Florida Law Review

Volume 74 | Issue 1 Article 4

January 2022

The Writing on the [Fire] Wall: "Mission Critical" Cybersecurity Derivative Litigation is on Delaware's Horizon

E. Paige Williams

THE WRITING ON THE [FIRE]WALL: "MISSION CRITICAL" CYBERSECURITY DERIVATIVE LITIGATION IS ON DELAWARE'S HORIZON

E. Paige Williams[*]

Abstract

The impact of the information economy during the last quarter century has been dramatic. But for all its glory, the information economy also presents vulnerabilities: a cybersecurity breach can materially affect firm value. Although some security breaches may be inevitable in the modern world, courts are increasingly considering the question of whether the corporation's directors and officers may be held liable under the theory that they acted in bad faith in their oversight of the corporation's cybersecurity. To date, no suit has survived a motion to dismiss but several have settled for sizeable amounts. A watershed decision from the Delaware Supreme Court and a series of chancery court decisions may provide the opening plaintiffs' lawyers have been looking for. With an unmatched data breach in SolarWinds, the writing is on the [fire]wall: Delaware corporations should brace themselves for "mission critical" cybersecurity derivative litigation.

INTRODUCTION 170

I. OVERSIGHT DUTIES: THE LEGAL FRAMEWORK 172

II. CYBERSECURITY OVERSIGHT: EFFORTS TO DATE 176
A. *The Demand Requirement and Wyndham Worldwide* 179
B. *The Business Judgment Rule and Home Depot* 180
C. *Unique Challenges to Cybersecurity Oversight Liability* 182

III. RECENT DEVELOPMENTS IN DELAWARE LAW 186
A. *"Mission Critical" Debuts in Delaware* 186
B. *"More Rigorously Exercised" Oversight Under Prong Two* 189
C. *A Choice Not to Invoke "Mission Critical"?* 191

* J.D. candidate 2022, University of Florida Levin College of Law; B.A. 2019, Washington and Lee University. I owe a huge debt of gratitude to my peers and friends on the *Florida Law Review* for their hard work and commitment to preparing this Note for publication. Many thanks are also due to the ultimate friend, Julie Zolty: this Note's publication would not have been possible without her tireless efforts. I dedicate this Note to my father, my late mother, Caleb Knight, and Beesly, the dog who was there for every word I wrote.

D. *"Mission Critical" in Complex Corporations*.....194
E. *Implications*.....197

IV. SOLARWINDS: CYBERSECURITY AS "MISSION CRITICAL".....198

CONCLUSION.....203

INTRODUCTION

In December 2020, SolarWinds Corporation—a Delaware company which creates and sells network-management tools to help its customers monitor outages, slowdowns, and security breaches—notified 33,000 of its customers that its top product, Orion, had been compromised.[1] Orion, which accounts for 45% of SolarWinds's revenue,[2] offers a one-stop shop for managing and monitoring information technology (IT) systems.[3] The program is utilized by federal agencies, private companies, and Fortune 500 businesses.[4] Hackers were able to exploit Orion's comprehensive access to SolarWinds's clients' networks by altering a software update that the company began rolling out to clients' computers between March and June of 2020.[5] Exactly how the hackers were able to achieve this feat has yet to be confirmed by SolarWinds, but cybersecurity experts are sounding the alarm, calling the attack "the most consequential cyber espionage campaign to date."[6] SolarWinds's market capitalization hovered around $7.3 billion the week before the announcement was

1. SolarWinds Corp., Current Report (Form 8-K) (Dec. 14, 2020), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/57108215-4458-4dd8-a5bf-55bd5e34d451.pdf [https://perma.cc/RN4D-77QB]. SolarWinds did not catch the breach themselves. They were instead notified by one of their customers, FireEye—now Mandiant—that they had been breached. *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor*, MANDIANT (Dec. 13, 2020), https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor [https://perma.cc/6L7Y-Y75J].

2. SolarWinds Corp., *supra* note 1.

3. *Orion Platform*, SOLARWINDS, https://www.SolarWinds.com/orion-platform [https://perma.cc/LVK8-QTXG].

4. Mia Jankowicz & Charles Davis, *These Big Firms and US Agencies All Use Software from the Company Breached in a Massive Hack Being Blamed on Russia*, BUS. INSIDER (Dec. 15, 2020, 9:45 AM), https://markets.businessinsider.com/news/stocks/list-of-companies-agencies-at-risk-after-solarwinds-hack-2020-12 [https://perma.cc/W3YQ-VBVF] (listing the Secret Service, the Department of Defense, the State Department, the Federal Reserve, and the National Security Agency among the agencies impacted by the breach).

5. SolarWinds Corp., *supra* note 1.

6. Hannah Murphy et al., *The Great Hack Attack: SolarWinds Breach Exposes Big Gaps in Cybersecurity*, FIN. TIMES (Dec. 18, 2020), https://www.ft.com/content/c13dbb51-907b-4db7-8347-30921ef931c2 [https://perma.cc/CMS6-CPU5] (quoting Dmitri Alperovitch, the co-founder of Crowdstrike, a cybersecurity group).

made; the week after the announcement, the company saw a nearly $3 billion drop to a trough of $4.45 billion on December 18.[7]

"The ascendancy and impact of the information economy during the last quarter century have been dramatic and unprecedented."[8] But for all its glory, the information economy also presents vulnerabilities: a cybersecurity breach can materially affect firm value for capital investors, long term and short term.[9] For another example, the Equifax data breach—which exposed approximately 143 million U.S. consumers' personal information[10]—caused a $6 billion loss of market capitalization.[11] In 2019, Moody's downgraded Equifax's outlook rating from "stable" to a "negative" due to the breach, and the credit rating agency has continued to cite the breach in its reports.[12]

Although some security breaches may be inevitable in the modern world, courts are increasingly considering the question of whether a corporation's directors and officers may be held liable under the theory that they acted in bad faith in overseeing the corporation's cybersecurity.[13] This takes the form of a derivative suit,[14] which is a suit

---

7. *SolarWinds Market Cap*, YCHARTS, https://ycharts.com/companies/SWI/market_cap [https://perma.cc/N9PL-D8YF]. Some industry leaders are suggesting insider trading may have occurred prior to the announcement as over $280 million in securities were sold by longtime institutional investors six days prior to the announcement. Drew Harwell & Douglas MacMillan, *Investors in Breached Software Firm SolarWinds Traded $280 Million in Stock Days Before Hack Was Revealed*, WASH. POST (Dec. 15, 2020, 11:41 PM), https://www.washingtonpost.com /technology /2020/12/15/SolarWinds-russia-breach-stock-trades/ [https://perma.cc/LJG9-7B6R].

8. Joshua Mitts & Eric Talley, *Informed Trading and Cybersecurity Breaches*, 9 HARV. BUS. L. REV. 1, 2 (2019).

9. *See generally* Georgios Spanos & Lefteris Angelis, *The Impact of Information Security Events to the Stock Market: A Systematic Literature Review*, 58 COMPUT. & SEC. 216 (2016) (analyzing thirty-seven papers and finding 75.6% of the studies measure statistically significant stock price reactions to the disclosure of data breaches).

10. Press Release, Equifax, Equifax Announces Cybersecurity Incident Involving Consumer Information (Sept. 7, 2017), https://investor.equifax.com/news-events/press-releases/detail/240/equifax-announces-cybersecurity-incident-involving-consumer [https://perma.cc/BG 8W-WL ZB].

11. AnnaMaria Andriotis et al., *"We've Been Breached": Inside the Equifax Hack*, WALL ST. J. (Sept. 18, 2017, 8:04 AM), https://www.wsj.com/articles/weve-beenbreached-inside-the-equifax-hack-1505693318 [https://perma.cc/Q8XJ-N2X7].

12. *See* Scott Kannry, *Bite, Not Bark: Moody's Downgrades Equifax on Cybersecurity Concerns*, AXIO (June 5, 2019), https://axio.com/insights/moodys-downgrades-equifax-cybersecurity/ [https://perma.cc/39R7-EL2Z]; *Rating Action: Moody's Downgrades Equifax Senior Unsecured to Baa2; Outlook Stable*, MOODY'S (Apr. 16, 2020), https://www.moodys.com/research/Moodys-downgrades-Equifax-senior-unsecured-to-Baa2-outlook-stable--PR_422690 [https://perma.cc/5DPF-ERJZ] ("Equifax's critical role in consumer finance, its possession of large amounts of private consumer data and the lingering damage to its reputation from the 2017 data breach leave it exposed to high regulatory and information security risks.").

13. Benjamin P. Edwards, *Cybersecurity Oversight Liability*, 35 GA. ST. U. L. REV. 663, 665 (2019).

14. *Id.*

against third parties—usually officers and directors—"brought by a shareholder on behalf of the corporation in which she holds stock."[15] Derivative suits typically concern alleged breaches of fiduciary duty to the corporation by directors or officers, with any recovery running to the shareholders pro rata.[16] Derivative suits "constitute an important corporate accountability mechanism because they alone target specific instances of managerial misconduct" against the corporation and aim to protect the shareholders from mismanagement.[17]

This Note will contribute to the broader conversation on cybersecurity through the narrow lens of derivative lawsuits in Delaware. It evaluates a recently introduced twist on the breach of the fiduciary duty of oversight when such a breach implicates "mission critical" aspects of the business.[18] This Note applies the new framework to the context of data breaches and argues that Delaware courts are ripe for such a claim.

Part I discusses shareholder derivative suits generally. Part II analyzes the hurdles that have halted cybersecurity oversight liability claims in the past and identifies challenges unique to cybersecurity oversight liability. In Part III, the Author discusses new Delaware case law that signals a slight but important change in the tides of *Caremark* claims; namely, that when courts apply the *Caremark* framework, their analysis will be informed by the notion found in recent Delaware Supreme Court decision *Marchand v. Barnhill*[19] that where a company's "mission critical" functions are subject to regulation,[20] "the board's oversight function must be *more rigorously* exercised."[21] Part IV analyzes the SolarWinds breach with *Marchand* in mind and concludes that the SolarWinds breach may demonstrate the possibility of such a watershed case for cybersecurity oversight liability that Delaware case law has been inching towards.

I. OVERSIGHT DUTIES: THE LEGAL FRAMEWORK

Scholars have identified four categories of litigation that might follow a data breach: (1) shareholder derivative suits; (2) securities fraud class actions; (3) class action lawsuits by the company's outside customers or business partners whose information was compromised; or (4) administrative agencies' enforcement actions under applicable state or

15. JEFFREY BAUMAN ET AL., BUSINESS ORGANIZATIONS LAW AND POLICY 663 (9th ed. 2017).

16. *Id.* at 663–64.

17. *Id.* at 663.

18. Marchand v. Barnhill, 212 A.3d 805, 824 (2019) (en banc).

19. 212 A.3d 805 (2019) (en banc).

20. *Id.* at 824.

21. *In re* Clovis Oncology, Inc. Derivative Litig., No. 2017-0222, 2019 WL 4850188, at *13 (Del. Ch. Oct. 1, 2019) (emphasis added).

federal laws.[22] After a data breach, a company might experience one or several of such actions; for example, Target was sued both by its shareholders and by a class of customers whose data was compromised.[23]

Shareholder derivative suits that have been brought against Delaware[24] corporations following a cybersecurity incident are often brought as claims that the directors breached their fiduciary duty of loyalty by failing to monitor the corporation.[25] The legal framework and pleading requirements of a successful derivative claim based on the duty to monitor[26] are notoriously difficult for plaintiff-shareholders to meet.[27] Indeed, Chancellor William Burton Chandler III remarked that such a claim is "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment."[28] These claims are referred to

22. *See* Michael Hooker & Jason Pill, *You've Been Hacked, and Now You're Being Sued: The Developing World of Cybersecurity Litigation*, 90 FLA. B.J. 30, 31 (2016) (describing the main categories of cybersecurity litigation).

