MISSION CRITICAL: *CAREMARK*, BLUE BELL, AND DIRECTOR RESPONSIBILITY FOR CYBERSECURITY GOVERNANCE

H. JUSTIN PACE* &
LAWRENCE J. TRAUTMAN**†

If the potential for *Caremark* liability hangs like the sword of Damocles over corporate directors of Delaware corporations, then that sword has been considerably more secure than that of the original myth. For decades, Chancellor Allen's description of a *Caremark* claim as "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment" held true. *Caremark* claims that survived a motion to dismiss were for decades few and far between. That changed in 2019. In the space of little over two years, Delaware courts have allowed five *Caremark* claims to survive a motion to dismiss. The thread holding that sword is beginning to look more like the single horsehair of the myth. The scope and likelihood of *Caremark* liability are matters of considerable interest and concern for directors. Under most circumstances, a board doing its job poorly is relevant only to the directors' duty of care and protected by the business judgment rule, exculpatory provisions under Section 102(b)(7), and advancement and indemnification. Failure to monitor under *Caremark*, however, is a breach of the duty of loyalty—a duty not protected by the business judgment rule. It cannot be exculpated, and it cannot be covered by indemnification.

This Article makes four key arguments. First, black letter *Caremark* doctrine has not changed, but it is newly reinvigorated, and the risks of *Caremark* liability for directors are greater than just a few years ago. Second, future *Caremark* liability will be centered on failure to provide board-level oversight of mission critical risks. Third, cybersecurity is mission critical to effectively *all* large companies today. Fourth, the risk of *Caremark* liability can be mitigated by taking a few simple steps to ensure that the board is

---

* BSBA, Western Carolina University; M.Acc, North Carolina State University; J.D., Northwestern University Pritzker School of Law. Mr. Pace is Assistant Professor of Business Law at Western Carolina University. He may be contacted at hpace@wcu.edu.

** BA, The American University; MBA, The George Washington University; J.D., Oklahoma City University School of Law. Mr. Trautman is Associate Professor of Business Law and Ethics at Prairie View A&M University. He may be contacted at Lawrence.J.Trautman@gmail.com.

† The authors wish to extend particular thanks to the following: the organizers of the 2021 Southeastern Academy of Legal Studies Conference and those judges who selected this paper as winner of the Best Proceedings Paper Award, Professor Robert Thomas and participants in the 2022 University of Florida Huber Hurst Legal Research Seminar, Tabrez Ebrahim, and Jessica Zeldin for their helpful comments on draft versions of this article.

addressing cybersecurity. This Article is the first to make these arguments together and the first to make the final argument.

INTRODUCTION

If the potential for *Caremark* liability for failures of oversight hangs like the sword of Damocles over corporate directors of Delaware corporations, then that sword has been considerably more secure than that of the original myth. For decades, Chancellor Allen's description of a *Caremark* claim as "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment"[1] held true. *Caremark* claims that survived a motion to dismiss were for decades few and far between.[2] That changed in 2019. In the space of little over two

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

2. There were as few as six over the course of the twenty-three years between *Caremark* and *Marchand*. *Stewart v. Wilmington Tr. SP Servs., Inc.*, 112 A.3d 271 (Del. Ch. 2015); *In re China Agritech, Inc. S'holder Deriv. Litig.*, No. 7163-VCL, 2013 WL 2181514 (Del. Ch. May 21, 2013); *Rich ex rel. Fuqi Int'l, Inc. v. Yu Kwai Chong*, 66 A.3d 963 (Del. Ch. 2013); *In re Am. Int'l Grp., Inc.*, 965 A.2d 763 (Del. Ch. 2009); *ATR-Kim Eng Fin. Corp. v. Araneta*, No. 489-N, 2006 WL 3783520 (Del. Ch. Dec.

years, Delaware courts have allowed five *Caremark* claims to survive in the corporation context[3] (along with one claim in the limited partnership context).[4] The thread holding that sword is beginning to look more like the single strand of horsehair of myth.

