EFiled: Oct 06 2021 04:11AM EDT
Transaction ID 66992145
Case No. 2019-0965-LWW

IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

FIREMEN'S RETIREMENT SYSTEM OF ST. LOUIS, derivatively on behalf of Marriott International, Inc.,	)	
Plaintiff,	)	
v.	)	C.A. No. 2019-0965-LWW
ARNE M. SORENSON, J.W. MARRIOTT, JR., KATHLEEN K. OBERG, DEBORAH MARRIOTT HARRISON, BAO GIANG VAL BAUDUIN, BRUCE HOFFMEISTER, STEPHANIE C. LINNARTZ, ERIC HIPPEAU, LAWRENCE W. KELLNER, GEORGE MUÑOZ, MARY K. BUSH, DEBRA L. LEE, FREDERICK A. HENDERSON, AYLWIN B. LEWIS, BRUCE W. DUNCAN, W. MITT ROMNEY, STEVEN S. REINEMUND, and SUSAN C. SCHWAB,	)	
Defendants,	)	
and	)	
MARRIOTT INTERNATIONAL, INC., a Delaware Corporation,	)	
Nominal Defendant.	)	

MEMORANDUM OPINION

Date Submitted: July 7, 2021
Date Decided: October 5, 2021

Samuel L. Closic and Eric Juray, PRICKETT, JONES & ELLIOTT, P.A., Wilmington, Delaware; Brian J. Robbins, Craig W. Smith, Gregory E. Del Gaizo, and Emily R. Bishop, ROBBINS LLP, San Diego, California; *Counsel for Plaintiff Firemen's Retirement System of St. Louis*

Raymond J. DiCamillo and John M. O'Toole, RICHARDS, LAYTON & FINGER, P.A., Wilmington, Delaware; Jason J. Mendro and Jeffrey S. Rosenberg, GIBSON, DUNN & CRUTCHER LLP, Washington, D.C.; Adam H. Offenhartz and Laura Kathryn O'Boyle, GIBSON, DUNN & CRUTCHER LLP, New York, New York; *Counsel for Defendants Arne M. Sorenson, J.W. Marriott, Jr., Kathleen K. Oberg, Deborah Marriott Harrison, Bao Giang Val Bauduin, Bruce Hoffmeister, Stephanie C. Linnartz, Eric Hippeau, Lawrence W. Kellner, George Muñoz, Mary K. Bush, Debra L. Lee, Frederick A. Henderson, Aylwin B. Lewis, Bruce W. Duncan, W. Mitt Romney, Steven S. Reinemund, and Susan C. Schwab, and Nominal Defendant Marriott International, Inc.*

WILL, Vice Chancellor

In the fall of 2018, Marriott International, Inc. discovered a data security breach that had exposed the personal information of up to 500 million guests. An investigation revealed that the cyberattack was perpetrated through the reservation database of Starwood Hotels and Resorts—which Marriott had acquired two years prior—and had begun in 2014. Marriott publicly announced the incident on November 30, 2018. A series of stockholder and consumer actions followed.

The stockholder plaintiff in this action brought a derivative lawsuit against several key executives and Marriott's directors for breaches of fiduciary duty. The plaintiff's claims are based on the defendants' conduct both before and after the acquisition of Starwood. Regarding the pre-acquisition time period, the plaintiff alleges that the defendants breached their fiduciary duties by failing to conduct adequate due diligence of Starwood's cybersecurity technology. Regarding the post-acquisition period, the plaintiff alleges that the defendants continued to operate Starwood's deficient systems, failed to timely disclose the data breach, and that the directors breached their duty of loyalty under *Caremark*. The defendants have moved to dismiss the complaint for failure to plead demand futility.

In this decision, I conclude that demand was not excused because none of the director defendants faces a substantial likelihood of liability on a non-exculpated claim. First, the plaintiff's claims regarding pre-acquisition due diligence are time

barred. They arose more than three years before the plaintiff's complaint was filed and no basis for tolling applies. Second, none of the directors face a substantial likelihood of liability under *Caremark*. Cybersecurity has increasingly become a central compliance risk deserving of board level monitoring at companies across sectors. But the allegations in the complaint do not meet the high bar required to state a *Caremark* claim. The plaintiff has not shown that the directors completely failed to undertake their oversight responsibilities, turned a blind eye to known compliance violations, or consciously failed to remediate cybersecurity failures. Finally, the plaintiff's claim based on unmet notification requirements is also unsupported by allegations of bad faith.

The Marriott board therefore retained its ability to assess whether to pursue litigation on behalf of the company. Demand is not excused. The motion to dismiss is granted pursuant to Court of Chancery Rule 23.1.

I. BACKGROUND

Unless otherwise noted, the following facts are drawn from the Amended Verified Stockholder Derivative Complaint and the documents it incorporates by

reference.[1] Any additional facts are either not subject to reasonable dispute or are subject to judicial notice.[2]

A. The Starwood Acquisition

Nominal defendant Marriott International, Inc. (the "Company") is a Delaware corporation headquartered in Bethesda, Maryland.[3] Founded in 1927, Marriott is one of the largest hospitality companies in the world.[4] Marriott operates,

---

[1] Verified Am. Deriv. Compl. ("Am. Compl.") (Dkt. 33). *See Winshall v. Viacom Int'l, Inc.*, 76 A.3d 808, 818 (Del. 2013) ("[A] plaintiff may not reference certain documents outside the complaint and at the same time prevent the court from considering those documents' actual terms." (quoting *Fletcher Int'l, Ltd. v. ION Geophysical Corp.*, 2011 WL 1167088, at *3 n.17 (Del. Ch. Mar. 29, 2011))); *Freedman v. Adams*, 2012 WL 1345638, at *5 (Del. Ch. Mar. 30, 2012) ("When a plaintiff expressly refers to and heavily relies upon documents in her complaint, these documents are considered to be incorporated by reference into the complaint . . . ."). The parties agreed that documents produced by Marriott pursuant to 8 *Del. C.* § 220 would be deemed incorporated into any complaint the plaintiff filed. *See* Defs.' Opening Br. 8 n.2 (Dkt. 40); *Amalgamated Bank v. Yahoo! Inc.*, 132 A.3d 752, 797 (Del. Ch. 2016). Citations in the form "Defs.' Ex. __" refer to exhibits to the Transmittal Declaration of John M. O'Toole, Esq. in Support of Defendants' Opening Brief in Support of their Motion to Dismiss the Verified Amended Stockholder Derivative Complaint (Dkt. 41, 66). Page numbers to these exhibits are designated by the last four digits of a Bates number, where appropriate.

[2] *See, e.g.*, *In re Books–A–Million, Inc. S'holders Litig.*, 2016 WL 5874974, at *1 (Del. Ch. Oct. 10, 2016) ("This court may consider the Proxy Statement to establish what was disclosed to stockholders and other facts that are not subject to reasonable dispute." (citing *In re Gen. Motors (Hughes) S'holder Litig.*, 897 A.2d 162, 170 (Del. 2006)); *Lima Delta Co. v. Glob. Aerospace, Inc.*, 2017 WL 4461423, at *4 (Del. Super. Oct. 5, 2017) (explaining that dockets, pleadings, and transcripts from a foreign action are subject to judicial notice).

[3] Am. Compl. ¶ 19.

[4] *Id.* ¶ 49.

manages, and franchises a broad portfolio of over 6,900 hotels and lodging facilities.[5]

On November 16, 2015, Marriott announced its intent to acquire Starwood Hotels and Resorts Worldwide, Inc. (the "Acquisition"), a hotel and leisure company whose brands included W Hotels, St. Regis, and Le Meridien.[6] At that time, Starwood had more than 1,270 properties providing approximately 360,000 rooms in 100 countries.[7] Marriott and Starwood would together create a more globally diversified company operating or franchising more than 5,500 hotels and 1.1 million rooms worldwide.[8]

In discussing the Acquisition, Marriott's then-President and Chief Executive Officer, Arne M. Sorenson,[9] described Starwood's guest loyalty program, Starwood Preferred Guest, as the "central, strategic rationale for the transaction" and the "most important piece of the [A]cquisition."[10] Starwood Preferred Guest had a devoted

---

[5] *Id.* ¶¶ 19, 69.

[6] *Id.* ¶¶ 1, 104.

[7] Defs.' Ex. 29 at 8.

[8] *Id.* at 97.

[9] On February 16, 2021, Marriott announced that Sorenson passed away on February 15, 2021. Marriott International, Inc. (Form 8-K) (Feb. 16, 2021). Sorenson had served as Marriott's President from May 2009 and Chief Executive Officer from May 2012 until his passing. Am. Compl. ¶ 20.

[10] *Id.* ¶ 78.

following of business travelers. Acquiring the program would expand Marriott's client base, increase its brand loyalty, and enhance the Company's ability to compete in an evolving global marketplace.[11]

B. Marriott's Due Diligence and Starwood's Data Security

Eleven months of due diligence commenced in late 2015, with ten months passing between the signing of the Agreement and Plan of Acquisition on November 15, 2015 and closing on September 23, 2016.[12] During that time, the Company, and Sorenson in particular, publicly touted Marriott's "extensive" diligence into Starwood and "joint integration planning" efforts.[13]

In the midst of the Company's diligence of Starwood, Marriott's Board of Directors ranked cybersecurity as the number one risk facing Marriott in 2016.[14] The Board at that time consisted of 11 members: defendants Sorenson, J.W. Marriott, Jr. (the Company's Executive Chairman and Chairman of the Board), Deborah Marriott Harrison (the Company's Global Cultural Ambassador Emeritus), Lawrence W. Kellner, George Muñoz, Mary K. Bush, Debra L. Lee, Frederick A. Henderson, Steven S. Reinemund, Susan C. Schwab, and W. Mitt Romney (together,

---

[11] *Id.* ¶¶ 75, 81; Defs.' Ex. 29 at 97.

[12] Am. Compl. ¶¶ 87, 109.

[13] *Id.* ¶¶ 179-81.