23. *See* Consumer Plaintiffs' Consolidated Class Action Complaint, *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304 (D. Minn. 2014); Kevin M. LaCroix, *Target Directors and Officers Hit with Derivative Suits Based on Data Breach*, D&O DIARY (Feb. 3, 2014), https://www.dandodiary.com/2014/02/articles/cyber-liability/target-directors-and-officers-hit-with-derivative-suits-based-on-data-breach/ [https://perma.cc/F8KM-VDBA].

24. As discussed above, this Note focuses on Delaware, but it is worth noting that the Model Business Corporation Act (MBCA) and other states take similar, if slightly different, approaches as compared to Delaware. For example, the drafters of the MBCA said a director may be held liable if he engaged in sustained inattention "when particular facts and circumstances of significant concern materialize that would alert a reasonably attentive director to the need for such inquiry." MODEL BUS. CORP. ACT § 8.31(a)(2)(iv) (AM. BAR. ASS'N 2016); *see also id.* § 8.31(a)(2)(iv) cmt. E (stating that the failure to exercise oversight can be characterized as "abdication and continued neglect by a director to devote attention, not a brief distraction or temporary interruption"). The MBCA is also similar to the Delaware code with respect to the director exculpation statute, allowing a charter provision designed to eliminate director liability except for "an intentional infliction of harm on the corporation or the shareholders." *Id.* § 2.02(b)(4)(ii).

25. *See, e.g.*, Plaintiffs' Memorandum of Law in Opposition to Defendants' Motion to Dismiss at 1, *In re* The Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317 (N.D. Ga. 2016) (No. 1:15-CV-2999), ECF No. 52 (blaming "[the board's] conscious failure to institute internal controls sufficient to oversee the risks HD faced in the event of a breach").

26. The various directors' and officers' fiduciary duties to shareholders are not easily demarcated. Indeed, some argue that the duty to monitor is, to an extent, really a duty of care violation. *See* Julian Velasco, *How Many Fiduciary Duties Are There in Corporate Law?*, 83 S. CAL. L. REV. 1231, 1281 (2010). Regardless, a breach of the duty of oversight was reimagined by the Delaware court as based on the duty of loyalty because proving a breach of the duty required a showing of bad faith. *See* Stone *ex rel.* AmSouth Bancorporation v. Ritter, 911 A.2d 362, 370 (Del. 2006).

27. *See In re* Merrill Lynch & Co., 773 F. Supp. 2d 330, 345 (S.D.N.Y. 2011) (noting that "few, if any, plaintiffs surmount this obstacle"); *In re* The Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317, 1325 (N.D. Ga. 2016) ("This is an incredibly high hurdle for the Plaintiffs to overcome, and it is not surprising that they fail to do so."). The pleading requirements are discussed in detail in Part II.

28. *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 967 (Del. Ch. 1996).

as *Caremark* claims, referring to *In re Caremark International Inc. Derivative Litigation*,[29] in which the Delaware Supreme Court originally recognized failure to monitor as an available claim that shareholders might bring in the wake of directorial mismanagement.[30]

In *Caremark*, plaintiff-shareholders sued derivatively, claiming that the members of Caremark's board of directors breached their fiduciary duty of care to Caremark by failing to assure compliance with "federal and state laws and regulations applicable to health care providers."[31] Due to Caremark's regulatory compliance failures, the U.S. Department of Health and Human Services and the Department of Justice investigated the company for four years.[32] Consequentially, in 1994, Caremark was charged in an indictment with multiple felonies.[33] Caremark pleaded guilty to mail fraud and agreed to pay civil and criminal fines.[34] In all, Caremark was required to make payments of $250 million.[35]

Chancellor Chandler explained that liability to the corporation may arise in two distinct contexts: from a board decision that results in a loss or an unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss.[36] In order to recover in the second context, plaintiffs would have to prove "either (1) that the directors knew or (2) should have known that violations of law were occurring and, in either event, (3) that the directors took no steps in a good faith effort to prevent or remedy that situation."[37] In order to establish a sufficient lack of good faith to impute liability, the plaintiff must prove there was a "lack of good faith as evidenced by sustained or systematic failure of a director to exercise reasonable oversight."[38]

Caremark and its progeny, in essence, merely require the board to set up and monitor a rationally designed reporting system. Liability will be found if: "(a) the directors utterly failed to implement any reporting or information system or controls; or (b) having implemented such a system

29. 698 A.2d 959 (Del. Ch. 1996).

30. *Id.* at 971. Note that the duty to monitor was reimagined by the Delaware court as based on the duty of loyalty, not the duty of care, because proving a breach of the duty required a showing of bad faith. *See Stone*, 911 A.2d at 369–70.

31. *Caremark*, 698 A.2d at 960.

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id.* at 960–61. The case came before the court upon a proposal for settlement wherein the court must "assess the strengths and weaknesses of the claims asserted in light of the discovery record and to evaluate the fairness and adequacy of the consideration offered to the corporation in exchange for the release of all claims made." *Id.* at 961. The court held that the settlement was fair and that the "very modest" amount of recovery was appropriate given the weakness of the plaintiffs' claims. *Id.* at 972.

36. *Id.* at 967.

37. *Id.* at 971.

38. *Id.*

or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."[39] Courts sometimes refer to these as "prong one" and "prong two" of the *Caremark* framework.[40] For ease of analysis, this Note will do the same.

To state a claim under prong one, plaintiffs must plead that the defendants "failed to make the required good faith effort to put a reasonable compliance and reporting system in place."[41] Courts do not require omniscience by the board;[42] instead, the idea is that there is a bottom-line requirement that it make a "good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention."[43] Thus, directors have great discretion to design context- and industry-specific monitoring systems "tailored to their companies' businesses and resources."[44] This is likely because the court has said that "the level of detail that is appropriate for such an information system is a question of business judgment."[45]

To state a claim under prong two, plaintiffs must plead that a "red flag" of noncompliance was waved before the defendants, but they chose to ignore it.[46] However, "red flags are only useful when they are either [waved] in one's face or displayed so that they are visible to the careful observer."[47] In response to the red flags, directors may pursue any course

39. Stone *ex rel.* AmSouth Bancorporation v. Ritter, 911 A.2d 362, 370 (Del. 2006) (emphasis omitted).

40. *See* Teamsters Loc. 443 Health Servs. & Ins. Plan v. Chou, No. 2019-0816, 2020 WL 5028065, at *26 (Del. Ch. Aug. 24, 2020).

41. Marchand v. Barnhill, 212 A.3d 805, 821 (2019) (en banc) (citing *Stone*, 911 A.2d at 370).

42. Hughes v. Hu, No. 2019-0112, 2020 WL 1987029, at *14 (Del. Ch. Apr. 27, 2020); *Caremark*, 698 A.2d at 971 ("But, of course, the duty to act in good faith to be informed cannot be thought to require directors to possess detailed information about all aspects of the operation of the enterprise. Such a requirement would simpl[y] be inconsistent with the scale and scope of efficient organization size in this technological age.").

43. *Caremark*, 698 A.2d at 970; *see also Stone*, 911 A.2d at 370, 372–73 (finding that a board was shielded from liability because oversight was "delegated to certain employees" and the board "rel[ied] on periodic reports" from those employees).

44. *Marchand*, 212 A.3d at 821.

45. *Caremark*, 698 A.2d at 970. "Business decision-makers must operate in the real world, with imperfect information, limited resources, and an uncertain future. To impose liability on directors for making a 'wrong' business decision would cripple their ability to earn returns for investors by taking business risks." *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 126 (Del. Ch. 2009).

46. *In re* Clovis Oncology, Inc. Derivative Litig., No. 2017-0222, 2019 WL 4850188, at *13 (Del. Ch. Oct. 1, 2019).

47. *Id.* (quoting Wood v. Baum, 953 A.2d 136, 143 (Del. 2008)). As *Marchand* will later make clear, the careful observer is one whose gaze is fixed on the company's mission critical regulatory issues. *See* discussion *infra* Section III.B.

of action that is reasonable and, as always, in good faith;[48] "[s]imply alleging that a board incorrectly exercised its business judgment and made a 'wrong' decision in response to red flags, however, is insufficient to plead bad faith."[49]

It is worth highlighting that the Delaware Supreme Court later determined that *Caremark* claims find their basis within the directors' duty to act in good faith, which is a subset of the duty of loyalty, not the duty of care.[50] "Where directors fail to act in the face of a known duty to act, thereby demonstrating a conscious disregard for their responsibilities, they breach their duty of loyalty by failing to discharge that fiduciary obligation in good faith."[51] Thus, *Caremark* has been reimagined as a duty of loyalty claim, meaning, a plaintiff must prove bad faith on the part of the defendant to impose liability.[52] As a result, to succeed on such a claim of failure of oversight, the plaintiff must show that the defendants either "*knew* they were not discharging their fiduciary obligations or that the directors demonstrated a *conscious* disregard for their responsibilities such as by failing to act in the face of a known duty to act"[53] in order to establish "the lack of good faith that is a necessary condition to liability."[54] This is significant in light of Delaware's director exculpation statute, which allows a corporation to limit or eliminate directors' personal liability for duty of care violations, but not for duty of loyalty violations.[55] In other words, directors can be held personally liable for successful *Caremark* claims. The threat of a judicial finding of bad faith has downstream impacts, including settlement incentives.[56]

II. CYBERSECURITY OVERSIGHT: EFFORTS TO DATE

Corporate law scholars debate the true impact of the *Caremark* progeny, some arguing it promises much more than it can deliver, others arguing it has the desired impact.[57] Regardless of the debatable elements

48. Lyondell Chem. Co. v. Ryan, 970 A.2d 235, 243 (Del. 2009) ("Directors' decisions must be reasonable, not perfect.").

49. Melbourne Mun. Firefighters' Pension Tr. Fund *ex rel.* Qualcomm, Inc. v. Jacobs, No. 10872, 2016 WL 4076369, at *9 (Del. Ch. Aug. 1, 2016), *aff'd*, 158 A.3d 449 (Del. 2017).

50. *Citigroup*, 964 A.2d at 122–23 (citing Stone *ex rel.* AmSouth Bancorporation v. Ritter, 911 A.2d 362, 370 (Del. 2006)).

51. *Stone*, 911 A.2d at 370 (footnote omitted).

52. *Id.*

53. *Citigroup*, 964 A.2d at 123.

54. *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 971 (Del. Ch. 1996).

55. DEL. CODE ANN. tit. 8, § 102(b)(7) (2021).

56. *See infra* note 58 and accompanying text.

57. *Compare* Lisa M. Fairfax, *Managing Expectations: Does the Directors' Duty to Monitor Promise More Than It Can Deliver?*, 10 U. ST. THOMAS L.J. 416, 418 (2012) (questioning whether reliance on oversight offers false hope for those seeking to enhance corporate governance

of the impact, "cases continue to be brought and judges continue to evaluate the claims seriously."[58] It is unsurprising then that in the cybersecurity incident context, no director has, as of this writing, been found liable under *Caremark*, and no suit has survived a motion to dismiss.[59] However, the claims continue to be brought, and industry leaders are sounding the alarm for directors and officers to pay attention to this budding area of potential liability.[60]

The reason for the continued filing of claims despite a lack of success may be that, even though courts appear loath to entertain these *Caremark* arguments, derivative actions in the cybersecurity context are settling with enough frequency to gain attention, and for increasing amounts. Following a breach that impacted more than 1,000 of its fast food locations through their cash registers,[61] a group of Wendy's shareholders brought suit derivatively against the corporation, arguing that the directors and officers "breached their duties of loyalty, care and good faith" by "failing to implement and enforce a system of effective internal controls and procedures with respect to data security."[62] The suit settled

---

and prevent corporate misconduct), *with* Todd Haugh, Caremark*'s Behavioral Legacy*, 90 TEMP. L. REV. 611, 612–13 (2018) (arguing Caremark's legal legacy is underwhelming but its behavioral impact is meaningful).

58. Ezra Wasserman Mitchell, Caremark*'s Hidden Promise*, 51 LOY. L.A. L. REV. 239, 242 n.4 (2018). This may have to do with the strong incentive structure for attorneys to bring claims. *See In re* Fuqua Indus., Inc. S'holder Litig., 752 A.2d 126, 133 (Del. Ch. 1999). Because plaintiffs do not recover individually for losses, there is generally a low incentive for plaintiffs to bring claims under a derivative suit; instead, corporate statutes include strong incentives for plaintiff's *lawyers* to bring the claims because their fees are paid through settlements or court. *Id.* ("Through the use of cost and fee shifting mechanisms, private attorneys are economically incentivized to perform this service on behalf of shareholders.").