Under what has come to be known as a *Caremark* claim, corporate directors who fail to provide adequate oversight may be held liable for breaching fiduciary duties they owed the corporation. *Caremark* claims typically arise where corporate employees caused the corporation to engage in some unlawful conduct, and plaintiffs allege the unlawful conduct would not have taken place had directors acted properly. There are two types of *Caremark* claims: failure to implement ("Type I") claims and failure to monitor ("Type II") claims. Under a Type I claim, the plaintiff alleges that "the directors utterly failed to implement any reporting or information system or controls."[5] Under a Type II claim, the plaintiff alleges that although the board implemented controls It "consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."[6] Conscious disregard is necessary;[7] *Caremark* is a high bar.

The scope and likelihood of *Caremark* liability are matters of considerable interest and concern for directors. Under most circumstances, a board doing its job poorly is relevant only to the directors' duty of care and protected by the business judgment rule, exculpatory provisions under Section 102(b)(7),[8] and advancement and indemnification. Failure to monitor under *Caremark*, however, is a breach of the duty of loyalty.[9] A breach of the duty of loyalty is not

---

21, 2006), *aff'd sub nom. Araneta v. ATR-Kim Eng Fin. Corp.*, 930 A.2d 928 (Del. 2007); *Saito v. McCall*, No. 17132-NC, 2004 WL 3029876 (Del. Ch. Dec. 20, 2004), *overruled on other grounds by Lambrecht v. O'Neal*, 3 A.3d 277 (Del. 2010).

3. *Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019); *In re The Boeing Co. Deriv. Litig.*, No. 2019-0907-MTZ, 2021 WL 4059934 (Del. Ch. Sept. 7, 2021); *Teamsters Local 443 v. Chou*, No. 2019-0816-SG, 2020 WL 5028065 (Del. Ch. Aug. 24, 2020); *Hughes v. Hu*, No. 2019-0112-JTL, 2020 WL 1987029 (Del. Ch. April 27, 2020); *In re Clovis Oncology, Inc. Deriv. Litig.*, No. 2017-0222-JRS, 2019 WL 4850188 (Del. Ch. Oct. 1, 2019).

4. *Inter-Marketing Grp. USA, Inc. v. Armstrong*, No. 2017-0030-TMR, 2020 WL 756965 (Del. Ch. Jan. 31, 2020).

5. *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006).

6. *Id.*

7. *See In re Walt Disney Co. Deriv. Litig.*, 906 A.2d 27, 62 (Del. 2006) ("[T]he concept of *intentional dereliction of duty*, a *conscious disregard for one's responsibilities*, is an appropriate (although not the only) standard for determining whether fiduciaries have acted in good faith.") (emphasis in original).

8. DEL. CODE ANN. tit. 8, § 102(b)(7) (2016).

9. *Guttman v. Huang*, 823 A.2d 492, 506 (Del. Ch. 2003) ("[D]irectors breach[] their duty of loyalty by failing to attend to their duties in good faith.").

protected by the business judgment rule. It cannot be exculpated.[10] And it cannot be covered by indemnification.[11]

In 2019, *Caremark* faced an abrupt shift in application, if not in theory. In June of that year, the Supreme Court of Delaware reversed a decision by the Delaware Court of Chancery (Chancery Court) dismissing a claim against the directors of Blue Bell Creameries, Inc. (Blue Bell) under *Caremark*.[12] Blue Bell is a manufacturer and seller of ice cream, and the plaintiffs' *Caremark* claim alleged that the board failed to implement food safety controls.[13] Blue Bell's alleged poor food safety practices led to a listeria outbreak that claimed three lives.[14] Notably, the Delaware Supreme Court emphasized that Blue Bell Creameries is a single product company and thus food safety is existential.[15]

