Ch. Dec. 18, 2017) (refusing to excuse a demand where the alleged red flag incidents did not put the directors "on notice of what eventually happened").

The Court should also reject Plaintiffs' arguments regarding the Thornton-Trump "Creating Security" PowerPoint presentation in April 2017 for the same reasons. Plaintiffs dramatically oversell the import of Thornton-Trump's "Creating Security" presentation. This presentation did not "blow the whistle" on SolarWinds' "lack of security" as Plaintiffs contend. (Op. Br. at 2.) The presentation was primarily a marketing piece that proposed that SolarWinds change its brand from a company that sells IT monitoring solutions to a company that sells security software. Thornton-Trump stressed in the presentation that the cybersecurity software market reached $75 Billion in 2015 and was "expected to reach $170 Billion by 2020."

(B117.) While the presentation proposes that SolarWinds "live within the security brand" and improve the internal commitment to security, it does not identify any specific cybersecurity deficiency or vulnerability.

And moreover, as the Court of Chancery explained, "there is no pleading that the Board was aware" of the presentation, which was made to "technology and marketing executives" before SolarWinds became a public company—and thus before the Board was appointed. (Op. at 27; *see also* A86 ¶ 97.) And while Thornton-Trump allegedly relayed his concerns to SolarWinds' Chief Marketing Officer, there is no allegation that the officer communicated this fact to any director. (A86 ¶ 97.) This presentation fails to support any claim of bad faith because Plaintiffs have not alleged that it was brought to the Board's attention during the relevant time period, and the Board cannot have acted in bad faith with respect to facts of which it was unaware.

There is also no allegation or evidence that any of the issues raised in the report were later connected to the Sunburst attack, or that the report identified any specific cybersecurity deficiencies that otherwise could have alerted the Board to an impending attack. Instead, the report contains a few high-level, generalized criticisms, such as a supposed "lack of security at the technical product level" and "minimal security leadership." (A86 ¶ 97.) Indeed, the main critique of the Thornton-Trump presentation was that the Company should appoint a senior director

of cybersecurity that reports directly to the CIO, which SolarWinds did two months later when it hired Tim Brown, the former head of information security at Dell Computer. (B113.) Thus, the information in the presentation is not sufficient to state a *Caremark* claim. *See Hamrock*, 2022 WL 2387653, at *25 ("General risks are not 'red flags' of a specific corporate trauma.").

And, finally, the Court of Chancery was correct that the 2019 cybersecurity presentation to the NCG Committee "is not a red flag or a fact supportive of bad faith or scienter" but was "in fact, an instance of oversight." (Op. at 27.) As previously discussed, although the presentation provided [redacted] (B61-89.) More importantly, the briefing [redacted]

The absence of any material cybersecurity breach at SolarWinds prior to the Sunburst attack is a critical distinction between this case and instances where Delaware courts have held that directors ignored red flags in bad faith. In *Boeing*, for example, the court identified a prior crash involving Boeing's 737 MAX aircraft that killed 189 people as a red flag of safety issues that the Board declined to

investigate. *Id.* at *33–34. The first crash (the Lion Air crash) and the second crash (the Ethiopian Airlines crash) were both caused by the same faulty sensor, and it was that connection that prompted the derivative litigation. *Id.* at *34. Plaintiffs offer no analogous allegations here. The Complaint makes no connection between any prior cybersecurity incident at SolarWinds and the Sunburst attack, and therefore Plaintiffs have failed to state a *Caremark* claim on this basis.

The cybersecurity briefing [redacted] This was, as the Court of Chancery found, an instance of oversight by the Board. (Op. at 27.) Plaintiffs' repeated references to the [redacted] language in the PowerPoint presentation do not change this analysis. That SolarWinds' management [redacted] does not give rise to a *Caremark* claim.

That was the holding of *Sorenson*—a case on all fours with the facts alleged here by Plaintiffs. *See* 2021 WL 4593777, at *1. Like the instant litigation, *Sorenson* involved a significant cybersecurity incident. *Id.* at *1. The plaintiffs alleged that Marriott's Board of Directors ignored red flags about the data protection systems of Starwood, a hotel chain Marriott had recently acquired. *Id.* The "so-called 'red flags'" in *Sorenson* are similar to plaintiff's allegations here—namely "updates to

the Board about aspects of Starwood's cybersecurity measures that needed improvement." *Id.* at *15. And, like in the presentation to the NCG Committee, Marriott's management "told the Board that it was addressing or would address the issues presented." *Id.* at *16. On these facts, the court held that there was no *Caremark* claim: "These facts are not reflective of a board that has decided to turn a blind eye to potential corporate wrongdoing." *Id.*

The facts of *Sorenson* and this case clearly contrast with the facts of *Boeing* and other cases where Delaware courts have ruled that plaintiffs sufficiently alleged bad faith based on directors' disregard of red flags. Those cases involve situations where directors had notice of specific prior instances of corporate wrongdoing or lack of compliance that foreshadowed a subsequent corporate trauma and failed to take any action. *See, e.g.*, *Teamsters Loc. 443 Health Servs. & Ins. Plan v. Chou*, 2020 WL 5028065, at *20 (Del. Ch. Aug. 24, 2020) (denying a motion to dismiss a red-flag *Caremark* claim where the plaintiffs adequately pleaded that the directors were "on notice" of "shortcomings" with respect to "critical drug health and safety regulations" and "did not respond to the potential gaps regarding drug health and safety risks"); *In re Clovis Oncology, Inc. Derivative Litig.*, 2019 WL 4850188, at *13–16 (Del. Ch. Oct. 1, 2019) (denying a motion to dismiss a claim brought under *Caremark*'s second prong where the plaintiffs alleged that directors were aware of a failure to comply with FDA regulations for clinical trials of the company's "mission

critical product" but took no action to ensure regulatory compliance).