59. "In fact, no derivative actions . . . in the context of cybersecurity have survived a motion to dismiss." Harris Yegelwel, *Cybersecurity Oversight: A Cautionary Tale for Directors*, 20 J. TECH. L. & POL'Y 233, 246 (2015); Reply Memorandum in Further Support of Defendants' Motion to Dismiss the Verified Consolidated Shareholder Derivative Complaint at 6, *In re* The Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317 (N.D. Ga. 2016) (No. 15-CV-2999), ECF No. 55; *see also, e.g.*, *In re* Heartland Payment Sys., Inc. Sec. Litig., No. 09-1043, 2009 WL 4798148, at *1 (D.N.J. Dec. 7, 2009) (granting motion to dismiss); Palkon v. Holmes, No. 2:14-CV-01234, 2014 WL 5341880, at *1 (D.N.J. Oct. 20, 2014) (same).

60. *See* Yegelwel, *supra* note 59, at 263; Kevin M. LaCroix, *Target Corporation Cybersecurity-Related Derivative Litigation Dismissed*, D&O DIARY (July 9, 2016), https://www.dandodiary.com/2016/07/articles/cyberliability/target-corporation-cybersecurity-related-derivative-litigation-dismissed/ [https://perma.cc/TXY5-AWUV] ("For some time now, many commentators, including me, have been predicting that cybersecurity-related litigation could become an important part of the D&O litigation environment.").

61. Billy Steele, *Wendy's Says over 1,000 Locations Affected by Credit Card Breach*, ENGADGET (July 8, 2016), https://www.engadget.com/2016-07-08-wendys-malware-credit-card-data-breach.html [https://perma.cc/L9YF-XEK7].

62. Verified Shareholder Derivative Complaint ¶ 9, Graham v. Peltz, No. 16-cv-1153 (S.D. Ohio Dec. 16, 2016).

for "new policies and a $950,000 attorneys' fees deal."[63] In July 2016, Yahoo announced it was subject to two breaches that may have exposed all three billion of Yahoo's customers' information.[64] The incident not only was the biggest exposure of data seen yet in its day, but it forced the company to renegotiate its recent buyout with Verizon, reducing the amount by $350 million.[65] Yahoo shareholders brought suit derivatively, alleging Yahoo leadership breached their fiduciary duty of oversight.[66] Yahoo settled with its shareholders for $29 million.[67] The massive data breach at credit-reporting agency Equifax exposed 143 million U.S. customers' names, Social Security numbers, birth dates, and addresses.[68] Some 209,000 credit card numbers were also exposed.[69] Derivative, securities fraud, and class action litigation ensued.[70] The derivative litigation settled in June 2020 for $32.5 million[71] and the securities litigation settled in February 2020 for $149 million.[72]

The difficulties associated with successfully bringing a *Caremark* claim in any context, much less the cybersecurity context, find their basis in two principles. First, *Caremark* claims have difficult pleading requirements. Second, *Caremark* claims are substantively difficult to prove because of the business judgment rule. The following examples demonstrate these difficulties.

---

63. Kat Greene, *Wendy's Strikes Deal in Data Breach Shareholder Row*, LAW360 (May 8, 2018, 10:21 PM), https://www.law360.com/articles/1040982/wendy-s-strikes-deal-in-data-breach-shareholder-row [https://perma.cc/5F98-88KX].

64. (Redacted)-Verified Amended Consolidated Shareholder Class Action and Derivative Complaint for Breach of Fiduciary Duties, Insider Trading, Unjust Enrichment, and Corporate Waste at 10, *In re* Yahoo! Inc. S'holder Litig., No. 17-CV-307054 (Cal. Super. Ct. Jan. 2, 2018).

65. *Id.* at 14, 63.

66. *Id.* at 5.

67. Kevin M. LaCroix, *Yahoo Data Breach-Related Derivative Suit Settled for $29 Million*, D&O DIARY (Jan. 21, 2019), https://www.dandodiary.com/2019/01/articles/cyber-liability/yahoo-data-breach-related-derivative-suit-settled-29-million/ [https://perma.cc/AT9J-UVCR].

68. Kevin M. LaCroix, *Equifax Data Breach-Related Securities Suit Settled for $149 Million*, D&O DIARY (Feb. 17, 2020), https://www.dandodiary.com/2020/02/articles/securities-litigation/equifax-data-breach-related-securities-suit-settled-for-149-million/ [https://perma.cc/Y8ZY-E5LX].

69. *Id.* The attack was eventually pinned on the Chinese military, and four individuals were indicted for the hacking in February 2020. Aruna Viswanatha et al., *Four Members of China's Military Indicted over Massive Equifax Breach*, WALL ST. J. (Feb. 11, 2020, 10:09 AM), https://www.wsj.com/articles/four-members-of-china-s-military-indicted-for-massive-equifax-breach-11581346824?mod=searchresults&page=1&pos=9 [https://perma.cc/DLR5-S43U].

70. LaCroix, *supra* note 68.

71. *See* Lead Plaintiffs' Unopposed Motion for Final Approval of Shareholder Derivative Settlement, Award of Attorneys' Fees, and Reimbursement of Expenses with Memorandum of Law in Support at 2, *In re* Equifax, Inc. Derivative Litig., No. 1:18-CV-00317 (N.D. Ga. June 1, 2020), ECF No. 133.

72. LaCroix, *supra* note 68.

A. *The Demand Requirement and Wyndham Worldwide*

To bring a *Caremark* claim through derivative litigation, shareholders must first demand that the directors bring the suit on behalf of the corporation, unless such a demand would be futile.[73] Futility is proven by pleading, with particularity, facts that provide a reasonable doubt that the directors were independent or disinterested in their evaluation of whether to bring suit.[74] An inference of interestedness is permitted only if there is a substantial likelihood of personal liability.[75] This is a critical hurdle for plaintiffs to clear, because—in cases where demand is not futile—it gives broad powers to the directors to determine whether to bring the suit.[76] If the directors choose not to pursue the claim, their decision is entitled to the protection of the business judgment rule.[77]

Palkon v. Holmes[78] demonstrates some of the difficulties associated with the demand requirement. Information was stolen from Wyndham Worldwide Corporation (WWC) on three occasions between April 2008 and January 2010.[79] Hackers breached WWC's main network and those of its hotels, performing a "brute force attack"[80] and obtaining the personal information of over 600,000 customers.[81] The plaintiff-

73. BAUMAN ET AL., *supra* note 15, at 681–82; *see also* Fireman's Ret. Sys. of St. Louis v. Sorenson, No. 2019-0965, 2021 WL 4593777, at *12 (Del. Ch. Oct. 5, 2021) (holding that the Marriott board "retained its ability to assess whether to pursue litigation on behalf of the company" and therefore rejecting plaintiff-shareholder's argument that demand was futile). This often involves the formation of a Special Litigation Committee, or SLC, to evaluate whether it would be in the corporation's best interests to pursue the claim. *See* Einhorn v. Culea, 612 N.W.2d 78, 89–90 (Wis. 2000) (describing factors a court should consider in evaluating the independence of an SLC).

74. Brehm v. Eisner, 746 A.2d 244, 256 (Del. 2000).

75. *In re* InfoUSA, Inc. S'holders Litig., 953 A.2d 963, 990 (Del. Ch. 2007). The independence of a director, as contrasted with the interestedness of a director, has to do with the director's *personal* relationships, not likelihood of liability, and is not readily applicable to the analysis in this Note. *See In re* Oracle Corp. Derivative Litig., 824 A.2d 917, 920 (Del. Ch. 2003).

76. *See Brehm*, 746 A.2d at 253 (quoting Aronson v. Lewis, 473 A.2d 805, 814 (Del. 1984)).

77. *Id.* at 253, 264. The business judgment rule is defined as the "presumption that in making a business decision the directors of a corporation acted on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company." *Aronson*, 473 A.2d at 812. The rule reflects the notion in corporate law that the shareholders only should have control over certain types of activity and give sufficient freedom to make business decisions to the directors. Kamin v. Am. Express Co., 383 N.Y.S.2d 807, 810–11 (Sup. Ct. 1976) ("The directors' room rather than the courtroom is the appropriate forum for thrashing out purely business questions which will have an impact on profits, market prices, competitive situations, or tax advantages.").

78. No. 2:14-cv-01234, 2014 WL 5341880 (D.N.J. Oct. 20, 2014).

79. *Id.* at *1.

80. *Id.* A brute force attack means the hackers guessed user IDs and passwords to enter an administrator's account, and then used "memory-scraping malware" to collect sensitive data. *Id.*

81. *Id.*

shareholder sent a letter to the board demanding that it bring litigation against the directors and officers.[82] The board instructed the Audit Committee to evaluate the demand and, following the Committee's investigation and recommendation, unanimously voted to not bring the lawsuit.[83]

Following the denial, the plaintiff filed a derivative suit against WWC and numerous of its corporate officials in *Palkon*, arguing that, given their allegations of bad faith, the board's decision to refuse plaintiff's demand was wrongful.[84] The court dismissed the claim because the plaintiff failed to plead "with particularity facts which raise a reasonable doubt that the Board acted (1) in good faith, or (2) based on a reasonable investigation."[85] The litigation failed before reaching either prong; instead, the demand pleading requirement proved to be a massive barrier for the plaintiff, preventing the *Caremark* claims from being fully analyzed on their merits.[86]

B. *The Business Judgment Rule and Home Depot*

For better or worse, the business judgment rule insulates corporate directors and officers from liability for many, if not most, of their actions.[87] The business judgment rule applies in many contexts in corporate law, and a complete analysis of its contours is beyond the scope of this Note.[88] However, as it relates to the merits of a *Caremark* claim, the business judgment rule is generally applied in such a way that so long as the director or officer performed her duties on an informed basis and in good faith, the courts will not second-guess his decisions.[89] In the *Caremark* context, the details of the system and the responses to red flags

82. *Id.*

83. *Id.* at *1–2.

84. *Id.* at *2.

85. *Id.* at *3.

86. The merits of a claim can come into play in demand futility contexts, but such was not at issue here. *See infra* Section II.B.

87. Stuart R. Cohn, *Demise of the Director's Duty of Care: Judicial Avoidance of Standards and Sanctions Through the Business Judgment Rule*, 62 TEX. L. REV. 591, 594 (1983). The idea is to reach an efficient equilibrium between the leadership's business risk-taking and protection of shareholders' interests. *See* Stephen H. Ellick, *Harmonizing the Procedures for Initiating and Terminating Derivative Litigation: A Modification of Delaware Law*, 60 GEO. WASH. L. REV. 1888, 1888–89 (1992); *see also* Cohn, *supra*, at 637–38 (arguing that the public interest should also be taken into account in cases that involve corporate directorships).

88. For comprehensive analysis, see generally Stephen M. Bainbridge, *The Business Judgment Rule as Abstention Doctrine*, 57 VAND. L. REV. 83 (2004), for a description of the functions of the business judgment rule, and Bernard S. Sharfman, *Shareholder Wealth Maximization and Its Implementation Under Corporate Law*, 66 FLA. L. REV. 389 (2015), which sketches the contours of judicial influence and the goals of corporate law.