The Chancery Court took the Delaware Supreme Court's hint. Within a little over two years, the Chancery Court would sustain *Caremark* claims in four cases.[16] In *Clovis*, the Chancery Court sustained a *Caremark* claim against directors of a pharmaceutical company who allowed the company to misrepresent the clinical trial success of one of its three drugs.[17] In *Hughes*, the Chancery Court sustained a *Caremark* claim against directors of a Chinese company incorporated in Delaware that suffered from severe and pervasive accounting issues.[18] In *Chou*, the Chancery Court sustained a *Caremark* claim against directors of a large pharmaceutical company who allowed an indirect subsidiary to

---

10. *See* DEL. CODE ANN. tit. 8, § 102(b)(7) ("[T]he certificate of incorporation may also contain . . . [a] provision eliminating or limiting the personal liability of a director or officer to the corporation . . . for monetary damages for breach of fiduciary duty as a director or officer, provided that such provision shall not eliminate or limit the liability of . . . [a] director or officer for acts or omissions not in good faith . . . .").

11. *Hermelin v. K-V Pharm. Co.*, 54 A.3d 1093, 1111 (Del. Ch. 2012) ("Sections 145(a) and (b) of the DGCL permit a corporation to indemnify [a director] so long as 'the person acted in good faith and in a manner the person reasonably believed to be in or not opposed to the best interests of the corporation, and, with respect to any criminal action or proceeding, had no reasonable cause to believe the person's conduct was unlawful.'") (citing DEL. CODE ANN. tit. 8, § 145(a)–(b) (2016)).

12. *Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019).

13. *Id.* at 807.

14. *Id.* at 814.

15. *See, e.g.*, *id.* at 809 ("As 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.").

16. *In re The Boeing Co. Deriv. Litig.*, No. 2019-0907-MTZ, 2021 WL 4059934 (Del. Ch. Sept. 7, 2021); *Teamsters Local 443 Health Servs. & Insur. Plan v. Chou*, No. 2019-0816-SG, 2020 WL 5028065 (Del. Ch. Aug. 24, 2020); *Hughes v. Hu*, No. 2019-0112-JTL, 2019 WL 1987029 (Del. Ch. Apr. 27, 2020); *In re Clovis Oncology, Inc. Deriv. Litig.*, No. 2017-0222-JRS, 2019 WL 4850188 (Del. Ch. Oct. 1, 2019).

17. *Clovis*, 2019 WL 4850188, at *1.

18. *Hughes*, 2019 WL 1987029, at *1.

essentially operate a criminal enterprise.[19] And in *Boeing*, the Chancery Court sustained a *Caremark* claim against directors of an airplane manufacturer who disregarded safety issues.[20]

There are three plausible interpretations of *Marchand* and the four Chancery Court cases that followed in its wake. First, the newly reinvigorated *Caremark* doctrine is only dangerous for monoline companies. Second, it is only dangerous for companies in highly regulated industries (and perhaps only companies regulated by the Food and Drug Administration (FDA)). The third, and most plausible, interpretation is that the newly reinvigorated *Caremark* doctrine will be limited to "mission critical" operations.[21]

Cybersecurity—encompassing data security, anti-hacking, data privacy, and more[22]—has become just such a mission critical risk for large corporations.[23] Cybersecurity incidents appear in the news at an alarming and increasing rate. In 2016, Yahoo announced data breaches affecting a combined 1.5 billion user accounts.[24] Yahoo settled a derivative lawsuit for $29 million,[25] and paid out almost $145 million

19. *Chou*, 2020 WL 5028065, at *2.

20. *Boeing*, 2021 WL 4059934, at *1.

21. "Mission critical" is a term introduced but not expressly defined by *Marchand* and picked up by later *Caremark* cases. *Marchand v. Barnhill*, 212 A.3d 805, 824 (Del. 2019); *see also Boeing*, 2021 WL 4059934 (using the term six times); *Chou*, 2020 WL 5028065 (using the term twenty-two times); *Clovis*, 2019 WL 4850188 (using the term six times).