[14] *Id.* ¶ 100.

the "Pre-Acquisition Board").[15] Despite knowing that cybersecurity was a pervasive risk in the hospitality industry that could affect Marriott's ability to achieve its goals,[16] the Pre-Acquisition Board did not order any specific due diligence into cybersecurity in connection with the planned Acquisition.[17]

On November 20, 2015—five days after Marriott and Starwood signed the merger agreement—Starwood disclosed that the point-of-sale systems at 54 of its hotels in North America had been infected by malware.[18] Several months later, an internal Marriott report summarizing the costs of integrating the Marriott Guest Loyalty and Starwood Preferred Guest databases noted that Starwood's systems lacked certain protections such as tokenization—the process of replacing sensitive data with unique identification symbols—and point-to-point encryption across its point-of-sale systems.[19] None of this information reached the Board before the Acquisition closed.

---

[15] *Id.* ¶¶ 20-21, 23, 28-32, 35-37.

[16] *Id.* ¶ 100.

[17] *Id.* ¶ 5.

[18] *Id.* ¶¶ 79, 88.

[19] *Id.*; *see* Kevin Batchelor, *What is Tokenization, and Why Is It So Important?*, Forbes (Apr. 19, 2019).

C. Starwood's Information Security Systems Post-Closing

Cybersecurity remained a "top level risk[]" for Marriott after the $13 billion Acquisition of Starwood closed on September 23, 2016.[20] Cybersecurity was viewed by the Board as the second biggest risk facing Marriott for fiscal year 2017.[21] By then, Marriott's data systems included Starwood's legacy systems, some of which remained in use post-Acquisition.[22]

The Board and Audit Committee were routinely apprised of cybersecurity issues after the Acquisition.[23] On February 8, 2017, for example, the Audit Committee—comprised of director defendants Henderson, Bush, Aylwin B. Lewis, and Muñoz—was told by Marriott's independent auditor Ernst & Young that audit committees were "expected to have an understanding of the business implications of cyber risks."[24] Internal Audit and Chief Audit Executive Keri Day also told the Audit Committee that Marriott had "established a Security Operations Center (SOC), an Incident Response (IR) plan, and related procedures" because its "incident

[20] Am. Compl. ¶¶ 76, 121.

[21] *Id.* ¶ 121.

[22] *Id.* ¶¶ 126-27.

[23] *Id.* ¶ 118.

[24] *Id.* ¶ 118; Defs.' Ex. 12 at 1238, 1240.

response plan [wa]s not up to date."[25] Day further reported that "[t]he Company [wa]s actively evaluating Starwood's exposures to cybersecurity risks."[26]

At a regularly scheduled meeting on February 10, 2017, the Marriott Board—which now included former Starwood directors Bruce W. Duncan, Eric Hippeau, and Lewis (together with the Pre-Acquisition Board members, the "Post-Acquisition Board")—was allegedly told for the first time about deficiencies in Starwood's cybersecurity controls.[27] During the February 10, 2017 meeting, defendant Bruce Hoffmeister, Marriott's Global Chief Information Officer, gave a presentation titled "Marriott Cybersecurity Report" to the full Post-Acquisition Board.[28] Hoffmeister discussed various steps that Marriott had taken to protect against data breaches, including the engagement of a "specialized security company" to manage its "Security Operations Center."[29] The "primary" step Marriott had taken to protect its own systems was tokenization.[30]

Hoffmeister told the Board that a review of Starwood's legacy data systems "revealed that, while there was a vibrant framework, tokenization was not adopted

---

[25] Am. Compl. ¶ 119; Defs.' Ex. 11 at 1118.

[26] Am. Compl. ¶ 118; Defs.' Ex. 11 at 1067.

[27] Am. Compl. ¶¶ 123-24.

[28] *Id.* ¶ 122; Defs.' Ex. 14 at 1279.

[29] Defs.' Ex. 14 at 1282.

[30] Am. Compl. ¶ 126; Defs.' Ex. 13 at 1249.

as a matter of course."[31] He described early findings by PricewaterhouseCoopers ("PwC"), which Marriott had hired post-Acquisition to conduct a "Starwood Security Program Assessment."[32] Hoffmeister's presentation explained that, in addition to not mandating tokenization, Starwood's "[b]rand standards did not mandate [payment card industry ('PCI')] compliance . . . or point-to-point encryption."[33] The Payment Card Industry Data Security Standard ("PCI DSS") is a set of security standards required by credit card companies to ensure the security of credit card transactions in the payment industry.[34]

The Board was also informed about PwC's four "Key Recommendations" for Marriott to "[u]pdate Starwood's brand standards," including mandating PCI and setting clear cybersecurity expectations.[35] Consistent with PwC's recommendation, Hoffmeister advised the Board on February 10, 2017 that there would be efforts to implement tokenization across Starwood's data systems.[36]

---

[31] Am. Compl. ¶ 124. Defs.' Ex. 13 at 1250.

[32] Am. Compl. ¶ 124; Defs.' Ex. 14 at 1287-88.

[33] Am. Compl. ¶¶ 124, 126; Defs.' Ex. 13 at 1249-50; Defs.' Ex. 14 at 1288.

[34] Am. Compl. ¶ 53.

[35] *Id.* ¶ 125; Defs.' Ex. 14 at 1287-88.

[36] Defs.' Ex. 13 at 1250.

D. Ongoing Migration of Starwood's Systems

The full Post-Acquisition Board was next updated on cybersecurity at a regularly scheduled meeting held on February 9, 2018.[37] At that meeting, defendant Chief Financial Officer Kathleen K. Oberg advised the Board that Marriott had undertaken several "Key Mitigating Activities" to address the Company's top risks including cybersecurity.[38] Those activities included adopting new technologies to strengthen cybersecurity and "[m]igration of Starwood systems to the Marriott established technology standards" with a September 2019 estimated completion date.[39] In addition, Marriott had "implement[ed] patching compliance tools and reporting framework within Starwood environments."[40] On May 3, 2018, Ernst & Young presented to the Audit Committee an assessment of "the effectiveness of the Company's controls over IT risks," which included "testing the conversion of Starwood legacy activities" to new systems.[41]

On August 9, 2018, Hoffmeister updated the full Board on "Noteworthy Security Events/Incidents," including 4 cybersecurity events which involved legacy

[37] Am. Compl. ¶ 127; Defs.' Ex. 16 at 1394.

[38] Am. Compl. ¶ 130.

[39] *Id.* ¶ 127; Defs.' Ex. 15 at 1386.

[40] Am. Compl. ¶ 127; Defs.' Ex. 15 at 1386.

[41] Defs.' Ex. 17 at 1496.

Starwood systems.[42] Those incidents included a cyberattack on a legacy Starwood franchise network and malware found on a legacy Starwood server utilized by the Marriott Law Department.[43] Hoffmeister "confirmed there were no successful attempts to download [or] install" the malware onto that server.[44] Hoffmeister also reported that the Company had "engaged a consultant to execute a cybersecurity assessment."[45]

E. Discovery of a Starwood Guest Reservation Database Breach

On September 7, 2018, Marriott received an alert that an unknown user had run a query in Starwood's guest reservation database.[46] A third party contractor that managed the guest reservation database informed Marriott's Information Technology department about the incident the following day.[47] Ten days later, on September 17, 2018, outside investigators engaged by Marriott uncovered malware on Starwood's system that had the potential to access, surveil, and gain

[42] Am. Compl. ¶ 128; Defs.' Ex. 19 at 1741; Defs.' Ex. 20 at 1783-90. Lewis was absent from the meeting. Defs.' Ex. 19 at 1741.

[43] Am. Compl. ¶ 128; Defs.' Ex. 20 at 1783, 1790. No guest data was lost from the franchise network attack. *Id.* at 1790.

[44] *Id.* at 1783.

[45] Defs.' Ex. 19 at 1746.

[46] Am. Compl. ¶¶ 8, 133.

[47] *Id.* at ¶ 133.

administrative control over the system computer.[48] Marriott's Information Technology department informed Sorenson about the ongoing investigation the same day.[49] On September 18, 2018, Sorenson notified the Board.[50] The Company notified the FBI of the intrusion on October 29, 2018 after Marriott's investigators found evidence of other malware in Starwood's database, including malware that hackers use to search a device for usernames and passwords.[51]

The Company's investigation continued into November 2018, with the Board and Audit Committee receiving regular updates from management and privileged briefings from Marriott's General Counsel.[52] In early November 2018, Marriott learned that the breach began as far back as July 2014.[53] On November 13, 2018, "[Marriott's] investigators discovered evidence that two compressed encrypted files had been deleted from a device they were examining."[54] On November 19, 2018,

---

[48] *Id.*

[49] *Id.* ¶ 136.

[50] *Id.*

[51] *Id.* ¶¶ 137-38.

[52] *E.g.*, *id.* ¶¶ 139-42; Defs.' Ex. 21 at 1946; Ex. 22 at 2079; Ex. 23 at 2084; *see also* Defs.' Exs. 25-27.

[53] Am. Compl. ¶ 139.

[54] Defs.' Ex. 28 at 2743.

the Company discovered that those files contained customers' personal information.[55]

Eleven days later, on November 30, 2018, the Company publicly announced the data security incident.[56] Marriott's press release explained that there had been unauthorized access to the Starwood network since 2014 that exposed the personal information of approximately 500 million guests.[57] The exploited information included guests' names, passport numbers, birth dates, email and mailing addresses, payment card details, and Starwood Preferred Guest account information.[58] The cyber attack resulted in one of the biggest data breaches in history.[59]

---

[55] Am. Compl. ¶ 140; Defs.' Ex. 28 at 2743.

[56] Am. Compl. ¶¶ 140-41, 143.

[57] *Id.* ¶ 143; *see also* Defs.' Ex. 28 at 2744 (Sorenson stating that the Breach involved less than 383 million unique guests).

[58] Am. Compl. ¶ 143.