89. *See* Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984), *overruled on other grounds by* Brehm v. Eisner, 746 A.2d 244, 254 (Del. 2000).

that emerge from the system are themselves a matter of business judgment.[90]

The dismissal in *In re The Home Depot, Inc. Shareholder Derivative Litigation*[91] demonstrates challenges associated with the business judgment rule in both the procedural stage and on the merits of the claim.[92] Home Depot was the target of a cybersecurity breach over several months in 2014 during which hackers stole the financial data of 56 million customers.[93] The hackers used a third-party vendor's username and password to breach Home Depot's network and install malware on cash registers that allowed the hackers to capture a customer's financial data every time a card was swiped.[94] The total cost to Home Depot was "estimated to eventually reach nearly $10 billion."[95] Home Depot, as a merchant dealing in credit card information, is subject to a private-ordering system called the Payment Card Industry Data Security Standards (PCI DSS), which is promulgated by credit card companies who may fine merchants who are out of compliance with its standards.[96] At the time of the data breach, the Home Depot board knew the company did not comply with the PCI DSS standards for data security by failing to encrypt point-of-sale data, allowing unauthorized access to customer information, and lacking the ability to adequately scan its network.[97] The board had allegedly instituted a compliance plan but would remain noncompliant for another two years.[98] According to the plaintiffs,

90. Marchand v. Barnhill, 212 A.3d 805, 821 (Del. 2019) (en banc).

91. 223 F. Supp. 3d 1317 (N.D. Ga. 2016).

92. The procedural posture of this case should not be confused with the previous discussion on *Palkon*. Here, the plaintiffs did not make a demand, arguing it would have been futile because the board could not have exercised independent business judgment in whether to bring suit given the strong likelihood of personal liability. Plaintiffs' Memorandum of Law in Opposition to Defendants' Motion to Dismiss, *supra* note 25, at 20–21. This may be contrasted with *Palkon*, where the plaintiff made a demand, and it was refused, which gave him much fewer options to proceed. Palkon v. Holmes, No. 2:14-CV-01234, 2014 WL 5341880, at *2–3 (D.N.J. Oct. 20, 2014). When a demand is purportedly futile, courts may treat it as a substantive question of law and analyze the case on its merits. *See In re The Home Depo*t, 223 F. Supp. 3d at 1325 (describing the connection between demand futility analysis and the merits of the claim).

93. *See In re The Home Depot*, 223 F. Supp. 3d at 1321.

94. *Id.* The malware was called BlackPOS and a similar version was used in the Target data breach. *Id.* The "POS" in BlackPOS refers to "point of sale" terminals, e.g., cash registers. *Id.*

95. *Id.*

96. *Id.* at 1322; *see* Edward A. Morse & Vasant Raval, *Private Ordering in Light of the Law: Achieving Consumer Protection through Payment Card Security Measures*, 10 DEPAUL BUS. & COM. L.J. 213, 215, 226 (2012) (comparing PCI DSS to Generally Accepted Accounting Principles, or GAAP, which "have become the established basis for U.S. financial reporting, and they are also used for limited purposes in constructing federal income tax laws," and noting that breaches of PCI DSS are punished by privately imposed fines).

97. Plaintiffs' Memorandum of Law in Opposition to Defendants' Motion to Dismiss, *supra* note 25, at 6.

98. *Id.* at 7.

"[h]ackers exploited the gaps in [Home Depot's] network well before the upgrades were completed."[99] The board attempted to rush through more compliance measures by installing encryption technology at seventy-five percent of its stores in just six days.[100]

The court explained that, in the face of knowing noncompliance with PCI DSS standards, as long as the directors pursued "*any* course of action that was reasonable, they would not have violated their duty of loyalty."[101] The court explained that "[w]ith the benefit of hindsight, one can safely say that the implementation of the plan was probably too slow, . . . [yet] '[s]imply 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.'"[102] Knowledge of the noncompliance paired with a remediation plan—even a bad one—is covered by the business judgment rule.[103]

For plaintiffs to succeed on their theory, they would have had to show complete inaction: "Delaware courts have held that '[b]ad faith cannot be shown by merely showing that the directors failed to do all they should have done under the circumstances.' Rather, they use language like 'utterly' and 'completely' to describe the failure necessary to violate the duty of loyalty by inaction."[104] In other contexts, plaintiff-shareholders have succeeded on a "red flag" theory for the second prong of the analysis when the allegations "evidence misconduct of such pervasiveness and magnitude . . . that [an] inference of deliberate disregard" by the board was reasonable.[105]

C. *Unique Challenges to Cybersecurity Oversight Liability*

As demonstrated by *Home Depot* and *Palkon*, many of the hurdles that have halted plaintiffs with cybersecurity oversight claims have been standard *Caremark* hurdles, not ones which are unique to cybersecurity. That being said, cybersecurity oversight liability does implicate its own set of unique issues. However, none of these issues have so far proven fatal to plaintiffs' claims.

Congress remains "hesitant to pass legislation requiring the whole private sector to adopt certain cybersecurity standards and best

99. *Id.*

100. *In re The Home Depot*, 223 F. Supp. at 1323.

101. *Id.* at 1326.

102. *Id.* at 1327 (third alteration in original) (quoting Melbourne Mun. Firefighters' Pension Tr. Fund *ex rel.* Qualcomm, Inc. v. Jacobs, No. 10872, 2016 WL 4076369, at *9 (Del. Ch. Aug. 1, 2016)).

103. *Id.* at 1326.

104. *Id.* (alteration in original) (footnote omitted) (quoting Wayne Cnty. Emps.' Ret. Sys. v Corti, No. 3534–CC, 2009 WL 2219260 (Del. Ch. July 24, 2009)).

105. *In re* Pfizer Inc. S'holder Derivative Litig., 722 F. Supp. 2d 453, 462 (S.D.N.Y. 2010).

practices."[106] Indeed, the United States does not have a general data-security statute.[107] The lack of well-established or consistent cybersecurity regulations may make a cybersecurity oversight claim more difficult to bring. While the last decade has witnessed an uptick in government responses to data breaches, cybersecurity remains a patchwork regulatory scheme. The Securities and Exchange Commission (SEC), the Department of Justice, the Department of Homeland Security, the Federal Communications Commission, the Financial Industry Regulatory Authority, and the Consumer Financial Protection Bureau, among others, have begun to make cybersecurity a priority, but have not issued any blanket requirements.[108] The Cybersecurity Enhancement Act of 2014[109] authorizes the Commerce Department's National Institute of Standards and Technology (NIST) to develop data security standards, but private companies are not required to comply.[110]

The Federal Trade Commission (FTC) seems to have taken the reigns on data security enforcement, and has enacted "seemingly mandatory standards, but they are loosely defined."[111] That being said, the Agency has brought law enforcement actions in the privacy and data security context more than 210 times and issued a $5 billion penalty—the largest consumer privacy penalty ever—against Facebook in 2019 for violating a 2012 FTC privacy order.[112] Furthermore, the FTC settled with Equifax

106. James Eastman, Note, *Avoiding Cyber-Pearl Harbor: Evaluating Government Efforts to Encourage Private Sector Critical Infrastructure Cybersecurity Improvements*, 18 COLUM. SCI. & TECH. L. REV. 515, 532 (2017).

107. *See* Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 COMPETITION 229, 230 (2015) ("[T]here is no general data-security statute in the United States.").

108. *See* Thad A. Davis et al., *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2015 COLUM. BUS. L. REV. 613, 618.

109. Pub. L. No. 113-274, 128 Stat. 2971 (codified as amended in scattered sections of 15 U.S.C.).

110. 15 U.S.C. § 7406(c); Eric J. Hyla, Note, *Corporate Cybersecurity: The International Threat to Private Networks and How Regulations Can Mitigate It*, 21 VAND. J. ENT. & TECH. L. 309, 320 (2018).

111. Hyla, *supra* note 110, at 320.

112. FED. TRADE COMM'N, FEDERAL TRADE COMMISSION 2020 PRIVACY AND DATA SECURITY UPDATE 2–3 (2020); Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019) [hereinafter Fed. Trade Comm'n, $5 Billion Penalty], https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/65VA-CNTU]. The Agency had issued a Consent Decree having to do with Facebook's use of user data, not security. Fed. Trade Comm'n, $5 Billion Penalty, *supra*.

for $700 million following its data breach in 2017.[113] The Agency has also recently settled with Zoom Video Communications.[114]

Some businesses may find themselves subject to regulation based on their activities. Federal statutes address data security in specific industries, like health care or financial services, and all fifty states have data-breach notification laws.[115] Additionally, government contractors are required to implement NIST standards for safeguarding government information.[116] Department of Defense (DoD) contractors have even more stringent standards for their contractors.[117]

Patchwork regulations find their mirror in the mismatched response from corporate leaders. According to Global Risk Reports 2019, business leaders in advanced economies rated cyberattacks among their top concerns, and rated such attacks as both high in likelihood and in overall impact.[118] Additionally, corporate boards are paying attention to cybersecurity risks, with 89% of directors in public companies saying that board meetings regularly include a discussion of cybersecurity.[119] And for good reason. Indeed, as the recent Delaware Court of Chancery

113. Press Release, Fed. Trade Comm'n, FTC Releases 2019 Privacy and Data Security Update (Feb. 25, 2020), https://www.ftc.gov/news-events/press-releases/2020/02/ftc-releases-2019-privacy-data-security-update [https://perma.cc/U959-6H4D].

114. Press Release, Fed. Trade Comm'n, FTC Requires Zoom to Enhance Its Security Practices as Part of Settlement (Nov. 9, 2020), https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement [https://perma.cc/D7 XV-DS3R].

115. Hyla, *supra* note 110, at 329–30, 331 n.155.

116. FAR 52.204-21(b) (2020). The regulation provides that the contractor must apply several basic safeguarding requirements and procedures to protect covered contractor information systems, including: limiting information system access to authorized users, providing protection from malicious code at appropriate locations within organizational information systems, updating malicious code protection mechanisms when new releases are available, and performing periodic scans of the information system with real-time scans of files from external sources as files are downloaded, opened, or executed. *Id.*; *see also* Bradley Wyatt, *Top Five Cybersecurity Requirements for Government Contractors*, WINVALE (Sept. 16, 2020), https://info.winvale.com/blog/top-five-cybersecurity-requirements-for-government-contractors [https://perma.cc/J5TU-XQVG] (explaining the regulation's requirements).

117. *See* 48 C.F.R. §§ 204.7300–.7304 (2021); *see also Compliance with Cybersecurity and Privacy Laws and Regulations*, NAT'L INST. OF STANDARDS & TECH. (Aug. 4, 2021), https://www.nist.gov/mep/cybersecurity-resources-manufacturers/dfars-compliance [https://perma.cc/ C3H6-5QY6] ("If your company produces products used by the Department of Defense (DoD), you may be required to comply with the minimum cybersecurity standards set by [federal defense regulations] . . . ."). The DoD also runs a Cybersecurity Maturity Model Certification test to ensure all requirements have been implemented. *Id.*

118. WORLD ECON. F., THE GLOBAL RISKS REPORT 2019, at 16 (2019), http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf [https://perma.cc/H4RH-QFWF].

119. Chirantan Chatterjee & D. Daniel Sokol, *Data Security, Data Breaches, and Compliance*, *in* CAMBRIDGE HANDBOOK ON COMPLIANCE 936, 943 (Benjamin van Rooji & D. Daniel Sokol eds., 2021).

decision *Fireman's Retirement System of St. Louis v. Sorenson*[120] notes: "[A]s the legal and regulatory frameworks governing cybersecurity advance and the risks become manifest, corporate governance must evolve to address them. The corporate harms presented by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place."[121]

While there appears to be awareness of the risks associated with insufficient cybersecurity measures, the compliance protocols and procedures are "not as fleshed out for data breaches as they are for traditional compliance issues such as anti-bribery and audit fraud."[122] Surveys suggest that most U.S. financial services firms begin using new technologies prior to creating the compliance programs necessary to ensure data security.[123] Further, as compared to traditional areas of compliance, data-breach-related compliance spending by firms remains much smaller.[124] Researchers have found evidence of little commitment from management and boards in regards to cybersecurity,[125] and that many Chief Information Security Officers believe that firms do not invest enough in cybersecurity.[126]

The lack of robust cybersecurity compliance investment may cause confusion in the *Caremark* context, with cybersecurity perhaps appearing to boards and managers as a business risk rather than a compliance risk. Courts may or may not share that opinion. "Delaware courts traditionally have viewed stockholder allegations that a board failed to oversee the company's obligation to comply with positive law, or positive regulatory mandates, more favorably in the *Caremark* paradigm than allegations that a board failed to oversee the company's efforts generally to avoid business risk."[127] Put another way, "it is more difficult to plead and prove *Caremark* liability based on a failure to monitor and prevent harm flowing from risks that confront the business in the ordinary course of its operations."[128] Indeed, in *Sorenson*, the plaintiff based its *Caremark* claim on Marriott's alleged noncompliance with PCI DSS, the private ordering of credit card companies via contracts with merchants.[129] The

120. No. 2019-0965, 2021 WL 4593777 (Del. Ch. Oct. 5, 2021).

121. *Id.* at *12.