In contrast, Delaware courts have rejected *Caremark* claims where management flagged potential areas of risk for directors and identified concrete steps the company was taking or would take to minimize the likelihood that those risks would materialize, absent any evidence that those risks had already manifested in the form of specific incidents similar to the subsequent corporate trauma. *See, e.g.*, *Corbat*, 2017 WL 6452240, at *20 (finding no bad faith where management informed the board that it was taking specific actions to address potential risk areas following reports of red flags of activity unrelated to the corporate trauma that prompted the derivative litigation).

Here, the unprecedented nature of the Sunburst attack raises an already high pleading bar even further. There is no dispute, even from Plaintiffs, that the Sunburst attack was highly sophisticated, novel, and conducted by a determined foreign actor with unlimited time and resources. Plaintiffs have not alleged that the Board received specific warnings of a scenario like Sunburst and consciously disregarded the risk of a likely attack. While there is reference to general warnings about threats from nation state actors and cyber criminals, there are no allegations that the Board knew of, and ignored, red flags indicating that SolarWinds would be the target of a black swan event like Sunburst.

CONCLUSION

For the foregoing reasons, Defendants-Below/Appellees respectfully request that the decisions of the Court of Chancery be affirmed.

DATED: January 19, 2023

OF COUNSEL:

Paul R. Bessette
Michael J. Biles
Tyler W. Highful
KING & SPALDING LLP
500 W. 2nd Street, Suite 1800
Austin, TX 78701

Benjamin Lee
Benjamin B. Watson
KING & SPALDING LLP
1180 Peachtree Street, NE
Atlanta, GA 30309

DLA PIPER LLP (US)

/s/ John L. Reed
John L. Reed (I.D. No. 3023)
Ronald N. Brown, III (I.D. No. 4831)
Peter H. Kyle (I.D. No. 5918)
Kelly L. Freund (I.D. No. 6280)
1201 North Market Street, Suite 2100
Wilmington, DE 19801
(302) 468-5700
john.reed@dlapiper.com
ronald.brown@dlapiper.com
peter.kyle@dlapiper.com
kelly.freund@dlapiper.com

Attorneys for Nominal Defendant-Below/Appellee SolarWinds Corporation

RICHARDS, LAYTON & FINGER, P.A.

/s/ Raymond J. DiCamillo
Raymond J. DiCamillo (#3188)
Kevin M. Gallagher (#5337)
Alexander M. Krischik (#6233)
Christian C. F. Roberts (#6694)
920 North King Street
Wilmington, Delaware 19801
(302) 651-7700

OF COUNSEL:

Sandra C. Goldstein, P.C.
Stefan Atkinson, P.C.
Byron Pacheco
KIRKLAND & ELLIS LLP
601 Lexington Avenue
New York, New York 10022
(212) 728-8000

Attorneys for Defendants-Below/Appellees William Bock, Seth Boro, Paul J. Cormier, Michael Hoffman, Dennis Howard, Catherine R. Kinney, James Lines, and Easwaran Sundaram

OF COUNSEL:

Sameer Advani
Wesley R. Powell
Patricia O. Haynes
WILLKIE FARR & GALLAGHER LLP
787 Seventh Avenue
New York, New York 10019
(212) 728-8000

MORRIS NICHOLS ARSHT & TUNNELL LLP

/s/ William M. Lafferty
William M. Lafferty (#2755)
Ryan D. Stottmann (#5237)
Alexandra M. Cumings (#6146)
1201 North Market Street
Wilmington, Delaware 19801
(302) 658-9200

Attorneys for Defendants-Below/Appellees Mike Bingle, Kenneth Hao, Jason White, and Michael Widmann

ABRAMS & BAYLISS LLP

OF COUNSEL:

/s/ Stephen C. Childs
Stephen C. Childs (#6711)
20 Montchanin Road, Suite 200
Wilmington, DE 19807
(302) 778-1150
childs@abramsbayliss.com

Peter L. Welsh
C. Thomas Brown
Patrick T. Roath
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
(617) 951-7865

Edward R. McNicholas
ROPES & GRAY LLP
2099 Pennsylvania Avenue, N.W.
Washington, DC 20006
(202) 508-4600

Counsel for Defendant-Below/ Appellee Kevin B. Thompson

CERTIFICATE OF SERVICE

I, John L. Reed, hereby certify that on this 8th day of February, 2023, I caused true and correct copies of the foregoing REDACTED PUBLIC VERSION of **APPELLEES' ANSWERING BRIEF** to be served upon the foregoing counsel of record in the manner indicated:

VIA FILE & SERVE*XPRESS*

Raymond J. DiCamillo
Kevin M. Gallagher
Alexander M. Krischik
Christian C. F. Roberts
RICHARDS, LAYTON & FINGER, P.A.
920 North King Street
Wilmington, DE 19801

William M. Lafferty
Ryan D. Stottmann
Alexandra M. Cumings
MORRIS NICHOLS ARSHT & TUNNELL LLP
1201 N. Market Street
Wilmington, DE 19899

Thomas Curry
SAXENA WHITE, P.A.
1000 North West Street, Suite 1200
Wilmington, DE 19801

A. Thompson Bayliss
Stephen C. Childs
ABRAMS & BAYLISS LLP
20 Montchanin Road
Wilmington, DE 19807

Michael J. Barry
Vivek Upadhya
GRANT & EISENHOFER P.A.
123 Justison Street, 7th Floor
Wilmington, DE 19801

/s/ John L. Reed
John L. Reed (I.D. No. 3023)