22. *See* JEFF KOSSEFF, CYBERSECURITY LAW, at xxiv–xxv (John Wiley & Sons, Inc., 2d ed. 2020); *see also* Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who and How It Works*, 5 J.L. & CYBER WARFARE 147, 151 (2016) ("The terms cybersecurity and cyberattack have become broadly used without widespread acceptance as to their exact meaning.").

23. *See Firemen's Ret. Sys. of St. Louis v. Sorenson (Marriott)*, No. 2019-0965-LWW, 2021 WL 4593777, at *1 (Del. Ch. Oct. 5, 2021) ("Cybersecurity has increasingly become a central compliance risk deserving of board level monitoring at companies across sectors.").

24. Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach*, 66 AM. U. L. REV. 1231, 1262 (2017) (citing Hayley Tsukayama, Craig Timberg & Brian Fung, *Yahoo Data Breach Casts "Cloud" over Verizon Deal*, WASH. POST: THE SWITCH (Sept. 22, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/09/22/report-yahoo-to-confirm-data-breach-affecting-hundreds-of-millions-of-accounts [https://perma.cc/UA5K-XLUB]); Vindu Goel & Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html [https://perma.cc/89VA-ESJG].

25. Craig A. Newman, *Lessons for Corporate Boardrooms from Yahoo's Cybersecurity Settlement*, N.Y. TIMES: DEALBOOK (Jan. 23, 2019), https://www.nytimes.com/2019/01/23/business/dealbook/yahoo-cyber-security-settlement.html [https://perma.cc/XHE6-E67Z]; Kevin M. LaCroix, *Equifax Data Breach-Related Securities Suit Settled for $149 Million*, THE D&O DIARY (Feb. 17,

combined for various claims.[26] The $29 million settlement is notable in part because $11 million of that $29 million went to the plaintiffs' attorneys' fees.[27] The proven potential to recover attorneys' fees gives entrepreneurial plaintiffs' attorneys an incentive to pursue claims for failure to monitor after high-profile data breaches are announced.[28] Equifax agreed to pay $149 million to settle securities litigation after a cyberbreach—"the largest ever cybersecurity-related securities class action settlement."[29]

Cyberattacks have not slowed. Two thousand twenty saw "the Pearl Harbor of American IT," when the SolarWinds Corporation (SolarWinds) hack infiltrated over 18,000 government and private networks.[30] Oil and gas company Colonial Pipeline was forced to both shut down pipeline operations and information technology systems for several days and pay $4.4 million after a ransomware attack in the first half of 2021.[31] Colonial Pipeline supplies almost half the gasoline and diesel for the East Coast of the United States, and even a short shutdown had a ripple effect that disrupted fuel prices and availability in the eastern U.S. for weeks.[32] As a result of the ransomware attack, Colonial Pipeline

---

2020), https://www.dandodiary.com/2020/02/articles/securities-litigation/equifax-data-breach-related-securities-suit-settled-for-149-million [https://perma.cc/RW67-DXNP].

26. *See* LaCroix, *supra* note 25.

27. *See* Newman, *supra* note 25; LaCroix, *supra* note 25.

28. *See* LaCroix, *supra* note 25 ("While the outcome of the pending cases remains to be seen, the fact is that the significant recovery in the Yahoo data breach derivative suit could well encourage other claimants to file similar lawsuits in the future.").

29. *Id.*

30. Steven Vaughan-Nichols, *SolarWinds: The More We Learn, the Worse It Looks*, ZDNET (Jan. 4, 2021), https://www.zdnet.com/article/solarwinds-the-more-we-learn-the-worse-it-looks; *see also* Tabrez Y. Ebrahim, *National Cybersecurity Innovation*, 123 W. VA. L. REV. 483, 485 (2020) ("Following Stuxnet, in 2012, U.S. Secretary of Defense Leon Panetta warned that the U.S. was vulnerable to a 'cyber Pearl Harbor' . . . ."); Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L., TECH. & POL'Y 341, 347; Lawrence J. Trautman, *Is Cyberattack The Next Pearl Harbor?,* 18 N.C. J.L. & TECH. 233, 235 (2016).