[59] *Id.* ¶ 217 (calling the incident the "second largest data breach in history"); *see* Aisha Al-Muslim, Dustin Volz, and Kimberly Chin, *Marriott Says Starwood Data Breach Affects Up to 500 Million People*, Wall St. J. (Nov. 30, 2018); Nicole Perlroth, Amie Tsang, and Adam Satariano, *Marriott Hacking Exposes Data of Up to 500 Million Guests*, N.Y. Times (Nov. 30, 2018) ("The assault . . . was one of the largest known thefts of personal records, second only to a 2013 breach of Yahoo that affected three billion user accounts and larger than a 2017 episode involving the credit bureau Equifax.").

Marriott's stock price dropped by more than 5.5% following the announcement.[60] In the weeks that followed, the stock price dropped $15.45 per share (more than 12%) from its high on November 29, 2018.[61]

F. Federal Lawsuits and Regulatory Investigations

Numerous lawsuits and regulatory investigations followed Marriott's November 30, 2018 announcement. Attorneys general of all 50 states and the District of Columbia, the Securities and Exchange Commission, the Federal Trade Commission, and certain committees of the U.S. Senate and House of Representatives, among others, opened investigations into the data breach.[62] Marriott also faced class action lawsuits for violations of federal securities laws, violations of state and federal consumer protection laws, and violations of state disclosure laws. Those lawsuits, along with a lawsuit by a financial institution accusing Marriott of failing to perform adequate due diligence during the acquisition, were consolidated for multi-district litigation (the "Federal Action") in the United States District Court for the District of Maryland.[63]

---

[60] Am. Compl. ¶ 151.

[61] *Id.*

[62] *Id.* ¶¶ 14, 152-54.

[63] *In re Marriott Int'l Inc., Customer Data Sec. Breach Litig.*, 2021 WL 2401641, at *1-3 (D. Md. June 11, 2021).

With respect to the consumer class action, the District of Maryland denied, in part, Marriott's motion to dismiss certain "bellwether" claims that the parties had selected to test the sufficiency of the pleadings. In doing so, the court held that the consumer plaintiffs plausibly stated claims that Marriott had violated the Maryland Personal Information Privacy Act's requirement to provide "timely notice to customers affected by [a] breach" by "fail[ing] to disclose the data breach for more than two months."[64] The court similarly denied Marriott's motion under Michigan's Identity Theft Protection Act, which also required timely notice to consumers.[65]

As for the federal securities law claims, the District of Maryland held that the statements challenged by the plaintiffs—including statements about due diligence and integration, risk factors, and protection of customer data—were not materially false or misleading and dismissed those claims with prejudice.[66] Delaware state law claims for breach of fiduciary duty, waste of corporate assets, and unjust enrichment were also dismissed without prejudice.[67]

---

[64] *In re Marriott Int'l Inc. Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 488 (D. Md. 2020).

[65] *Id.* at 490.

[66] *Marriott*, 2021 WL 2401641, at *6-7.

[67] *Id.* at *19.

G. This Derivative Litigation

The plaintiff filed this derivative action on December 3, 2019 after obtaining roughly 3,000 pages of documents from the Company pursuant to 8 *Del. C.* § 220.[68] The plaintiff's books and records request was limited to Board-level "cybersecurity" documents since May 23, 2014.[69] On March 16, 2020, the plaintiff filed an amended complaint, the operative complaint in this action (the "Complaint").[70]

The Complaint asserts a single claim for breach of fiduciary duty against 13 of the 14 directors who served on the Board when the Complaint was filed (*i.e.*, the Post-Acquisition Board), several officers, and one former director (Romney).[71] The claim is based on allegations that the individual defendants breached their fiduciary duties by (1) failing to "undertake cybersecurity and technology due diligence" during the Acquisition; (2) failing to implement adequate internal controls after the Acquisition; and (3) concealing the data security incident until November 30, 2018.[72]

---

[68] Defs.' Opening Br. 16.

[69] Am. Compl. ¶ 107; *see* Pl.'s Answering Br. 23 n.10 (Dkt. 51). The production did not include officer-level documents. *Id.*; Mot. to Dismiss Hr'g Tr. 55 (noting that the plaintiff did not press to receive a beneath-the-board Section 220 production).

[70] Dkt. 33.

[71] Am. Compl. ¶¶ 20-37. The four officer defendants are Oberg, Hoffmeister, Bao Giang Val Bauduin (Marriott's Controller and Chief Accounting Officer), and Stephanie C. Linnartz (Marriott's Chief Commercial Officer and Executive Vice President). Am. Compl. ¶¶ 22, 24-26.

[72] *Id.* ¶¶ 20-37, 246-47. The Complaint also advances other theories for breach of fiduciary duty such as "violating the Company's Guidelines" and suggests that certain defendants

On April 30, 2020, the defendants moved to dismiss the Complaint.[73] After the reassignment of this matter from then-Chancellor Bouchard, I heard re-argument on the motion to dismiss on July 7, 2021.[74]

II. ANALYSIS

The defendants have moved to dismiss the Complaint under Court of Chancery Rule 23.1 for failure to make a demand on the Board. For the reasons explained below, I conclude that demand was not excused. The Complaint is therefore dismissed in its entirety.

A. The Legal Standard for Demand Excusal

"The decision whether to initiate or pursue a lawsuit on behalf of the corporation is generally within the power and responsibility of the board of directors."[75] A stockholder plaintiff can pursue claims belonging to the corporation if (1) the corporation's directors wrongfully refused a demand to authorize the

---

could not impartially consider a demand because of the Securities Class Action. *See* Am. Compl. ¶ 238. But these issues were not briefed or pressed at argument. Issues not briefed are waived. *See, e.g.*, *Emerald P'rs v. Berlin*, 726 A.2d 1215, 1224 (Del. 1999). The plaintiff also withdrew its assertions of breach of fiduciary duty based on disclosure violations after overlapping claims were dismissed in the Federal Action. *See* Mot. to Dismiss Hr'g Reargument Tr. at 67 (hereinafter "Reargument Hr'g Tr.") (Dkt. 87); *Marriott*, 2021 WL 2407518, at *45.

[73] Dkt. 39.

[74] Dkt. 87.

[75] *In re Citigroup Inc. S'holder Deriv. Litig.*, 964 A.2d 106, 120 (Del. Ch. 2009) (citing 8 *Del. C.* § 141(a)).

corporation to bring the suit or (2) a demand would have been futile because the directors were incapable of impartially considering the demand.[76] Because the plaintiff did not make a demand on Marriott's Board, the Complaint must plead particularized factual allegations establishing that demand was excused.[77]

The parties initially debated whether the *Aronson* or *Rales* standard for assessing demand excusal should apply.[78] The defendants argued that the *Rales* standard applied because the plaintiff's claims are predicated upon the Board's alleged failure to act and not a challenge to an affirmative decision.[79] The plaintiff agreed that *Rales* applied other than to the claim challenging the Board's decision to complete the Acquisition without conducting cybersecurity due diligence, which it argued should be analyzed under *Aronson*.[80]

That question became moot after the Delaware Supreme Court's decision in *United Foods & Commercial Workers Union v. Zuckerberg*.[81] There, the Court held that it is "no longer necessary to determine whether the *Aronson* test or the *Rales*

---

[76] *See Rales v. Blasband*, 634 A.2d 927, 932 (Del. 1993).

[77] Ct. Ch. R. 23.1; *see, e.g.*, *Guttman v. Huang*, 823 A.2d 492, 499 (Del. Ch. 2003).

[78] *See Aronson v. Lewis*, 473 A.2d 805, 814 (Del. 1984) *overruled on other grounds by Brehm v. Eisner*, 746 A.2d 244 (Del. 2000); *Rales* 634 A.2d at 932-935.

[79] Defs.' Reply Br. 5 (Dkt. 65).

[80] Pl.'s Answering Br. 20-22.

[81] 2021 WL 4344361 (Del. 2021).

test governs a complaint's demand-futility allegations."[82] Instead, the Court adopted a three-part "universal test" for assessing demand futility that is "consistent with and enhances" *Aronson*, *Rales*, and their progeny, which "remain good law."[83] Going forward:

> Delaware courts should ask the following three questions on a director-by-director basis when evaluating allegations of demand futility:
>
> (i) whether the director received a material personal benefit from the alleged misconduct that is the subject of the litigation demand;
>
> (ii) whether the director faces a substantial likelihood of liability on any of the claims that would be the subject of the litigation demand; and
>
> (iii) whether the director lacks independence from someone who received a material personal benefit from the alleged misconduct that would be the subject of the litigation demand or who would face a substantial likelihood of liability on any of the claims that are the subject of the litigation demand.[84]

Demand is excused as futile if "the answer to any of the questions is 'yes' for at least half of the members of the demand board."[85] The "analysis is conducted on a claim-by-claim basis."[86]

---

[82] *Id.* at *17.

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] *Beam v. Stewart*, 833 A.2d 961, 977 (Del. Ch. 2003).

While engaging in this analysis, I confine myself to the well-pleaded allegations of the Complaint, the documents incorporated into the Complaint by reference, and facts subject to judicial notice.[87] All reasonable inferences from the allegations in the Complaint are drawn in favor of the plaintiff.[88] "Rule 23.1 is not satisfied by conclusory statements or mere notice pleading."[89] Instead, "[w]hat the pleader must set forth are particularized factual statements that are essential to the claim."[90]

B. The Demand Excusal Analysis in This Case

"The court 'counts heads' of the members of a board to determine whether a majority of its members are disinterested and independent for demand futility purposes."[91] The Board in place when this litigation was filed had 14 members: the Post-Acquisition Board members (Sorenson, Marriott, Jr., Harrison, Kellner, Muñoz, Bush, Lee, Henderson, Reinemund, Schwab, Duncan, Hippeau, and Lewis), excluding Romney who was replaced by non-party Margaret M. McCarthy

---

[87] *See, e.g.*, *White v. Panic*, 783 A.2d 543, 546-47 (Del. 2001); *see also Gen. Motors*, 897 A.2d at 170.