122. Chatterjee & Sokol, *supra* note 119, at 943.

123. *Id.* at 944.

124. *Id.* at 943.

125. *Id.*; *see also* MARTIN C. LIBICKI ET AL., THE DEFENDER'S DILEMMA: CHARTING A COURSE TOWARD CYBERSECURITY 11 (2015).

126. Chatterjee & Sokol, *supra* note 119, at 944.

127. *In re* Facebook, Inc. Section 220 Litig., No. 2018-0661, 2019 WL 2320842, at *2 (Del. Ch. May 31, 2019).

128. *Id.* at *14 n.150.

129. No. 2019-0965, 2021 WL 4593777, at *14 (Del. Ch. Oct. 5, 2021).

chancery court dismissed the case, reasoning that "[p]leading non-compliance with non-binding industry standards, like the PCI DSS, is not the same as pleading that directors knowingly permitted a company to violate positive law."[130] Yet, neither the court in *In re The Home Depot* nor the court in *Palkon* seemed to take issue with the lack of clear and prominent regulatory systems. In fact, in *Home Depot*, the court seemed to accept noncompliance with PCI DSS just as troublesome as noncompliance with a regulatory body's standards.[131] Or, at any rate, the court did not say it was a basis of dismissal.[132] Meanwhile, in *Palkon*, no cybersecurity standard was discussed at all. And, in those cases, the companies were not even required to comply with the stringent government contractor requirements, FTC Consent Decrees, or other company-specific data security protocols to which some companies find themselves subject.

III. RECENT DEVELOPMENTS IN DELAWARE LAW

A Delaware Supreme Court seminal case and a series of four Delaware Court of Chancery decisions may provide the opening plaintiff's attorneys are looking for to bring a successful cybersecurity oversight liability claim. Taken together, the cases present a new twist on the *Caremark* framework, wherein plaintiffs may find their claims easier to bring when a board fails to exercise their oversight duties "more rigorously" in the face of "mission critical" oversight duties.

A. *"Mission Critical" Debuts in Delaware*

In *Marchand v. Barnhill*,[133] a unanimous Supreme Court of Delaware reversed the chancery court's dismissal of a *Caremark* claim and allowed a case to proceed against the board of Blue Bell Creameries, an ice cream manufacturer that caused a deadly listeria outbreak.[134] Plaintiffs alleged that a lack of boardroom oversight resulted in the outbreak and subsequent nationwide recall of its products, causing monetary losses to investors.[135]

130. *Id.*

131. *See In re* The Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317, 1322 (N.D. Ga. 2016) ("Home Depot's contracts with financial institutions required them to comply with the [PCI DSS] . . . , which established a minimum level of protection for data security. . . . [T]he Board and the Audit Committee were informed by M. Carey that Home Depot was out of compliance with PCI DSS on multiple levels.").

132. *See id.* at 1327.

133. 212 A.3d 805 (Del. 2019) (en banc).

134. *Id.* at 807–09.

135. *Id.* at 807. Stockholders also suffered losses because, after the operational shutdown, Blue Bell suffered a liquidity crisis that forced it to accept a dilutive private equity investment. *Id.*

In the case, a Blue Bell shareholder filed a derivative suit against Blue Bell's management and board, asserting two claims based on: (1) "management's alleged failure to respond appropriately to the red and yellow flags about growing food safety issues[;]" and (2) "the board's violation of its duty of loyalty, under *Caremark*, by failing to implement any reporting system and therefore failing to inform itself about Blue Bell's food safety compliance."[136] The chancery court concluded that there was a monitoring system in place based on Blue Bell's compliance with Food and Drug Administration (FDA) regulations, ongoing third-party monitoring for contamination, and consistent reporting by senior management to Blue Bell's board on operations.[137] The court noted that "[w]hat Plaintiff really attempts to challenge is not the *existence* of monitoring and reporting controls, but the *effectiveness* of monitoring and reporting controls in particular instances."[138] As a result, the court held that demand was not excused as to the *Caremark* claims and dismissed the complaint.[139] Plaintiffs appealed.[140]

Chief Judge Leo E. Strine Jr. for the Supreme Court of Delaware began the opinion by laying out the context of the listeria outbreak, explaining that as a U.S. food manufacturer, Blue Bell operates in a heavily regulated industry.[141] The court noted that Blue Bell complied—at least "nominally"—with the FDA regulations: the company distributed a sanitation manual with standard operating and reporting procedures, and had written procedures for processing and reporting consumer complaints.[142] Additionally, Blue Bell engaged a third-party laboratory and conducted food-safety auditing to test for dangerous contaminants in its facilities, and the government regularly inspected Blue Bell's facilities and provided the results to management.[143] The defendants argued that those systems, plus the fact that the Blue Bell board met monthly and

136. *Id.* at 815–16.

137. Marchand v. Barnhill, No. 2017-0586, 2018 WL 4657159, at *11, *17–18 (Del. Ch. Sept. 27, 2018), *rev'd*, 212 A.3d 805 (Del. 2019) (en banc).

138. *Id.* This might be both compared and contrasted with the plaintiff's pleading issues in *In re Home Depot*, discussed in Part I, wherein the court noted the board responded to the known noncompliance, but in the plaintiff's opinion, "it moved too slowly." *In re* The Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317, 1326 (N.D. Ga. 2016). Here, the chancery court said the plaintiffs were complaining about the effectiveness of the *reporting controls*. *Marchand*, 2018 WL 4657159, at *18. Both would be subject to the business judgment rule so long as undertaken in good faith.

139. *Marchand*, 2018 WL 4657159, at *19.

140. *Marchand*, 212 A.3d at 807.

141. *Id.* at 810. "Specifically, FDA regulations require food manufacturers to conduct operations 'with adequate sanitation principles' and, in line with that obligation, 'must prepare . . . and implement a written food safety plan.'" *Id.* (footnote omitted) (quoting 21 C.F.R. § 110.80).

142. *Id.* at 822–23, 823 n.110.

143. *Id.* at 823 n.110.

regularly reviewed reports relating to manufacturing operations from the company CEO and VP of Operations, demonstrated that a reporting system was in place, and therefore plaintiffs lost on prong one arguments.[144] The court disagreed.

First, the court noted that "the fact that Blue Bell nominally complied with FDA regulations does not imply that the *board* implemented a system to monitor food safety *at the board level*."[145] The court then quoted *Caremark*, in a footnote, adding emphasis that:

> [I]t is important that the *board* exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the *board* that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility.[146]

The court explained that the plaintiffs fairly pled 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 and the board was not presented with any material information about food safety."[147] The court said it was "inferable that there was no expectation of reporting to the board of any kind."[148] In reversing the lower court's grant of the motion to dismiss, the court explained that:

> Although *Caremark* may not require as much as some commentators wish, it does require that a board make a good faith effort to put in place a reasonable system of monitoring and reporting about the corporation's *central compliance risks*. In Blue Bell's case, *food safety was essential and mission critical*.[149]

And thus, the court inferred that the board did not make the good faith effort that *Caremark* requires.[150] The court reversed, and the plaintiffs

144. *Marchand*, 2018 WL 4657159, at *6, *17.

145. *Marchand*, 212 A.3d at 823.

146. *Id.* at 823 n.111 (quoting Stone *ex rel.* AmSouth Bancorporation v. Ritter, 911 A.2d 362, 368 (Del. 2006)).

147. *Id.* at 809. Note that this holding rests in prong one of *Caremark* and the use of the "red and yellow flag" language did not shift this opinion into prong two. Note also that the court rests its holding in the *board's* lack of reporting mechanisms, not *management's* handling of the issue. The court takes issue with the fact that at Blue Bell: (1) there was no board committee that addressed food safety; (2) there were no regular processes or protocols that required management to keep the board apprised of food safety compliance practices, risks, or reports; (3) while the board was given certain favorable information about food safety by management, it was not given important reports that presented a very different picture; and (4) the board meetings are devoid of any suggestion that there was any regular discussion of food safety issues. *Id.* at 813.

148. *Id.*

149. *Id.* at 824 (emphasis added) (footnote omitted).

150. *Id.* at 822.

survived the motion to dismiss, a key hurdle to bringing a suit of this nature.[151]

The decision has sparked debate. Some argue the case established "key precedent surrounding the role and performance of corporate director responsibilities and director liability when it comes to the exercise of risk oversight."[152] This is especially instructive when juxtaposed to the role of management. In other words, the board risks liability "if it simply leaves compliance and risk oversight entirely to the prerogatives of management."[153] This is a fair interpretation, but not the one that the chancery courts follow. A second, more persuasive interpretation singles out the court's use of the term "mission critical." This interpretation argues that because "Blue Bell made just one product, and the food-safety issue that arose with respect to that product virtually shut down the company[,] imperiled its continued existence," and harmed the general public, the issue was truly "mission critical."[154] Since *Marchand* was decided, a series of chancery court decisions have shed more light on how Delaware courts interpret the decision and show that the "mission critical" interpretation prevails.

B. *"More Rigorously Exercised" Oversight Under Prong Two*

In *In re Clovis Oncology, Inc.*,[155] the chancery court applied "mission critical" analysis to prong two of the *Caremark* framework. The court found that the plaintiffs had sufficiently stated a claim for a breach of the duty of oversight, and the complaint survived a motion to dismiss.[156] Clovis, an upstart biopharmaceutical company with three drugs in development (but none on the market), identified one of the drugs, Roci,

151. Perhaps unsurprisingly, the case settled after this ruling. The $60 million settlement included $9 million in legal fees. Angela Morris, *Sweet! $9 Million Attorney Fee Slated for Houston Firm That Secured Blue Bell Listeria Settlement*, LAW.COM (Apr. 27, 2020, 2:15 PM), https://www.law.com/texaslawyer/2020/04/27/sweet-9-million-attorney-fee-slated-for-houston-firm-that-secured-blue-bell-listeria-settlement/?slreturn=20200924065555 [https://perma.cc/WKB2-QG LB].

152. Paul Ferrillo et al., *Boards Should Care More About Recent "Caremark" Claims and Cybersecurity*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Sept. 15, 2020), https://corpgov.law.harvard.edu/2020/09/15/boards-should-care-more-about-recent-caremark-claims-and-cybersecurity/#5 [https://perma.cc/5MP8-8D53].

153. Cydney Posner, *Delaware Supreme Court Allows Caremark Duty of Loyalty Claims Against Directors to Survive Dismissal Motion*, COOLEY PUBCO (July 12, 2019), https://cooleypubco.com/2019/07/12/delaware-marchand-v-barnhill/ [https://perma.cc/HF4S-JN5M].

154. Marjorie Duffy et al., *Delaware Supreme Court Reinforces Directors' Oversight Obligations on Mission-Critical Subjects*, JD SUPRA (Aug. 8, 2019), https://www.jdsupra.com/legalnews/delaware-supreme-court-reinforces-63547/ [https://perma .cc/982Z-4L4W].