31. Charlie Osborne, *Colonial Pipeline CEO: Paying DarkSide Ransom Was The 'Right Thing to Do for The Country,'* ZDNET (May 20, 2021), https://www.zdnet.com/article/colonial-pipeline-ceo-paying-darkside-ransom-was-the-right-thing-to-do-for-the-country; *see generally* Lawrence J. Trautman & Peter C. Ormerod, *WannaCry, Ransomware, and the Emerging Threat to Corporations*, 86 TENN. L. REV. 503, 507–11 (2019) (discussing the history of ransomware as a tool against corporations).

32. David E. Sanger, Clifford Krauss & Nicole Perlroth, *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, N.Y. TIMES, https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html [https://perma.cc/XTK8-8A7U] (May 13, 2021).

faced two class action lawsuits[33] and a lawsuit brought by a gas station owner seeking $5 million.[34] IT firm Kaseya suffered a cyberattack on its remote-monitoring and management tool that compromised an estimated "800 to 1500 small to medium-sized companies" in mid-2021.[35] It took nine days for Kaseya to get customers back live.[36] It took another eleven days for Kaseya to obtain a decryptor that would allow affected customers to restore their data.[37] "A Russia-linked criminal gang" demanded $70 million from Kaseya (in Bitcoin) for a decryptor.[38] After the fact, several employees claimed "they flagged wide-ranging cybersecurity concerns to company leaders" but alleged that the issues were not resolved.[39] Companies that house sensitive data of many other companies pose a particular risk.[40]

Vulnerability intelligence expert Brian Martin observed that, "Every company in the world that uses technology relies on both hardware and software from sources out of their control . . . [that] likely come from Malaysia, Indonesia, and Taiwan while software comes from all over the world."[41] Whether these components and software can be trusted is an irrelevant question since there is no practical alternative.[42] Mr. Martin stated, "[w]ith more software using some form of automatic updates, the compromise of the parent company [like in SolarWinds] may pose a risk

---

33. Complaint, *EZ Mart 1, LLC v. Colonial Pipeline Co.*, No. 21-cv-02522-MHC (N.D. Ga. Jun. 21, 2021); Complaint, *Dickerson v. CDPQ Colonial Partners, L.P.*, No. 21-cv-02098-MHC (N.D. Ga. May 18, 2021).

34. *North Carolina Gas Station Owner Sues Colonial Pipeline for Losses After Ransomware Attack*, WTVD-TV RALEIGH-DURHAM (June 22, 2021), https://abc11.com/colonial-pipeline-gas-prices-shortage/10821125 [https://perma.cc/NCJ7-8XZV].

35. Charlie Osborne, *Updated Kaseya Ransomware Attack FAQ: What We Know Now*, ZDNET (July 23, 2021), https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now.

36. *Updates Regarding VSA Security Incident*, KASEYA, https://www.kaseya.com/potential-attack-on-kaseya-vsa [https://perma.cc/X57T-MVWF] (July 26, 2021, 1:00 PM).

37. *Id.*

38. Ryan Gallagher & Andrew Martin, *Kaseya Failed to Address SecurityBefore Hack, Ex-Employees Say*, BLOOMBERG (July 10, 2021, 7:00 AM), https://www.bloomberg.com/news/articles/2021-07-10/kaseya-failed-to-address-security-before-hack-ex-employees-say [https://perma.cc/6F45-LM9M].

39. *Id.*

40. *See, e.g.*, Brian Fung, *Ransomware Hits Law Firm with Dozens of Major Corporate Clients*, CNN BUSINESS, https://www.cnn.com/2021/07/19/tech/ransomware-law-firm/index.html [https://perma.cc/JW72-UD73] (July 19, 2021, 4:40 PM) (reporting on a ransomware attack affecting a law firm that was serving "over a dozen sectors of the economy," including "a large array of Fortune 500 companies").