[88] *Brehm*, 746 A.2d at 255.

[89] *Id.* at 254.

[90] *Id.*

[91] *See In re Zimmer Biomet Hldgs. Inc. Deriv. Litig.*, 2021 WL 3779155, at *10 (Del. Ch. Aug. 25, 2021).

(together, the "Demand Board").[92] The plaintiff does not challenge the impartiality of McCarthy. Nor does the plaintiff claim that any director received a material personal benefit from the challenged conduct.

The plaintiff only alleges that four members of the Demand Board—Sorenson, Marriott, Jr., Harrison, and Reinemund—lack (or lacked) independence.[93] Even if the plaintiff could sufficiently demonstrate that these four directors lacked independence, it must also impugn the disinterestedness of at least three others to show that a majority of the Demand Board could not consider a demand.[94] The plaintiff attempts to make that showing by arguing that the Post-Acquisition Board members all face a substantial likelihood of personal liability.[95]

"To establish a substantial likelihood of liability at the pleading stage, a plaintiff must 'make a threshold showing, through the allegation of particularized facts, that their claims have some merit.'"[96] Because Marriott's certificate of incorporation contains a provision exculpating its directors for breaches of the duty

[92] Am. Compl. ¶¶ 20-21, 23, 27-37, 227.

[93] Pl.'s Answering Br. 59.

[94] *See Zuckerberg*, 2021 WL 4344361, at *17.

[95] Pl.'s Answering Br. 20-21.

[96] *In re TrueCar, Inc. S'holder Deriv. Litig.*, 2020 WL 5816761, at *12 (Del. Ch. Sept. 30, 2020) (quoting *Rales*, 634 A.2d at 934).

of care, as permitted under 8 *Del. C.* § 102(b)(7),[97] "the plaintiff[] must plead with particularity facts that support a meritorious claim for breach of the duty of loyalty."[98] The Complaint focuses on three areas of potential liability based on the Board's alleged failure to: (1) conduct pre-Acquisition due diligence into Starwood's cybersecurity; (2) remedy deficiencies in Starwood's information protection systems post-Acquisition; and (3) timely disclose the data security incident.

The outcome of my analysis on each issue is that none of the Post-Acquisition Board members face a substantial likelihood of liability for a non-exculpated claim. Any claim based on pre-Acquisition due diligence is time-barred. The remaining claims fall short of pleading a breach of the directors' duty of loyalty. At least 10 of the 14 Demand Board members were therefore both disinterested and independent with respect to a pre-suit litigation demand. I need not decide whether the remaining four directors lacked independence.

1. The Plaintiff's Challenge to Pre-Acquisition Due Diligence is Time Barred.

The plaintiff asserts that the 11 members of the Pre-Acquisition Board face a substantial likelihood of personal liability for their "decision to complete the

[97] Defs.' Ex. 4 at 12.

[98] *Zimmer*, 2021 WL 3779155, at *12; *see Zuckerberg*, 2021 WL 4344361, at *8-15 (holding that exculpated care claims do not satisfy the second prong of *Aronson* and do not render a director incapable of impartially considering a litigation demand).

Acquisition without conducting any due diligence into Starwood's cybersecurity."[99] The defendants contend that the claim is time barred.[100] Delaware's three-year statute of limitations applies by analogy to equitable claims seeking legal relief.[101] Absent tolling, the limitations period "begins to run from the time of the [allegedly] wrongful act, without regard for whether the plaintiff became aware of the wrongdoing at that time."[102]

Here, the plaintiff's breach of fiduciary duty claim seeking monetary damages is subject to the analogous three-year statute of limitations.[103] The alleged wrongful act—the Pre-Acquisition Board's approval of the Acquisition, allegedly without adequate cybersecurity due diligence—occurred before Marriott announced that approval on December 22, 2015.[104] At the latest, the statute of limitations began to

---

[99] Pl.'s Answering Br. 21 (emphasis removed).

[100] *See* Defs.' Reply Br. 8 n.3; Defs.' Supp. Br. 5 (Dkt. 81).

[101] *See Kraft v. Wisdom-Tree Invs., Inc.*, 145 A.3d 969, 979-81, 983 (Del. Ch. 2016) (explaining that for equitable claims seeking legal relief, such as "a breach of fiduciary duty action seeking monetary damages," the "analogous limitations period [will] operate as a strong presumption of laches"); *see also* 10 *Del. C.* § 8106.

[102] *Kraft*, 145 A.3d at 989 (citing *Wal-Mart Stores, Inc. v. AIG Life Ins. Co.*, 860 A.2d 312, 319 (Del. 2004)); *see also Tilden v. Cunningham*, 2018 WL 5307706, at *14 (Del. Ch. Oct. 26, 2018) ("[T]he law in Delaware is crystal clear that a claim accrues as soon as the wrongful act occurs.").

[103] *See Kraft*, 145 A.3d at 983.

[104] Defs.' Ex. 29 at 97 (explaining that the Board approved the merger agreement on November 15, 2015 and recommended stockholder approval).

run on September 23, 2016 when the Acquisition closed.[105] The plaintiff filed this action more than three years later on December 3, 2019. The plaintiff's due diligence-based claim is therefore barred as untimely "absent tolling or other extraordinary circumstances."[106] The plaintiff contends that the defendants waived their untimeliness defenses and also advances two tolling arguments. None of the plaintiff's arguments have merit.

a. Waiver

The plaintiff first contends that defendants waived their untimeliness argument because it was not raised in their opening brief.[107] "Under the briefing rules, a party is obliged in its motion and opening brief to set forth all of the grounds, authorities and arguments supporting its motion."[108]

No such waiver occurred. As I wrote to counsel when requesting supplemental briefing, it was not apparent from the Complaint that the plaintiff was

---

[105] Am. Compl. ¶ 104; *see* Mot. to Dismiss Hr'g Tr. at 51-52, 54 ("The Court: [W]hat are you alleging is the wrongful act that would have triggered the statute of limitations? Is it the acquisition or is it the board approval? [Counsel]: It is the acquisition, Your Honor. It is not the board approval.").

[106] *Kraft*, 145 A.3d at 982-83.

[107] Pl.'s Supp. Br. 2 (Dkt. 82).

[108] *Franklin Balance Sheet Inv. Fund v. Crowley*, 2006 WL 3095952, at *4 (Del. Ch. Oct. 19, 2006) (citing Ct. Ch. R. 7(b), 171); *see Thor Merritt Square, LLC v. Bayview Malls LLC*, 2010 WL 972776, at *5 (Del. Ch. Mar. 5, 2010) ("The failure to raise a legal issue in an opening brief generally constitutes a waiver of the ability to raise that issue in connection with a matter under submission to the court.").

challenging the closing of the Acquisition as an affirmative act of the Board.[109] The plaintiff's answering brief squarely presented the argument that the Board's "decision to complete the acquisition without conducting . . . due diligence into Starwood's cybersecurity" was itself a breach of the duty of loyalty.[110] The defendants raised the untimeliness of that "reformulated" claim in their reply brief,[111] which appropriately "consisted of material necessary to respond to the answering brief."[112]

b. Equitable Tolling and Fraudulent Concealment

The plaintiff also argues that the claim is not time-barred because the statute of limitations was tolled pursuant to fraudulent concealment and equitable tolling.[113] The doctrines of fraudulent concealment and equitable tolling "permit[] tolling of the limitations period where 'the facts underlying the claim [are] so hidden that a reasonable plaintiff could not timely discover them.'"[114] Fraudulent concealment may be demonstrated where a defendant conceals information through an affirmative

---

[109] Dkt. 78 at 2-3.

[110] Pl.'s Answering Br. 21-22; *compare* Am. Compl. ¶ 228.

[111] Defs.' Reply Br. 8 n.3.

[112] *Crowley*, 2006 WL 3095952, at *4.

[113] Pl.'s Supp. Br. 5.

[114] *Weiss v. Swanson*, 948 A.2d 433, 451 (Del. Ch. 2008) (quoting *In re Dean Witter P'ship Litig.*, 1998 WL 442456, at *6 (Del. Ch. July 17, 1998)).

act of "actual artifice" that prevents a plaintiff from gaining knowledge of the facts or misdirects a plaintiff from the truth.[115] Equitable tolling can toll the statute of limitations for self-dealing claims, even without actual concealment, where a plaintiff relies "on the competence and good faith of a fiduciary."[116]

The plaintiff asserts that the defendants cannot "point to a single allegation in the Complaint" demonstrating that stockholders were on notice that the Pre-Acquisition Board did not conduct cybersecurity due diligence.[117] But it is the plaintiff's burden to plead specific facts demonstrating that the statute of limitations was tolled before this litigation was filed.[118] Assuming the facts alleged in the Complaint as true, neither tolling doctrine is applicable.

The plaintiff does not allege any affirmative acts of concealment that could support the application of fraudulent concealment. "Mere silence is insufficient . . . ."[119] The only acts that the plaintiff cites are public statements by Sorenson and

---

[115] *Id.* (quoting *In re Tyson Foods, Inc.*, 919 A.2d 563, 585 (Del. Ch. 2007)); *State v. Pettinaro Enters.*, 870 A.2d 513, 531 (Del. Ch. 2005) ("Fraudulent concealment may be found to exist where a defendant knowingly acted to prevent a plaintiff from learning facts or otherwise made misrepresentations intended to 'put the plaintiff off the trail of inquiry.'" (quoting *Halpern v. Barran*, 313 A.2d 139, 143 (Del. Ch. 1973))).

[116] *Weiss*, 948 A.2d at 451.

[117] Pl.'s Supp. Br. 7.

[118] *Weiss*, 948 A.2d at 451.