155 No. 2017-0222, 2019 WL 4850188, at *1, *18 (Del. Ch. Oct. 1, 2019).

156. *Id.* at *1, *18.

as especially promising.[157] Roci, a therapy for the treatment of lung cancer, performed well during the early stages of its clinical trial but data from later stages revealed the drug likely would not be approved for market by the FDA.[158] Plaintiffs, Clovis stockholders, argued that members of the Clovis board "breached their fiduciary duties by failing to oversee the Roci clinical trial and then allowing the Company to mislead the market regarding the drug's efficacy."[159] These breaches, plaintiffs argued, "caused Roci to sustain corporate trauma in the form of a sudden and significant depression in market capitalization."[160]

The court invoked the "mission critical" language from *Marchand*, explaining that Roci was Clovis's mission critical product because the company had no other drugs on the market, and this was its most promising drug in development.[161] In rejecting the defendants' motion to dismiss, Vice Chancellor Joseph R. Slights III interpreted *Marchand* as "underscor[ing] the importance of the board's oversight function when the company is operating in the midst of 'mission critical' regulatory compliance risk."[162] He also noted that *Marchand* "makes clear" that where a company operates in such a "mission critical" regulatory environment, "the board's oversight function must be more rigorously exercised."[163] However, unlike the court in *Marchand,* Vice Chancellor Slights found the plaintiffs unable to establish a breach of the first prong of the *Caremark* framework because the board did have oversight and reporting systems in place for the clinical trials and the board "reviewed detailed information regarding [Roci's] . . . trial at each Board meeting."[164]

Vice Chancellor Slights instead found the plaintiffs' allegations were sufficient to survive a motion to dismiss under the second prong.[165] The court said that red flags are only useful when "visible to the careful observer"[166] and "the careful observer is one whose gaze is fixed on the

157. *Id.* at *1–2.

158. *Id.* at *1.

159. *Id.*

160. *Id.* Clovis was also the subject of a securities class action lawsuit. The securities suit settled for $25 million in cash and $117 million in Clovis stock. *Clovis Securities Litigation Settlement Website*, https://www.clovissecuritieslitigation.com/ [https://perma.cc/WQ3E-MG8V]. The SEC also pursued an enforcement action against three Clovis officials, which led to a consent decree requiring the company to pay $20 million, and the CEO and CFO to pay $250,000 and $100,000 in civil penalties. *Executives Charged with Misleading Investors About Cancer Drug*, Exchange Act Release No. 24273 (Sept. 18, 2018), https://www.sec.gov/litigation/litreleases/2018/lr24273.htm [https://perma.cc/ET3B-E8SG].

161. *Clovis*, 2019 WL 4850188, at *2, *14.

162. *Id.* at *12.

163. *Id.* at *13.

164. *Id.* (alteration in original).

165. *Id.* at *15.

166. *Id.* at *13 (quoting Wood v. Baum, 953 A.2d. 136, 143 (Del. 2008)).

company's mission critical regulatory issues."[167] For Clovis, this was Roci's clinical trial and the related FDA regulations governing that study.[168] Thus, the court held that the plaintiffs had sufficiently pleaded a *Caremark* claim on the fact that the board consciously ignored red flags that revealed a "mission critical failure to comply with the [clinical trial] protocol and associated FDA regulations."[169] Clovis's board's conscious disregard of the red flags imperiled FDA approval of a promising drug that was "intrinsically critical to [Clovis's] business operation."[170] Vice Chancellor Slights found that "this failure of oversight caused monetary and reputational harm to the Company."[171]

C. *A Choice Not to Invoke "Mission Critical"?*

A Delaware court's decision not to invoke *Marchand*'s "mission critical" concept may be as telling as a decision to invoke it. In two of the four cases lending insight on *Marchand*, the court cited *Marchand* but did not apply the "mission critical" concept to the facts at issue. Clear guidance about when to apply the concept remains to be seen.

On April 27, 2020, in *Hughes v. Hu*,[172] the chancery court found that the plaintiff had stated a claim for breach of the duty of oversight.[173] But this case demonstrates what kind of corporation and what kind of regulation that Delaware courts may not consider "mission critical."

The lawsuit involved Kandi Technologies Company, a Delaware corporation based in China.[174] The company's SEC filings showed that the company had been struggling with its financial reporting and internal controls since at least 2010.[175] The company was later forced to restate several years' worth of financial statements and also to disclose that its internal staff lacked sufficient expertise for compliance with U.S.

167. *Id.*

168. *Id.* at *14.

169. *Id.* at *15.

170. *Id.* at *1 (quoting Marchand v. Barnhill, 212 A.3d 805, 822 (Del. 2019) (en banc)).

171. *Id.* at *15. The Vice Chancellor specifically found that the plaintiffs had alleged that the "Board ignored multiple warning signs that management was inaccurately reporting" the cancer drug's efficacy. *Id.* at *1. The court pointed to board slides that explicitly warn that the clinical trial numbers are "[u]nconfirmed." *Id.* at *15 n.210 (alteration in original). Plaintiffs, supported by scholarly articles, argued that "confirmation [of responses] is the 'industry standard.'" *Id.* (alteration in original). The court explained that since Roci was such an important product for the company, the board presentations with unconfirmed numbers should have prompted "questions—if not objections—from the Board." *Id.* The court also rejected Clovis's reliance defense under 8 Del. C. § 141(e) because the reliance was unreasonable again given the importance of the product. *Id.*

172. No. 2019-0112, 2020 WL 1987029 (Del. Ch. Apr. 27, 2020).

173. *Id.* at *1.

174. *Id.*

175. *Id.*

reporting requirements.[176] The court said, "[d]espite having pledged three years earlier to get its house in order, the Company had none of these necessary competencies."[177] The plaintiff alleged that the director-defendants consciously failed to establish a board-level system of oversight for the company's financial statements, choosing instead to rely on management "while devoting patently inadequate time to the necessary tasks."[178] The defendants moved to dismiss the lawsuit, arguing failure to make a demand.[179] Plaintiffs argued their demand was excused because the board faced a substantial likelihood of liability.[180]

Like the court in *Marchand,* the chancery court decided the case on prong one of the *Caremark* framework.[181] Vice Chancellor J. Travis Laster noted that the company may have "had the trappings of oversight," including the existence of a board-level audit committee, a Chief Financial Officer, an internal audit department, a code of ethics, and an external auditor.[182] However, these trappings were insufficient, as "the Company's Audit Committee met sporadically, devoted inadequate time to its work, had clear notice of irregularities, and consciously turned a blind eye to their continuation."[183]

The court distinguished this case from an earlier case, *In re General Motors Co. Derivative Litigation*,[184] in which the court held that the "plaintiffs could not plead that the directors faced a substantial likelihood of *Caremark* liability by arguing that the board 'should have[] had a *better* reporting system.'"[185] Here, the court said, the board was far less active; the Audit Committee never met for longer than one hour and typically only once per year, "suggest[ing] that they devoted patently inadequate time to their work."[186] To the court, this pattern of behavior indicated that they failed to act in good faith to maintain a board-level monitoring system by following management "blindly" even after they had demonstrated an inability to report accurately.[187] The court, in the

176. *Id.*
177. *Id.*
178. *Id.*
179. *Id.*
180. *Id.*
181. *Id.* at *14–17.
182. *Id.* at *14.
183. *Id.* at *16.
184. No. 9627, 2015 WL 3958724 (Del. Ch. June 26, 2015).
185. *Hughes*, 2020 WL 1987029, at *16 (alteration in original) (quoting *In re Gen. Motors Co.,* 2015 WL 3958724, at *15). The board in *General Motors* "regularly reviewed the company's risk management structure, identified the top risks facing the company's business, and received presentations on product safety and quality." *Id.*
186. *Id*.
187. *Id.* The court also noted that the audit committee may rely in good faith upon reports by management and other experts under the Delaware corporate statute. *Id.*; DEL. CODE ANN. tit. 8,

accounting compliance context, did not invoke the "mission critical" aspect of *Marchand*, despite quoting the case several times.

The court came closer to clear analysis of "mission critical" issues in *Fireman's Retirement System of St. Louis v. Sorenson*.[188] In *Sorenson*, a plaintiff-shareholder sued the officers and directors of Marriott following a data breach which implicated the personal information of up to 500 million guests.[189] The vulnerability originated from Marriott's $13 billion acquisition of Starwood.[190] According to the plaintiff, "despite Starwood's data being the crown jewel of the Acquisition, the Board . . . failed to conduct or review any due diligence on Starwood's information security systems and risks, IT operations, or technology before closing the Acquisition."[191] Moreover, the plaintiff argued, customer data was "'mission critical' to the Company's ability to effectively market its rooms and service."[192]

Vice Chancellor Lori W. Will, who was sworn into the Court of Chancery on May 26, 2021, decided the case.[193] While Vice Chancellor Will acknowledged the importance of cybersecurity, she noted that "[t]he growing risks posed by cybersecurity threats do not, however, lower the high threshold that a plaintiff must meet to plead a *Caremark* claim."[194] Further, Vice Chancellor Will did not seem to find plaintiff's "mission critical" arguments persuasive, and indirectly dismissed them by saying:

> 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. Cybersecurity, however, is an area of consequential risk that spans modern business sectors.[195]

The chancery court did not elaborate on its decision not to analyze the case under the "mission critical" concept. The court instead analyzed the post-acquisition board's actions under the standard prong one and prong two of *Caremark*. Under the first prong, the court found it sufficient that "the Board and Audit Committee were 'routinely apprised' on

§ 141(e) (2021). The holding does not conflict with this statute because the court found the board failed to act in good faith in its reliance on management. *Hughes*, 2020 WL 1987029, at *16.

188. No. 2019-0965, 2021 WL 4593777 (Del. Ch. Oct. 5, 2021).

189. *Id.* at *1.

190. *Id.*

191. Verified Amended Stockholder Derivative Complaint ¶ 5, *Sorenson*, No. 2019-0965.

192. *Id.* ¶ 50.

193. *Judicial Officers*, DEL. CTS., https://courts.delaware.gov/chancery/judges.aspx [https://perma.cc/5VN9-765B]; *Sorenson*, 2021 WL 4593777, at *1.

194. *Sorenson*, 2021 WL 4593777 at *12.

195. *Id.* at *11 (footnote omitted).

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."[196] Under the second prong, the court found plaintiff's arguments unpersuasive, reasoning that (1) plaintiffs did not allege any "known illegal conduct, lawbreaking, or violations of a regulatory mandate," and (2) the board's response, though imperfect and "probably too slow," did not have the requisite scienter to qualify as a violation of a fiduciary duty.[197] Accordingly, the court granted the motion to dismiss.[198]

D. *"Mission Critical" in Complex Corporations*

On August 24, 2020, the chancery court denied a motion to dismiss in an action against the board of directors of AmerisourceBergen (ABC).[199] The lawsuit, *Teamsters Local 443 Health Services & Insurance Plan v. Chou*,[200] involved underlying allegations concerning the distribution of cancer medication at one of the company's subsidiaries.[201] The subsidiary would purchase single-dose sterile vials of cancer drugs, which are intentionally overfilled by the manufacturer to account for human error in filling syringes and to permit the medical provider to discharge a small amount before injection to avoid air bubbles.[202] The subsidiary would then "pool[]" the overfill, which was not intended for patient use, and fill additional syringes for resale.[203] "This process was unsterile and led to the contamination of the drugs . . . ."[204] Ultimately, the subsidiary pleaded guilty to criminal charges and settled civil claims.[205] ABC shareholders sued under several theories, the relevant one here being *Caremark*.[206]

In denying the motion to dismiss, the court found that the notion of "mission critical" regulation had been properly invoked.[207] The court explained that while ABC "is a relatively more complex corporation than either Blue Bell Creameries or Clovis, that does not mean the concept of mission critical compliance risk is inapplicable here."[208] And, since ABC

196. *Id.* at *13.
197. *Id.* at *15–16.
198. *Id.* at *19.
199. Teamsters Loc. 443 Health Servs. & Ins. Plan v. Chou, No. 2019-0816, 2020 WL 5028065, at *2, *26 (Del. Ch. Aug. 24, 2020).
200. No. 2019-0816, 2020 WL 5028065 (Del. Ch. Aug. 24, 2020).
201. *Id.* at *1.
202. *Id.*
203. *Id.*
204. *Id.*
205. *Id.* at *7–8.
206. *Id.* at *2.
207. *Id.* at *18.
208. *Id.*

is a "manufacturer, distributor, and packager of pharmaceutical drugs," the FDA regulations that it skirted related to mission critical aspects of its business.[209]

In thinking about the implications of this case, it is worth noting that Vice Chancellor Sam Glasscock III did observe the broader societal implications of ABC's and Blue Bell's businesses.[210] Along these lines, the court made a key observation at the outset of the case:

> A judge in the *Caremark* context must be careful to remember the issues before her. At issue is *not* whether specific or society-wide victims may themselves receive a remedy for corporate misconduct. Instead, the issue is whether the corporation, whose directors have allegedly allowed it to commit bad acts, should *itself* recover damages that ultimately inure to the benefit of the corporate owners, its stockholders. This unusual posture raises the question of whether *Caremark* liability is merely a branch of fiduciary liability designed to make the beneficiaries of that duty whole for breach, or whether it should be seen also as a blunt but useful tool to encourage good corporate citizenship. That question is for academic discussion, not judicial resolution; again, a judge in equity must be mindful that it is the corporation, not that corporation's victims, to whom any recovery will flow.[211]

This note from Vice Chancellor Glasscock underscores an important implication of the *Marchand* decision. That is, the court should not consider the society-wide victims in deciding a *Caremark* case, but the central business purposes of the corporation. Here, incidentally, that central business purpose included the good corporate citizenship goal of not hurting people because that was a regulatory requirement inherent in producing and selling cancer drugs.[212] Indeed, Vice Chancellor Glasscock noted that "flouting laws meant to ensure the safety and purity of drugs destined for patients suffering from cancer is directly inimical to the central purpose of ABC's business" given the "[l]aws and regulations

209. *Id.*

210. *Id.* at *1.