[119] *Krahmer v. Christie's Inc.*, 911 A.2d 399, 407 (Del. Ch. 2006).

others touting Marriott's "extensive" due diligence of Starwood.[120] There is no reason to doubt the truth of those statements generally. The plaintiff points to no representation that Marriott was undertaking cybersecurity diligence in particular. Nor does the plaintiff allege specific facts that would suggest Marriott's statements were meant to throw stockholders "off the trail of inquiry."[121]

As to equitable tolling, there are no allegations in the Complaint that permit a reasonable inference of wrongful self-dealing. In fact, the plaintiff does not allege that any of the individual defendants benefitted from the conduct challenged in the Complaint. For claims that do not involve self-dealing, "equitable tolling operates in much the same way as the doctrine of fraudulent concealment," and an affirmative act of concealment is required.[122] Again, the plaintiff has not made that showing.

---

[120] Pl.'s Supp. Br. 5 (citing Am. Compl. ¶¶ 12, 104, 174, 179, 180-83). The court need not consider similar statements about the Company's general due diligence in Marriott's Form S-4, filed in connection with the Acquisition. *See* Pl.'s Supp. Br. 7 (asking that the court decline to take judicial notice of the Form S-4).

[121] *Pettinaro Enters.*, 870 A.2d at 531.

[122] *Litman v. Prudential-Bache Props., Inc.*, 1994 WL 30529, at *3 (Del. Ch. Jan. 14, 1994). In *Litman*, then-Vice Chancellor Chandler discussed then-Chancellor Allen's decision in *Kahn v. Seaboard Corp.*, 625 A.2d 269 (Del. Ch. 1993), where the court explained that affirmative acts of concealment may not be necessary to apply the doctrine of equitable tolling if "the parties to the litigation stand in a fiduciary relationship to each other *and* where the plaintiff alleges self-dealing." *Litman*, 1994 WL 30529, at *3 (emphasis added). *Litman* held that "[i]n situations that do not involve self-dealing, equitable tolling . . . operate[s] to toll a limitations period when the defendant has engaged in certain acts that would prevent the plaintiff from discovering the alleged wrong." *Id.*

c. Tolling During Inspection Demand

Finally, the plaintiff argues the statute of limitations was tolled while the plaintiff pursued an inspection demand pursuant to 8 *Del. C.* § 220. Even if the analogous statute of limitations began to run on September 23, 2016 when the Acquisition closed, it was not tolled by the plaintiff's January 4, 2019 books and records demand.[123] The plaintiff relies on precedent where the court has tolled the statute of limitations during the pendency of Section 220 litigation.[124] The plaintiff does not, however, cite any authority to support the notion that service of a books and records demand alone tolls the statute of limitations for a subsequent plenary lawsuit.

In *Technicorp*, the court explained that "the institution of other litigation to ascertain the facts involved in the later suit will toll the statute of limitations while that litigation proceeds."[125] Likewise, in *Sutherland*, the court noted that the Section 220 lawsuit tolled the applicable three-year statute of limitations . . . during the

[123] Am. Compl. ¶¶ 79, 218; *see supra* 23-24. No allegation that the Board undertook the "wrongful act" of closing the Acquisition is found in the Complaint. The Board's recommendation that stockholders approve the Acquisition is the last affirmative act of the Board in the pre-Acquisition time period.

[124] *See Technicorp Int'l II v. Johnston*, 2000 WL 713750, at *9 (Del. Ch. May 31, 2000); *Sutherland v. Sutherland*, 2009 WL 857468, at *4-5 (Del. Ch. Mar. 23, 2009).

[125] 2000 WL 713750, at *9.

pendency of the plaintiff's Section 220 action"[126] Here, despite the running of the statute of limitations during its Section 220 investigation, the plaintiff did not file a Section 220 lawsuit. Further, "there is no hard and fast rule tolling the running of the statute of limitations during the pendency of books and records litigation."[127] Nor did the plaintiff obtain a tolling agreement with the defendants while its investigation continued.[128]

Tolling considerations are different for a Section 220 demand and a Section 220 lawsuit. The former has no formal schedule. A stockholder could serve a Section 220 demand that fails to satisfy even the basic statutory requirements of Section 220(b) and use the demand effectively as a placeholder. A Section 220

---

[126] 2009 WL 857468, at *5.

[127] *Sutherland*, 2009 WL 1177047, at *1; *see also Sutherland v. Sutherland*, 2010 WL 1838968, at *5 n.19 (Del. Ch. May 3, 2010) (explaining that a court should consider whether the plaintiff "was, or should have been, aware of [the derivative] claims during the pendency of the § 220 Action"). In *Gotham P'rs, L.P. v. Hallwood Realty P'rs, L.P.*, the court explained that a plaintiff could defeat a laches defense by showing "that it asserted its rights in a timely manner by making [a] demand [under Section 220] *and* filing th[at] action." 714 A.2d 96, 104-05 (Del. Ch. 1998) (emphasis added). The court did not say that a timely demand alone would toll the statute of limitations until a subsequent plenary action was filed. Rather, the court was discussing how a stockholder can demonstrate that it asserted its rights or claim—both through a books and records demand and in pursuing litigation—in a manner that defeats a laches defense. *Id.*

[128] As a result, there is no basis to apply the doctrine of equitable estoppel, as the plaintiff suggests. *See* Pl.'s Supp. Br. 10-11. The plaintiff asserts that the defendant "slow-rolled" the process of producing documents in response to its Section 220 demand, leading the plaintiff to rely on that conduct to its detriment. *Id.* But the plaintiff had the right to file Section 220 litigation, a plenary suit, or demand a tolling agreement.

lawsuit, by contrast, is a summary proceeding with "expedited discovery and a prompt hearing."[129] Unlike a demand, a Section 220 action presents "strong evidence that [a] plaintiff was aggressively asserting its claims."[130] There may be an instance where a stockholder's dogged pursuit of its statutory books and records rights provides a basis for tolling. But this lawsuit, where the stockholder took nearly 11 months between serving a demand and filing a plenary lawsuit, is not it.

2. The Plaintiff's Challenges to Cybersecurity Oversight Post-Closing Do Not Excuse Demand.

The plaintiff next argues that a majority of the Demand Board faces a substantial likelihood of liability for their "conscious and bad faith decision not to remedy Starwood's severely deficient information protection systems post-Acquisition."[131] As often stated, oversight liability under *Caremark* is "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment."[132] To prevail, the plaintiff must plead particularized facts showing that either (1) "the directors utterly failed to implement any reporting or information system or controls" or (2) "having implemented such a system or controls,

[129] *Cutlip v. CBA Int'l, Inc. I*, 1995 WL 694422, at *1 (Del. Ch. Oct. 27, 1995).

[130] *Gotham P'rs*, 714 A.2d at 105.

[131] Pl.'s Answering Br. 34.

[132] *In re Caremark Int'l Inc. Deriv. Litig.*, 698 A.2d 959, 967 (Del. Ch. 1996).

consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."[133]

Compliance risk oversight generally falls within the governance responsibilities of the board of directors.[134] Key enterprise risks affecting a corporation's "mission critical" components has been a focus of Delaware courts in assessing potential oversight liability, particularly where a board has allegedly failed to implement reporting systems or controls to monitor those risks.[135] Cybersecurity, however, is an area of consequential risk that spans modern business sectors. In the past several years alone, cyberattacks have affected thousands of companies and government agencies. High-profile data breaches have exposed customer data at businesses from Yahoo! to Target and Home Depot.[136] Targeted attacks have shut

---

[133] *Stone v. Ritter*, 911 A.2d 362, 370 (Del. Ch. 2006).

[134] *See Okla. Firefighters Pension & Ret. Sys. v. Corbat*, 2017 WL 6452240, at *18 (Del. Ch. Dec. 18, 2017) ("[E]valuation of risk is a core function of the exercise of business judgment."); *Marchand v. Barnhill*, 212 A.3d 805, 824 (Del. 2019) (describing the board's duty to "put in place a reasonable system of monitoring and reporting about the corporation's central compliance risk").

[135] *See, e.g.*, *Marchand*, 212 A.3d at 824 (finding that board-level monitoring on food safety was needed where "food safety . . . essential and mission critical" to an ice cream manufacturer); *In re Boeing Co. Deriv. Litig.*, 2021 WL 4059934, at *26 (Del. Ch. Sept. 7, 2021) (finding airplane safety "mission critical" to an airplane manufacturer's business); *see also In re Clovis Oncology, Inc. Deriv. Litig.*, 2019 WL 4850188, at *14-15 (Del. Ch. Oct. 1, 2019) (denying motion to dismiss in the context of *Caremark*'s second prong where red flags about a "monoline" company's single promising drug were ignored).

[136] Stockholder litigation followed. *See, e.g.*, *In re Home Depot, Inc. S'holder Deriv. Litig.*, 223 F. Supp. 3d 1317 (N.D. Ga. 2016); *Davis v. Steinhafel*, Lead Case No. 14-cv-203 (PAM/JJK) (D. Minn. July 7, 2016) (ORDER); *Okla. Firefighters Pension & Ret. Sys. v.*

down hospitals and taken offline major fuel pipelines.[137] Regulators in the United States and abroad have become more active in issuing cybersecurity guidance and undertaking enforcement activities in response.[138] The President of the United States has named cybersecurity a "top priority and essential to national and economic security."[139]

Delaware courts have not broadened a board's *Caremark* duties to include monitoring risk in the context of business decisions.[140] Oversight violations are

---

Brandt, C.A. No. 2017-0133-SG (Del. Ch. Feb. 23, 2017); *In re Yahoo! Inc., S'holder Litig.*, No. 17-CV-307054 (Cal. Super. Ct. Mar. 2, 2018).

[137] *See* Robert McMillan and Melanie Evans, *Ransomware Attack Hits Universal Health Services*, Wall St. J. (Sept. 30, 2020); Christopher Bing and Stephanie Kelly, *Cyber Attack Shuts Down U.S. Fuel Pipeline 'Jugular,' Biden Briefed*, Reuters (May 8, 2021).

[138] *See, e.g.*, Cal. Civ. Code §§ 1798.110, 1798.150 (West 2021) (imposing data collection obligations on companies doing business in California and providing consumers with a private right of action to address harms caused by data breaches); European Union General Data Protection Regulation, Council Regulation 2016/679 (mandating data security measures and breach notification); *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, 83 Fed. Reg. 8,166 (Feb. 22, 2018) (Sec. & Exch. Comm'n) ("[T]he Commission believes that the development of effective disclosure controls and procedures is best achieved when a company's directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents that the company has faced or is likely to face."); Jared Ho, *Corporate Boards: Don't Underestimate Your Role in Data Security Oversight,* Fed. Trade Comm'n (Apr. 28, 2021).

[139] Exec. Order No. 14,208, 86 Fed. Reg. at 26,633 (2021).

[140] *See, e.g.*, *Reiter v. Fairbank*, 2016 WL 6081823, at *8 (Del. Ch. Oct. 18, 2016) ("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."); *In re Goldman Sachs Grp., Inc. S'holder Litig.*, 2011 WL 4826104, at *21 (Del. Ch. Oct. 12, 2011) (stating that the Court of Chancery has "not definitively stated whether a board's *Caremark* duties involve a duty to monitor business risk"); *Corbat*, 2017

typically found where companies—particularly those operating within a highly-regulated industry—violate the law or run afoul of regulatory mandates.[141] But as the legal and regulatory frameworks governing cybersecurity advance and the risks become manifest, corporate governance must evolve to address them.[142] The corporate harms presented by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place.

The growing risks posed by cybersecurity threats do not, however, lower the high threshold that a plaintiff must meet to plead a *Caremark* claim. For either prong of *Caremark*, "a showing of bad faith conduct . . . is essential to establish director

---

WL 6452240, at *18 (stating that a "failure to monitor or properly limit business risk" is a "theory of director liability that this Court has never definitively accepted"); *In re Facebook, Inc. Section 220 Litig.*, 2019 WL 2320842, at *14 (Del. Ch. May 30, 2019) ("The legal academy has observed that Delaware courts are more inclined to find Caremark oversight liability at the board level when the company operates in the midst of obligations imposed upon it by positive law yet fails to implement compliance systems, or fails to monitor existing compliance systems, such that a violation of law and resulting liability occurs.").

[141] *E.g.*, *La. Mun. Police Empls.' Ret. Sys. v. Pyott*, 46 A.3d 313, 355 (Del. Ch. 2012) (finding it was reasonable to infer directors approved a business plan allowing for illegal off-label marketing); *In re Massey Energy Co.*, 2011 WL 2176479, at *20-21 (Del. Ch. May 31, 2011) ("[A] fiduciary of a Delaware corporation cannot be loyal to a Delaware corporation by knowingly causing it to seek profit by violating the law.").

[142] *See* Leo E. Strine, Jr., Kirby M. Smith & Reilly S. Steel, *Caremark and ESG: Perfect Together: A Practical Approach to Implementing an Integrated, Efficient and Effective Caremark and EESG Strategy*, 106 Iowa L. Rev. 1885, 1893 (describing "the first principle of corporate law: corporations may only conduct lawful business by lawful means").

oversight liability."[143] Only a "sustained or systemic failure of the board to exercise oversight . . . will establish the lack of good faith that is a necessary condition to liability."[144] The Complaint in this case falls well short of demonstrating that the Post-Acquisition Board members face a substantial likelihood of liability for a sustained, bad faith failure of oversight. Demand is therefore not futile on that basis.

a. Cybersecurity Reporting Systems and Controls

To the extent the plaintiff attempts to put forward a claim under *Caremark*'s first prong, I find that effort unpersuasive. Delaware law imposes on directors a duty to ensure that board-level monitoring and reporting systems are in place. But because doing so is a disinterested business judgment, "directors have great discretion to design context- and industry-specific approaches tailored to their companies' businesses and resources."[145] For directors to face liability under *Caremark*'s first prong, a plaintiff must show that the director "made no good faith effort to ensure the company had in place any 'system of controls.'"[146]

---

[143] *Stone*, 911 A.2d at 370.

[144] *Caremark*, 698 A.2d at 971.

[145] *Marchand*, 212 A.3d at 821; *Citigroup*, 964 A.2d at 125 (explaining that although "directors of Delaware corporations have certain responsibilities to implement and monitor a system of oversight" that "obligation does not eviscerate the core protections of the business judgment rule").

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

Marriott's Board consistently ranked cybersecurity as a primary risk facing the Company.[147] The plaintiff does not, however, assert that the Post-Acquisition Board "utterly failed" to implement any reporting system or internal controls to address it.[148] Instead, the Complaint and documents incorporated into it demonstrate that the directors surpassed *Caremark*'s baseline requirement that they "try" in good faith to put a "reasonable compliance and reporting system in place."[149]

The Complaint, for example, describes how the Board and Audit Committee were "routinely apprised" on cybersecurity risks and mitigation, provided with annual reports on the Company's Enterprise Risk Assessment that specifically evaluated cyber risks, and engaged outside consultants to improve and auditors to audit corporate cybersecurity practices.[150] The Complaint also describes internal controls over the Company's public disclosure practices.[151] And when management received information that the plaintiff describes as "red flags" indicating

---

[147] *E.g.*, Am. Compl. ¶¶ 100, 118.

[148] *See Rojas v. Ellison*, 2019 WL 3408812, at *9 (Del. Ch. July 29, 2019); *Horman v. Abney*, 2017 WL 242571, at *8 & n.46 (Del. Ch. Jan. 19, 2017) (noting that, in the *Caremark* context, "utterly failed" is a "linguistically extreme formulation" that means "absolute, total" (citations omitted)).

[149] *Marchand*, 212 A.2d at 821.

[150] *See* Am. Compl. ¶¶ 118-130; *supra notes* 6-10 (describing ongoing updates to directors on information protection and cybersecurity).

[151] Am. Comp. ¶¶ 42-44.

vulnerabilities, the reports were delivered to the Board.[152] To the extent that the plaintiff contends the Post-Acquisition Board faces liability under the first prong of *Caremark*, that argument is meritless.[153] The Complaint itself shows that the Board has systems in place to assess cybersecurity risks.

b. No Failure to Monitor or Oversee Operations

The plaintiff's primary argument is that the Post-Acquisition Board faces a substantial likelihood of liability under the second prong of *Caremark* for consciously disregarding "red flags" indicating that Marriott was violating positive law.[154] For purposes of *Caremark*, a plaintiff must plead that the board knew about "red flags" alerting them to corporate misconduct and "consciously failed to act after learning about evidence of illegality."[155] The plaintiff has not, however, pleaded

---

[152] *Compare Marchand*, 212 A.2d at 809 ("Consistent with this dearth of any board-level effort at monitoring, the complaint pleads particularized facts supporting an inference that during a crucial period when yellow and red flags about food safety were presented to management, there was no equivalent reporting to the board.").

[153] *See Home Depot*, 223 F. Supp. 3d at 1326 (applying Delaware law and finding, in the context of a data security incident, that allegations of "numerous instances where the Audit Committee received regular reports from management on the state of [the company's] data security, and the Board in turn received briefings from both management and the Audit Committee" led to the conclusion that "the Board was fulfilling its duty of loyalty to ensure that a reasonable system of reporting existed"); *see also Corporate Risk Hlds. LLC v. Rowlands*, 2018 WL 9517195, at *4 (S.D.N.Y. Sept. 28, 2018) (finding swift efforts "to address [security] breach with contingency plans to ascertain and mitigate the harm" foreclosed claim under the "first category of *Caremark* liability").

[154] Pl.'s Answering. Br. 34-35.

[155] *Pyott*, 46 A.3d at 341; *see also Melbourne Mun. Firefighters' Pension Tr. v. Jacobs*, 2016 WL 4076369, at *12 (Del. Ch. Aug. 1, 2016) (distinguishing *Pyott* and *Massey*

with particularity that the Post-Acquisition Board learned of legal or regulatory violations. And even if it had, the Board did not consciously choose to remain idle.

i. *No known violations of law*

The plaintiff argues that the Post-Acquisition Board knew that Starwood's systems violated the law because it learned in February 2017 that Starwood's "[b]rand standards did not mandate PCI compliance, tokenization, or point-to-point encryption."[156] But the PCI DSS standards are required by financial institutions with which companies contract, not mandated by law.[157] Nor is tokenization, which can reduce the amount of cardholder data in a digital environment and streamline PCI DSS compliance efforts.[158] Pleading non-compliance with non-binding industry

---

because "the Board, at all times, was under the impression that its conduct did *not* violate applicable . . . laws"); *South v. Baker*, 62 A.3d 1, 14-15 (Del. 2012) (explaining that a plaintiff who cannot plead actual director involvement in "decisions that violated positive law" can "plead that the board consciously failed to act after learning about evidence of illegality—the proverbial 'red flag'"); *see generally* Elizabeth Pollman, Corporate Disobedience, 68 Duke L.J. 709, 723 (2019).

[156] Am. Compl. ¶ 124.

[157] Those standards, set by the PCI Security Standards Council, founded by American Express, Discover, JCB International, Mastercard and Visa, are intended to reduce credit card fraud. *See* PSI Security Standards Council, *PCI Security* https://www.pcisecuritystandards.org/pci_security/.

[158] *See* PCI Security Standards Council, *Tokenization Product Security Guidelines* (Apr. 2015) https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf.

standards, like the PCI DSS, is not the same as pleading that directors knowingly permitted a company to violate positive law.[159]

The plaintiff also argues that the failure to improve Starwood's deficient systems risked the violation of various laws, including the FTC Act, state privacy acts and unfair competition laws, and "international regulatory standards."[160] Simply listing statues "in vague, broad terms" without alleging what law was violated and how is insufficient to state a *Caremark* claim.[161] The only law the parties specifically address in their briefs is the FTC Act. The plaintiff asserts that the Board's knowledge of PCI DSS non-compliance is enough to support a reasonable inference that its members knew Starwood's cybersecurity practices fell short of the FTC's heightened requirements.[162] The defendants respond that the FTC only "recommends" data security practices and requires companies to maintain

---

[159] *Wilkin v. Narachi*, 2018 WL 1100372, at *12 (Del. Ch. Feb. 28, 2018) ("Pleading violations of nonbinding recommendations does not constitute pleading a violation of positive law such that the board faces a substantial likelihood of liability and cannot consider demand.").