211. *Id.*

212. An interesting question that is beyond the scope of this Note is what role a stated mission statement has in this analysis. Take, for example, Twitter: "The mission we serve as Twitter, Inc. is to give everyone the power to create and share ideas and information instantly without barriers. Our business and revenue will always follow that mission in ways that improve —and do not detract from—a free and global conversation." *Investor Relations FAQ*, TWITTER, INC., https://investor.twitterinc.com/contact/faq/default.aspx [https://perma.cc/4ULZ-GBCF]; *see also* Justin Fox, *Why Twitter's Mission Statement Matters*, HARV. BUS. REV. (Nov. 13, 2014), https://hbr.org/ 2014/11/why-twitters-mission-statement-matters [https://perma.cc/BX4G-H44L] (calling the following mission statement uninspiring, though perhaps accurate: "The Company's primary objective is to maximize long-term stockholder value, while adhering to the laws of the jurisdictions in which it operates and at all times observing the highest ethical standards.").

governing the health and safety of drugs are thus the 'most central . . . safety and legal compliance issue facing the company.'"[213]

Here, as opposed to *Marchand*, the chancery court decided the case under prong two of the *Caremark* liability framework.[214] That is, in *Marchand* the court took issue with an absence of a meaningful reporting mechanism to the board (as opposed to management), whereas here, the chancery court expressly refrains from making such a determination.[215] Instead, the chancery court relies on the one-two punch plaintiffs demonstrated: the board's knowledge of the red flags and subsequent inaction.[216] In doing so, scholars argue, Vice Chancellor Glasscock "was able to cabin the case into well-trod *Caremark* ground, without the need to venture into the new territory explored in *Marchand*."[217] However, the court did still apply the new mission critical analysis from *Marchand* and *Clovis* to the prong two analysis found here, stating that this prong requires directors to be "careful observer[s]."[218] Articulating that standard, the court stated that the "careful observer" is "one whose gaze is fixed on the company's mission critical regulatory issues."[219]

In the end, Vice Chancellor Glasscock found that plaintiffs had sufficiently alleged that the directors had pleaded "particularized facts from which it is reasonably conceivable that a majority of the Board 'knew of evidence of corporate misconduct—the proverbial "red flag"—yet acted in bad faith by consciously disregarding its duty to address that misconduct.'"[220]

---

213. *Teamsters*, 2020 WL 5028065, at *18 (quoting Marchand v. Barnhill, 212 A.3d 805, 824 (Del. 2019) (en banc)).

214. *Id.* at *26.

215. *Id.* ("Because the Complaint survives under a 'prong two' theory, I need not decide whether the Director Defendants face a substantial likelihood of liability under 'prong one' of *Caremark*.").

216. *Id.* at *24.

217. Ann Lipton, *A Cautious Caremark Opinion*, L. PROFESSOR BLOGS NETWORK: BUS. L. PROFESSOR BLOG (Aug. 29, 2020), https://lawprofessors.typepad.com/business_law/2020/08/a-cautious-caremark-opinion.html [https://perma.cc/88NC-VSQY].

218. *Teamsters*, 2020 WL 5028065, at *17 (quoting *In re* Clovis Oncology, Inc. Derivative Litig., No. 2017-0222, 2019 WL 4850188, at *13 (Del. Ch. Oct. 1, 2019)).

219. *Id.*

220. *Id.* at *25 (quoting Horman v. Abney, No. 12290, 2017 WL 242571, at *6 (Del. Ch. Jan. 19, 2017)). Such subsequently ignored "red flags" included: (1) an outside law firm's report that had concluded the subsidiary's compliance mechanisms had gaps, on which the board's audit committee failed to follow up on; (2) a former executive of the subsidiary had filed a complaint under seal alleging that the subsidiary's business was essentially an illegal operation; (3) the company's 2010 and 2011 10-Ks, signed by the directors, disclosed the suit and the board still failed to take any remedial steps; and, (4) the subsidiary had received a subpoena from federal prosecutors, which was disclosed in the company's 2012 10-K, but which was not referenced in any board or committee minutes. *Id.* at *19–25.

E. *Implications*

This series of cases following *Marchand* lend interpretive insight into the Delaware courts' treatment of this arguably new *Caremark* framework. It could be argued that the cases which survived motions to dismiss are mere anomalies, reflecting the egregious surrounding circumstances and significant lack of directorial and managerial oversight as opposed to anything new and exciting going on in Delaware. The three cases that survived motions to dismiss involved egregious circumstances outside of the directly relevant facts.[221] However, such a narrow view does not give sufficient credence to the role of "mission critical" compliance issues.

Marchand, *Clovis*, and *Teamsters* emphasized that the board's oversight responsibilities were particularly important with respect to "mission critical" regulatory requirements.[222] That is, the claims arose out of circumstances that involved compliance requirements that the board should have been watching, given the importance of the requirements to the company's operations and business success. Importantly, the court in *Hughes* did not invoke the "mission critical" notion even though the breach involved key SEC regulations of accounting practices.[223] One explanation for this absence may be that in *Marchand*, *Clovis*, and *Teamsters*, the regulatory requirements had consumer protection implications. However, the *Teamsters* opinion clarified that the mission critical aspect of these cases was not directly tied to the potential for society-wide victims; instead, it was the inimical nature of the board's lack of oversight to the central business purpose of the corporation that made it a "mission critical" oversight breach.[224] Thus, presumably, because the central business purpose of Kandi Technologies was not accounting-related, the regulations did not invoke the mission critical language in the opinion.

Moving forward, when courts apply the *Caremark* framework, their analysis will be informed by the notion found in *Marchand* that where a company's "mission critical" functions are subject to regulation, "the

221. In *Marchand*, the background included the deaths of customers that had consumed Blue Bell's ice cream. Marchand v. Barnhill, 212 A.3d 805, 807 (Del. 2019) (en banc). In *Clovis*, the derivative claim related to circumstances that had already been the subject of a massive securities class action lawsuit settlement and a settled SEC enforcement action. *Clovis*, 2019 WL 4850188, at *9. In *Teamsters*, the claim found its roots in a subsidiary that the court described as basically an entirely illegal business whose business model was to engage in illegal and unsanitary "pool[ing]" of cancer treatment drugs. *Teamsters*, 2020 WL 5028065, at *1.

222. *Marchand*, 212 A.3d at 824; *Clovis*, 2019 WL 4850188, at *14; *Teamsters*, 2020 WL 5028065, at *18.

223. Hughes v. Hu, No. 2019-0112, 2020 WL 1987029, at *1 (Del. Ch. Apr. 27, 2020).

224. *Teamsters*, 2020 WL 5028065, at *1, *18 ("[F]louting laws meant to ensure the safety and purity of drugs destined for patients suffering from cancer is directly inimical to the central purpose of ABC's business.").

board's oversight function must be *more rigorously* exercised."[225] These cases seem to suggest that, at the very least, a claim is easier to bring when the alleged breach in oversight had to do with mission critical compliance issues. Under prong two of the *Caremark* framework, this means the careful observer is one whose gaze is fixed on the mission critical regulatory requirements. Under prong one, the case law is less comprehensive, with *Marchand* as the only authority on mission critical reporting systems. There, the court found the board-level reporting system was simply nonexistent. It remains to be seen how the court may evaluate a claim where a defendant has not utterly failed to establish a reporting system, but the plaintiff argues the system is faulty or implemented with something less culpable than a lack of good faith, like gross negligence. The case law was close to reaching the issue with both *Hughes v. Hu* and *Sorenson*, however the regulatory issues were not "mission critical" in those cases and thus the court was able to stay within the standard *Caremark* framework.

Notably, *Marchand* and most of its progeny were decided after the prominent case law on cybersecurity oversight liability.[226] The new ground broken by these cases presents interesting questions in the cybersecurity context: Could there be mission critical cybersecurity regulation? And would such a finding mean a claim would survive a motion to dismiss?

IV. SOLARWINDS: CYBERSECURITY AS "MISSION CRITICAL"

Now, with the reinvigoration of the *Caremark* framework in mission critical settings, Delaware is ripe for a watershed cybersecurity oversight case. Because a finding that cybersecurity is mission critical would make the claims easier for plaintiffs to bring, it could be the catalyst to push an otherwise borderline oversight case into litigious viability. But what would mission critical cybersecurity look like in a corporation? Would cybersecurity oversight be treated by the courts more like the accounting oversight in *Hughes*? Or could a corporation have a business model so dependent upon strong cybersecurity that it could be said to be "mission critical?"

225. *Clovis*, 2019 WL 4850188, at *13 (emphasis added).

226. *Marchand* was decided in June of 2019. *Marchand*, 212 A.3d at 805. *In re The Home Depot* was decided in 2016. *In re* The Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317, 1332 (N.D. Ga. 2016). *Palkon* was decided in 2014. Palkon v. Holmes, No. 2:14-CV-01234, 2014 WL 5341880, at *1 (D.N.J. Oct. 20, 2014). *Equifax* was settled soon after *Marchand*. *See* Lead Plaintiffs' Unopposed Motion for Final Approval of Shareholder Derivative Settlement, Award of Attorneys' Fees, and Reimbursement of Expenses with Memorandum of Law in Support, *supra* note 71, at 2.

SolarWinds issued a Form 8-K on December 12, 2020, announcing it had been breached by a nation-state hacker.[227] The impact on the corporation and its investors has been devastating. The market capitalization of SolarWinds has fallen by 22%.[228] To compound the issue, there are allegations of insider trading violations given that there was a high volume of trading prior to the announcement.[229]

SolarWinds is uniquely situated to be devastated by a cyber incident. The corporation itself even identified cybersecurity as one of its top threats.[230] The company explained in its February 2020 Form 10-K:

> We are heavily dependent on our technology infrastructure to sell our products and operate our business, and our customers rely on our technology to help manage their own IT infrastructure. . . .
>
> . . . .
>
> . . . The costs to us to eliminate or address the foregoing security problems and security vulnerabilities before or after a cyber incident could be significant. Our remediation efforts may not be successful and could result in interruptions, delays or cessation of service and loss of existing or potential customers that may impede sales of our products or other critical functions. We could lose existing or potential customers in connection with any actual or perceived security vulnerabilities in our websites or our products.[231]

The risk statement noted that the frequency and sophistication of the attacks appear to be increasing and acknowledges that the costs associated with the necessary cybersecurity and liability for failure are steep.[232] What the Form 10-K does not address specifically is that SolarWinds possesses a perfect confluence of factors that makes it the ideal target for a hacker.