[160] Am. Compl. ¶¶ 58-63.

[161] *See Narachi*, 2018 WL 1100372, at *12 (finding demand not excused where the plaintiff listed various statutes and regulations but did not specify what law was violated because "[m]erely discussing these statutes in vague, broad terms does not support a finding that Director Defendants' decisions somehow violated these statutes"); *Desimone v. Barrow*, 924 A.2d 908, 928 (Del. Ch. 2007) ("I do not accept cursory contentions of wrongdoing as a substitute for the pleading of particularized facts. Mere notice pleading is insufficient to meet the plaintiff's burden to show demand excusal in a derivative case.").

[162] Pl.'s Answering Br. 41 n.18.

"reasonable" cybersecurity practices.[163] Whether the FTC expects PCI DSS standards or tokenization, however, does not change the fact that there are no allegations in the Complaint that the Post-Acquisition Board knew about the FTC's requirements or that Marriott was violating them. A *Caremark* claim requires that a plaintiff demonstrate scienter.[164] The plaintiff here has not.

In short, there is no known illegal conduct, lawbreaking, or violations of a regulatory mandate alleged in the Complaint that could support a finding that the Post-Acquisition Board faces a substantial likelihood of liability for failed oversight. That reality distinguishes this case from those relied upon by the plaintiff. In *Massey*, the plaintiffs pleaded "a myriad of particularized facts" demonstrating the board's knowledge of serious violations of mining safety laws and that the directors knowingly "caus[ed] [the company] to seek profit" through unlawful acts.[165] In

---

[163] Am. Compl. ¶¶ 57-59; Statement of the FTC, *FTC v. LifeLock* (Dec. 17, 2015) (explaining that "the reasonableness of security will depend on the facts and circumstances of each case").

[164] *E.g.*, *Hays v. Almeida*, 2019 WL 3389172, at *3 (Del. Ch. July 26, 2019) (ORDER) (rejecting the argument that directors faced oversight liability where "the complaint [did] not allege that the directors knew that Walgreens was violating the law or even engaging in the conduct that risked violating the law"); *Teamsters Local 443 Health Servs. & Ins. Plan v. Chou*, 2020 WL 5028065, at *16 (Del. Ch. Aug. 24, 2020) ("Because a *Caremark* claim must plead bad faith, 'a plaintiff must allege facts that allow a reasonable inference that the directors acted with scienter which, in turn, requires not only proof that a director acted inconsistently with his fiduciary duties, but also most importantly, that the director knew he was so acting.'" (quoting *Corbat*, 2017 WL 6452240, at *14)).

[165] *Massey*, 2011 WL 2176479, at *20.

Westmoreland, the United States Court of Appeals for the Seventh Circuit found that the plaintiffs pleaded particularized facts that the board "took no action to ensure the company's timely compliance with the law," despite the repeated warnings from the FDA—which were passed along to the board—that the company was in violation of FDA regulations.[166] And in *Abbott Labs*, the Seventh Circuit likewise found that a board's failure to rectify known, ongoing, and pervasive violations of FDA regulations could constitute bad faith and excuse demand.[167] The plaintiff in this action has not pleaded particularized facts that the Post-Acquisition Board knowingly permitted Marriott to violate the law.[168]

---

[166] *Westmoreland Cty. Emp. Ret. Sys. v. Parkinson*, 727 F.3d 719, 726-29 (7th Cir. 2013).

[167] *In re Abbott Lab'ys Deriv. S'holders Litig.*, 325 F.3d 795, 808-09 (7th Cir. 2003).

[168] In October 2020, the United Kingdom Information Commissioner's Office fined Marriott £18.4 million ($24.0 million) in connection with the cyberattack for violating the General Data Protection Regulation (GDPR). *See ICO Fines Marriott 18.4 Million Pounds for Failing to Secure Customer Data*, Reuters (Oct. 30, 2020); *see* Am. Compl. ¶¶ 164-65. The GDPR was adopted on April 14, 2016 and became enforceable on March 25, 2018. *See* GDPR, *supra* note 137. The GDPR requires, among other things, that customers handling European Union citizens' data implement reasonable data protection measures to protect consumers' personal data and privacy from loss or exposure. *See* GDPR Art. 5; Am. Compl. ¶ 62. The plaintiff alleges that "the defendants failed to comply with various provisions of the GDPR which required Marriott to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk." Am. Compl. ¶ 163. But the Complaint lacks any particularized facts suggesting that the Post-Acquisition Board intentionally violated the GDPR or knowingly permitted GDPR violations to continue unabated. There are no allegations suggesting that Marriott's directors "viewed themselves or [Marriott] as above the law." *Corbat*, 2017 WL 6452240, at *24 (explaining that alleged "failed" efforts "to comply with the wide range of laws and regulations that govern large financial institutions" are "not enough to support a plausible inference of bad faith" and that [b]ad results alone do not imply bad faith."); *In re Walt Disney Co. Deriv. Litig.*, 906 A.2d 27, 67 (Del. 2006) (noting that "a failure to act in good

ii. *No conscious disregard of "red flags"*

The plaintiff also contends that the Post-Acquisition Board faces a substantial risk of liability for ignoring several "red flags" about Starwood's inadequate data protection systems post-closing. Those "red flags" are not of illegality, as previously discussed.[169] The plaintiff does not allege that the directors were told, for example, that Starwood's standards ran afoul of regulatory or legal requirements. The so-called "red flags" were updates to the Board about aspects of Starwood's cybersecurity measures that needed improvement.[170]

The purported "red flags" the plaintiff focuses on are as follows. First, five members of the Demand Board learned at a February 8, 2017 Audit Committee meeting that Internal Audit rated Marriott as "Needs Improvement" for cybersecurity and that its "incident response plan [wa]s not up to date."[171] Second, the Board was told by Hoffmeister on February 10, 2017 that Starwood's data

---

faith may be shown . . . where the fiduciary acts with the intent to violate applicable positive law" or "where the fiduciary intentionally fails to act in the face of a known duty to act, demonstrating a conscious disregard for his duties" (citation omitted)). Although not briefed by the parties in any event, the ICO fine is not a basis to find that the Post-Acquisition Board faces a substantial likelihood of liability for a bad faith oversight violation.

[169] *See supra* Section II.B.2.b.i.

[170] *See Citigroup*, 964 A.2d at 124-26; *see infra* note 184.

[171] Am. Compl. ¶¶ 118-19.

security standards did not mandate PCI compliance or tokenization.[172] And third, PwC told the Board that Starwood's "[d]ecentralized technology management model" created a "greater opportunity for deviation from the expected published standard."[173] These "red flags" were effectively ignored, the plaintiff asserts, because the Board waited a year before taking up Starwood's information protection systems again.[174]

Even if the gaps in Starwood's data security evidenced the sort of compliance failure that could support a viable claim under the second prong of *Caremark*, the Complaint lacks particularized allegations that the Board consciously overlooked or failed to address them.[175] As the defendants point out, no "red flags" were deliberately disregarded.[176] Rather, management told the Board that it was addressing or would address the issues presented.[177]

At the same February 10, 2017 meeting where the Board learned about Starwood's PCI non-compliance, Hoffmeister reported there "would be efforts made

---

[172] *Id.* ¶ 124.

[173] *Id.*

[174] *Id.* ¶ 130; Defs.' Ex. 15 at 1386.

[175] *See Desimone*, 924 A.2d at 940 ("Delaware courts routinely reject the conclusory allegation that because illegal behavior occurred, internal controls must have been deficient, and the board must have known so.").

[176] Defs.' Opening Br. 39-40.

[177] Defs.' Reply Br. 15.

immediately to remedy" Starwood's lack of tokenization.[178] In addition, the presentation given to the Board confirmed that the Company had a plan in place to "consolidate Marriott + Starwood [s]ecurity."[179] The Board was also told about several recommendations that PwC had made to appropriately update Starwood's brand standards and detailed "Intended Actions" to address those recommendations.[180] These facts are not reflective of a board that has decided to turn a blind eye to potential corporate wrongdoing.[181]

Perhaps the entirety of Starwood's deficiencies were not addressed "immediately," as Hoffmeister told the Board they could be. And, with hindsight knowledge of the extent of the data breach, the implementation plan was probably too slow. It wasn't until the following year on February 9, 2018 that the Board was

---

[178] Am. Compl. ¶ 126.

[179] *Id.* ¶¶ 122, 124; Defs.' Ex. 14 at 1284-85.

[180] Am. Compl. ¶ 125.

[181] *See Corbat*, 2017 WL 6452240 at *17 (finding no substantial likelihood of liability for bad faith failed oversight where the board was presented with an action plan by management and outside advisors); *id.* at *22 (finding no particularized allegations of board inaction where the company "dealt with [a] red flag in a manner that cannot be said to reflect bad faith"); *Reiter*, 2016 WL 6081823, at *13 (declining to draw inference that directors knew they were breaching fiduciary duties by allowing corporate violations of law where "the same reports that described the Company's heightened compliance risk simultaneously explained to the directors in considerable detail on a regular basis the initiatives management was taking to address those problems and to ameliorate . . . compliance risk").

next updated about those migration efforts.[182] But, the plaintiff does not allege that the full Board had any reason to suspect that management was not promptly acting on PwC's recommendations.[183] As the documents incorporated into the Complaint confirm, management had "enhance[ed] monitoring," "[e]xpand[ed] enterprise security logging and event management," and "[e]xpand[ed] the use of third party monitoring" among other numerous actions between February 2017 and 2018.[184] An attempted yet failed remediation effort generally cannot implicate bad faith.[185]

Finally, the plaintiff asserts that the Post-Acquisition Board is exposed to *Caremark* liability for its failure to immediately discontinue use of the Starwood guest reservation system after learning, in September 2018, that it was infected with

---

[182] *Id.* at 1366, 1386 (Oberg's Enterprise Risk Assessment presentation, detailing a detailed "Cybersecurity Risk Scorecard" that described current risk mitigation efforts and tracked performance, including the anticipated "[m]igration of Starwood systems to the Marriott established technology standards" for end user devices by September 2019).

[183] *See Horman*, 2017 WL 242571, at *13 ("Delaware courts have consistently rejected . . . the inference that directors must have known about a problem because someone was supposed to tell them about it." (quoting *Cottrell v. Duke*, 829 F.3d 983, 995 (8th Cir. 2016) (alteration in original))).

[184] Defs.' Ex. 30 at 1372.

[185] *See Richardson v. Clark*, 2020 WL 7861335, at *11 (Del. Ch. Dec. 31, 2020); *see also Jacobs*, 2016 WL 4076369, at *9 ("Simply alleging that a board incorrectly exercised its business judgment and made a 'wrong' decision in response to red flags . . . is not enough to plead bad faith."); *Home Depot*, 223 F. Supp. 3d at 1326-27 (finding no substantial likelihood of liability for *Caremark* violation based on allegation that implementation to remedy deficiency in company's data security was not completed fast enough where allegations did not demonstrate bad faith).

malware that could allow attackers to access customer data.[186] The plaintiff does not allege that the Board learned on September 17, 2018 that an immediate shutdown of the system was necessary to protect consumer data but chose to continue its use nonetheless. According to the Complaint, Marriott did not learn about the extent of the breach and that customer data had been accessed until November 2018.[187] The Complaint and documents incorporated into it demonstrate that the Board continued to receive detailed updates on the "incredible amount of work" management and forensic specialists performed throughout November 2018 to investigate and address the problem.[188] There are no facts pleaded to suggest that the directors' ignorance on the extent of the breach in September 2018 is the result of a breach of fiduciary duty.[189] The plaintiff has therefore failed to demonstrate that a majority of the Demand Board faces a substantial likelihood of liability for consciously disregarding "red flags."

---

[186] Pl.'s Answering Br. 13-14, 37.

[187] Am. Compl. ¶¶ 139-41.

[188] Defs.' Ex. 21 at 1946-47; Defs.' Exs. 25-27.

[189] *See Horman*, 2017 WL 242571, at *15 (explaining that the size of the ultimate harm is "not a sufficient basis on which to rest liability" absent facts showing a "board's ignorance can only be explained by a breach of fiduciary duty" (quoting *David B. Shaev Profit Sharing Acct. v. Armstrong*, 2006 WL 391931, at *6 (Del. Ch. Feb. 13, 2006)).

iii. *Notification Requirements Regarding the Breach*

The plaintiff's final theory of liability for the Demand Board is another variation of alleged failure to comply with positive law—this time, based on the timing of Marriott's disclosure of the data breach. The plaintiff contends that Marriott was "required by various state laws to expeditiously disclose the data breach" and that the Board "knew they were required by their fiduciary duties to cause Marriott to disclose this information" in compliance with those laws.[190] By not alerting the public about the incident until November 30, 2018—despite the Board first learning of malware on September 18, 2018—the plaintiff alleges that notification laws were violated.

The plaintiff's argument suffers from many of the same flaws as those regarding PCI DSS and tokenization. To start, the plaintiff does not allege that the directors were informed about the applicable notification laws. Directors cannot be liable under the second prong of *Caremark* for legal violations that they did not know about.[191]

Of the notification laws of 31 states and territories that the plaintiff asserts were violated by Marriott's "83-day delay" in notifying individuals affected by the

[190] Pl.'s Answering Br. 55.

[191] *See Horman*, 2017 WL 242571, at *11 (explaining that directors are liable if they "become aware of the red flags and do nothing in response").

breach,[192] only three statutes—of Delaware, Maryland, and Michigan—are addressed in the parties' briefs. Those laws each concern notification requirements in the event of the disclosure of personal data.[193] Maryland's Personal Information Privacy Act requires a business that has discovered or has been notified of a security breach to conduct a prompt investigation to determine if "Personal Information" has or will be misused.[194] If it has, the business is required to notify the affected individuals "as soon as reasonably practicable."[195] Michigan's notification law likewise defines a "security breach" as the "unauthorized access and acquisition of data that compromises the security or confidentiality of personal information."[196]

---

[192] Am. Compl. ¶ 172.

[193] At argument, the plaintiff explained that it focused on Maryland and Michigan because those states' notification laws were selected as bellwether claims in the Federal Action and on Delaware given the action in this court. *See* Reargument Hr'g Tr.; Pl.'s Answering Br. 56 n.26; Defs.' Opening Br. 49-50; Defs.' Reply Br. 21 n.8.

[194] Md. Code Ann., Com. Law § 14-3504(b)(1) (West 2021). "Personal Information" is defined to include:

> An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: . . . a passport number . . . [a]n account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account.

Id. § 14-3501(e)(1)(i).

[195] *Id.* §§ 14-3504(b)(2), 14-3504(c)(2).

[196] Mich. Comp. Laws Ann. § 445.63(b) (West 2021). "Personal information" is defined to include:

Delaware's Consumer Security Breach Act also requires notification "without unreasonable delay" when a resident's "personal information was breached or is reasonably believed to have been breached."[197]

The plaintiff points to the fact that consumer class action claims based on the Maryland and Michigan notification statutes survived a motion to dismiss in the Federal Action as a basis for finding liability here.[198] Those claims were not, however, brought against the members of the Demand Board and cannot implicate their liability.[199] Under the heightened pleading standards of Rule 23.1, the lack of particularized allegations indicating that the directors consciously disregarded or intentionally violated positive law is dispositive.

> [T]he first name or first initial and last name linked to 1 or more of the following data elements of a resident of this state: (i) Social security number[;] (ii) Driver license number or state personal identification card number[;] (iii) Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts.

Id. § 445.63(r).

[197] 6 *Del. C.* § 12B-102(a).

[198] *Marriott*, 440 F. Supp. 3d at 487, 490.

[199] *See generally id. Cf. Pfeiffer v. Toll*, 989 A.2d 683, 690 (Del. Ch. 2010), *abrogated on other grounds by Kahn v. Kohlberg Kravis Roberts & Co. L.P.*, 23 A.3d 831 (Del. 2011) (finding demand futile based, in part, on federal court decision holding that the same individual defendants acted with scienter regarding "the same trades at issue" in the Delaware action).

Regardless, there are no allegations that the Board *knew* personal data was accessed such that the notification obligations had been triggered prior to November 2018.[200] The plaintiff suggests that it "strains credulity" to conclude the Board did not know personal information was accessed given the severity of the breach.[201] But as the defendants point out, discovering malware is not the same as discovering that personal information has been accessed.[202] The Complaint plainly states that Marriott first discovered that "customers' personal information" was potentially accessed on November 19, 2018.[203] Marriott's notification of interested parties 10 days later and public announcement of its investigatory findings on the eleventh day are not obvious violations of notification laws that suggest bad faith on the part of the Board.[204]

---

[200] *See supra* note 164 (discussing the scienter requirement for an oversight claim).

[201] Pl.'s Answering Br. 57.

[202] Am. Compl. ¶¶ 140, 217; Defs.' Reply Br. 20.

[203] Am. Compl. ¶ 140.

[204] *Id.* ¶¶ 142-43. The plaintiff originally argued that the members of the Audit Committee face a substantial likelihood of liability for issuing a Form 10-Q on November 6, 2018 that "remained silent as to the Breach." *Id.* ¶¶ 139, 248; Pl.'s Answering Br. 56. After the District Court in the Federal Action dismissed securities law claims for allegedly false and misleading disclosures with prejudice, the plaintiff here determined not to press its disclosure claims. *See* Mot. to Dismiss Hr'g Tr. 59. Had they not, the claim likely would have failed because the plaintiff does not ascribe any bad faith actions or motives to the Audit Committee members who approved the Form 10-Q. The claim would, at most, implicate the directors' "'erroneous judgment' concerning the proper scope and content of the disclosure." *Orman v. Cullman*, 794 A.2d 5, 41 (Del. Ch. 2002) (quoting *Crescent/Mach I P'rs, L.P. v. Turner*, 846 A.2d 963, 987 (Del. Ch. 2000)); *see also*

* * *

The data breach that is at the center of this case was momentous in scale and put the data of hundreds of millions of people at risk. Critically, however, 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. One could argue that the Complaint depicts a preventable scenario because the directors did not respond to internal reports about inadequate data security risks as swiftly as they might have. But the difference between a flawed effort and a deliberate failure to act is one of extent and intent. A *Caremark* violation requires a plaintiff to demonstrate the latter.

Here, the Complaint lacks particularized allegations demonstrating that the Post-Acquisition Board knew that the vulnerabilities in Starwood's data system ran afoul of the law, that it nonetheless chose not to address them, or that it scorned legal notification requirements. Having failed to show that those directors consciously disregarded positive law or acted in bad faith, the plaintiff has not impugned the ability of any member of the Demand Board to impartially consider a demand based on a substantial likelihood of liability for failed oversight.

Morrison v. Berry, 2019 WL 7369431, at *18 (Del. Ch. Dec. 31, 2019) ("Bad faith, in the context of omissions, requires that the omission be intentional and constitute more than an error of judgment or gross negligence.").

III. CONCLUSION

The plaintiff failed to allege particularized facts that could support a finding that any member of the Demand Board faced a substantial likelihood of liability on a non-exculpated claim. Any claim based on pre-Acquisition due diligence is time barred. The remaining claims are unsupported by particularized allegations demonstrating that the Post-Acquisition Board acted in bad faith with regard to cybersecurity oversight, compliance, or notification of the data breach. As a result, a demand made on the Demand Board would not have been futile with respect to the plaintiff's breach of fiduciary duty claim. The defendants' Motion to Dismiss is granted and the Complaint is dismissed pursuant to Court of Chancery Rule 23.1.