First, SolarWinds has a massive reach; the company's CEO, Kevin Thompson, said on an earnings call in October 2020 that "[w]e don't think anyone else in the market is really even close in terms of the breadth

227. SolarWinds Corp., *supra* note 1.

228. Harwell & MacMillan, *supra* note 7.

229. *Id.* No formal investigation has been undertaken but "a former enforcement official at the U.S. Securities and Exchange Commission and an accounting expert both said the trades would likely spark an investigation by federal securities watchdogs into whether they amounted to insider trading." *Id.*

230. SolarWinds Corp., Annual Report (Form 10-K) 15 (Feb. 14, 2020), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/bfeac216-9185-4145-86f1-f2d0ad277699.pdf [https://perma.cc/ 39RV-PBXP].

231. *Id.*

232. *Id.*

of coverage we have. . . . We manage everyone's network gear."[233] Among those customers are not only federal agencies, but huge corporations with their own massive reach, like Microsoft and CISCO.[234] Second, SolarWinds's products offer hackers deep access to its customers' networks; indeed, the hackers that compromised the company used this very aspect against its targets.[235] The type of malware inserted was "'code signed' with the appropriate SolarWinds certificate" which made the backdoor much more difficult to identify because it "look[ed] like a legitimate and safe component for their Orion product."[236] The code-signed backdoor access also meant the hacker could access anything the Orion software could access; as a comprehensive IT solutions program, that usually meant the entire network.[237] Furthermore, as code-signed malware, the hackers were able to dodge the customer's firewalls.[238] A breach of this company's product could have provided hackers unfettered access to the most sensitive information in the United States.[239]

To date, there has not been a *Caremark* suit brought against the directors and officers of SolarWinds,[240] and in analyzing the SolarWinds hack from a *Caremark* and *Marchand* perspective, the Author does not purport to pass judgment on the actions that the directors or officers may or may not have taken.[241] However, despite the lack of facts available to

233. *SolarWinds Corporation (SWI) Q3 2020 Earnings Call Transcript*, MOTLEY FOOL TRANSCRIBING (Oct. 28, 2020, 4:01 AM), https://www.fool.com/earnings/call-transcripts/2020/10/28/solarwinds-corporation-swi-q3-2020-earnings-call-t/ [https://perma.cc/9VB2-GYAW].

234. Sebastian Moss, *Tech Companies Like Intel, Nvidia, Microsoft, and Cisco Installed SolarWinds Malware*, DATA CTR. DYNAMICS (Dec. 23, 2020), https://www.datacenterdynamics.com/en/news/tech-companies-intel-nvidia-microsoft-and-cisco-installed-solarwinds-malware/ [https://perma.cc/CZ3M-LFNQ].

235. Tara Seals, *The SolarWinds Perfect Storm: Default Password, Access Sales and More*, THREATPOST (Dec. 17, 2020, 4:25 PM), https://threatpost.com/solarwinds-default-password-access-sales/162327/ [https://perma.cc/TN6B-FBD8].

236. *Id.*

237. *Id.*

238. *Id.*

239. Jankowicz & Davis, *supra* note 4 (listing the Secret Service, the Department of Defense, the State Department, the Federal Reserve, and the National Security Agency among the agencies impacted by the breach).

240. Shareholders have filed several class action lawsuits including a securities fraud claim, alleging SolarWinds made misleading statements in its Form 10-K and Form 10-Q Securities and Exchange Commission filings. *See* Class Action Complaint for Violation of the Federal Securities Laws ¶ 15, Bremer v. SolarWinds Corp., No. 1:21-cv-00002 (W.D. Tex. filed Jan. 4, 2021), ECF No. 1. Two other lawsuits were filed, and the three lawsuits have been consolidated. *In re* Solarwinds Corp. Sec. Litig., No. 1:21-cv-00138 (W.D. Tex. filed Feb. 9, 2021)). None of the complaints include *Caremark* allegations.

241. One hot-button issue has been the allegation that SolarWinds's update network password was, for some amount of time, "Solarwinds123." *Id.* ¶ 20. How the 2020 breach

analyze the board or management's oversight, SolarWinds offers a useful exercise in determining what kind of a corporation might have a "mission critical" regulatory issue in cybersecurity and therefore "the board's oversight function must be more rigorously"[242] or "actively exercise[d]."[243]

The Delaware courts have described a company with one product line as having mission critical compliance issues. For example, the Supreme Court held that "one of Blue Bell's central compliance issues is food safety" because "[a]s a monoline company that makes a single product—ice cream—Blue Bell can only thrive if its consumers enjoyed its products and were confident that its products were safe to eat."[244] The chancery court reasoned that pharmaceutical company Clovis was, like Blue Bell Creameries, a "monoline company operat[ing] in a highly regulated industry" and the Clovis board's conscious disregard imperiled FDA approval of a promising drug that was "intrinsically critical to [Clovis's] business operation."[245] And, while the court noted that ABC is "a relatively more complex corporation than either Blue Bell Creameries or Clovis," because it is a "manufacturer, distributor, and packager of pharmaceutical drugs," the FDA regulations that it skirted still related to mission critical aspects of its business.[246] Meanwhile, "mission critical" analysis was not invoked by the court in *Hughes* when oversight issues related to accounting regulations of an electric vehicle battery manufacturer.[247]

Sorenson came close to the issue but ultimately lends little insight into the question of whether "mission critical" cybersecurity could exist and,

---

occurred is still unknown, but experts have hypothesized that it was not via the "SolarWinds123" password vulnerability, which was changed in 2019. Rachel Satter et al., *Hackers Used SolarWind's Dominance Against It in Sprawling Spy Campaign*, REUTERS (Dec. 15, 2020, 9:08 PM), https://www.reuters.com/article/global-cyber-solarwinds-idUSKBN28P2N8 [https://perma.cc/3NE4-VBLU]. Security experts are raising red flags about other aspects of SolarWinds cybersecurity, beyond the "SolarWinds123" issue, namely, that there are also reports that in 2017, cybercriminals were selling access to SolarWinds on dark web markets. *Id.* On two occasions in February 2021, SolarWinds leadership was called to testify about the breach in hearings before congressional committees. Christian T. Fjeld, *Hearings on the SolarWinds Hack and Possible Policy Responses*, NAT'L L. REV. (Mar. 4, 2021), https://www.natlawreview.com/article/hearings-solarwinds-hack-and-possible-policy-responses [https://perma.cc/XRJ9-2HRP].

242. *In re* Clovis Oncology, Inc. Derivative Litig., No. 2017-0222, 2019 WL 4850188, at *13 (Del. Ch. Oct. 1, 2019).

243. Teamsters Loc. 443 Health Servs. & Ins. Plan v. Chou, No. 2019-0816, 2020 WL 5028065, at *18 (Del. Ch. Aug. 24, 2020).

244. Marchand v. Barnhill, 212 A.3d 805, 809 (Del. 2019) (en banc).

245. *Clovis*, 2019 WL 4850188, at *1, *13.

246. *Teamsters*, 2020 WL 5028065, at *18.

247. *See* Hughes v. Hu, No. 2019-0112, 2020 WL 1987029, at *1 (Del. Ch. Apr. 27, 2020).

if so, what it would look like.[248] The court in *Sorenson* was presented with the argument that customer data was "mission critical" to Marriott, but the court made no specific findings on the issue.[249] The court merely commented that while Delaware courts have been considering "mission critical" components of a corporation when analyzing *Caremark* claims, cybersecurity "is an area of consequential risk that spans modern business sectors."[250] With that, the court dispensed with "mission critical" notions and provided no further analysis on the topic. Readers may rightfully wonder what relevance to attribute to the fact that cybersecurity "spans modern business sectors." While it may be true that cybersecurity spans business sectors, many such regulatory issues can be mission critical to one company and not another. A regulatory obligation should not be foreclosed from its importance to a single company merely because it is also applicable to another company.

Sorenson did not involve a company like SolarWinds. SolarWinds, like Blue Bell and Clovis, is a monoline company. SolarWinds might have different flavors of their product, but the heart of the product is network security solutions.[251] Because of the nature of their product and the entities with whom SolarWinds does business, at a minimum, SolarWinds must comply with certain government contractor-specific regulations set out by NIST;[252] as a contractor who works with the DoD, SolarWinds is also subject to additional strict requirements.[253] These requirements relate directly to the central business purpose of SolarWinds: to offer network management solutions so that their customers can ensure their networks are secure.[254] That central purpose has led SolarWinds to provide services to the nation's most sensitive entities such as the DoD and the National Security Agency.[255] As a company with only one kind of product, with cybersecurity inherent to

248. Fireman's Ret. Sys. of St. Louis v. Sorenson, No. 2019-0965, 2021 WL 4593777 (Del. Ch. Oct. 5, 2021).

249. Verified Amended Stockholder Derivative Complaint, *supra* note 191, ¶ 5.

250. *Sorenson*, 2021 WL 4593777, at *11.

251. SolarWinds Corp., *supra* note 230, at 3 ("SolarWinds is a leading provider of information technology, or IT, infrastructure management software. Our products give organizations worldwide, regardless of type, size or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments . . . . Our business is focused on building products that enable technology professionals to manage 'all things IT.'").

252. *See supra* Section II.C for discussion of the standards government contractors must meet.

253. *See supra* Section II.C.

254. SolarWinds Corp., *supra* note 230, at 3.

255. Jankowicz & Davis, *supra* note 4.

its survival as a corporation, cybersecurity compliance is mission critical for SolarWinds.[256]

CONCLUSION

The unmatched cybersecurity breach that rocked SolarWinds demonstrates the potential for a finding of mission critical cybersecurity even in the face of *Sorenson*'s lukewarm rejection of the notion. Because such a finding makes *Caremark* claims easier for plaintiffs to bring, it could be the catalyst to push an otherwise borderline oversight case into the litigiously viable space. Thus, with the path laid out by *Marchand* and its progeny, the writing is on the [fire]wall: Delaware is primed for "mission critical" cybersecurity litigation.

Yet, it should be remembered that the existence of "mission critical" cybersecurity oversight is not an automatic boon to plaintiffs. Although such a finding may make bringing a claim slightly easier, it does not allow plaintiffs to skirt the difficult pleading requirements that were the death knell for *Palkon* or the protection of the business judgment rule that shielded defendants in *In re The Home Depot*. A finding of "mission critical" regulation will only mean the courts will require the board's oversight function to be "more rigorously"[257] or "actively exercise[d]"[258] to avoid derivative liability. In some situations, it may not matter how rigorously oversight was exercised, a cybersecurity breach may be inevitable.

Conversely, those companies who might not so strongly depend on tight cybersecurity for their continued existence will not receive a free pass either. Like Marriott and its customer data or Kandi Technologies and the accounting regulations, many companies simply won't have "mission critical" cybersecurity. However, the standard *Caremark* framework will still apply. And, as *Hughes* demonstrates, it is still

256. The best counterargument to this conclusion is that SolarWinds does not operate in a "highly regulated industry." *In re* Clovis Oncology, Inc. Derivative Litig., No. 2017-0222, 2019 WL 4850188, at *1 (Del. Ch. Oct. 1, 2019). As discussed in Part II, however, this patchwork framework of cybersecurity regulations has not stopped chancery courts from considering *Caremark* claims in the past. Delaware courts have not yet taken up the issue of how regulated an industry must be to be considered "highly regulated" for the purposes of "mission critical." The courts have also not given guidance in the *Marchand* progeny about the conceptual role that the industry's level of regulation plays on the question. Arguably, the relevant inquiry is met by the other factors inherent in a *Caremark* claim. If a corporation is subject to regulations that strike at the heart of its central business purpose, the directors and officers of that corporation should be required to more rigorously exercise oversight over the implementation of those regulations. The number of industry-wide regulations should not be relevant to the inquiry as it is the actions of the board, not the actions of others, that have an impact on *Caremark* liability.

257. *Clovis*, 2019 WL 4850188, at *13.

258. Teamsters Loc. 443 Health Servs. & Ins. Plan v. Chou, No. 2019-0816, 2020 WL 5028065, at *18 (Del. Ch. Aug. 24, 2020).

possible to bring a *Caremark* claim without invoking "mission critical" analysis.

As the importance of cybersecurity increases, and especially if the federal government institutes sweeping private-sector cybersecurity regulation, the threat of cybersecurity oversight derivative litigation may simply become a fact of life for corporate governance.