41. Brian Martin, *Sharks Are Scary but Worry About Mosquitos*, *in* 2021 MID YEAR REPORT: VULNERABILITY QUICKVIEW 4, 5 (2021).

42. *Id.* at 5.

. . . . However, the alternative is not enabling automatic updates and creating a process to verify those patches before they are deployed."[43]

Corporate boards are responsible for cybersecurity.[44] Directors have a duty to ensure the corporation takes reasonable measures to protect corporate data.[45] This duty has legal teeth to it, including by federal and state statute.[46] Personal liability for breaches of the duty of care, however, are of limited concern for directors because they are protected by the business judgment rule, corporate indemnification, and Section 102(b)(7) exculpatory provisions.[47] The newly increased risk of *Caremark* liability drastically changes the landscape for potential liability because failure to properly monitor cybersecurity can violate the duty of loyalty.[48]

The boards of U.S. publicly traded companies are not rising to the task—only six percent have a compliance committee.[49] A large majority of C-suite IT executives grade their board's performance on cybersecurity as fair or poor.[50] Boards also suffer from a lack of cybersecurity subject matter expertise relative to other areas like strategy or the competitive landscape.[51] This is not to say that cybersecurity is not

---

43. *Id.*

44. *See* Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. MARSHALL J. COMPUT. & INFO. L. 313, 328 (2011) ("Simply put, IT governance and the effective application of an IT governance framework are the responsibilities of the board of directors and executive management.").

45. Trautman & Ormerod, *supra* note 24, at 1234–35, 1239 (citing THOMAS J. SMEDINGHOFF, INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE 39 (2008)).

46. *Id.* at 1235–38 (discussing statutory obligations to protect corporate data).

47. *See generally* H. Justin Pace, *Rogue Corporations: Unlawful Corporate Conduct and Fiduciary Duty*, 85 MO. L. REV. 1, 6, 8–9 (2020).

48. *Id.* at 10.

49. *See* John Armour, Brandon Garrett, Jeffrey Gordon & Geeyoung Min, *Board Compliance*, 104 MINN. L. REV. 1191, 1225 (2020) [hereinafter, Armour, *Board Compliance*]. *But see Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025*, GARTNER (Jan. 28, 2021) [hereinafter Gartner Jan. 28, 2021 Press Release], https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated- [https://perma.cc/S3V2-DXM2].

50. Teresa L. Johnson & Ben Fackler, *2020 in Hindsight: Key Considerations for Directors in 2021*, HARV. L. SCH. F. ON CORP. GOV. (Apr. 7, 2021), https://corpgov.law.harvard.edu/2021/04/07/2020-in-hindsight-key-considerations-for-directors-in-2021 [https://perma.cc/Y7AR-ZY6S].

51. *Id.* ("[W]hen executives were asked to grade their Board's subject matter expertise, IT/digital/data privacy and cyber risk expertise were at the bottom."); PricewaterhouseCoopers LLP and The Conference Board, *Board Effectiveness: A Survey of the C Suite*, PRICEWATERHOUSECOOPERS LLP 21 (Nov. 2021), https://www.pwc.com/us/en/services/governance-insights-center/pwc-board-effectiveness-a-survey-of-the-c-suite-final.pdf

recognized as mission critical. Over sixty percent of surveyed "governance specialists" recognized cybersecurity as an elevated and "strategic, enterprise-wide risk."[52] In a separate survey, technology skills and experience (including specifically in the cybersecurity context) were identified as important in the selection of directors more often than leadership experience, industry knowledge, and financial expertise.[53] A prominent commentator in the directors' and officers' (D&O) liability insurance space identified cybersecurity as one of the top ten D&O stories of 2020 and 2021.[54] The COVID-19 pandemic led to many more employees working remotely and business being conducted virtually, creating issues demanding board-level attention.[55]

Fiduciary duties require corporate directors to act in the best interest of the corporation, not society as a whole. Fiduciary obligation law is a "blunt . . . tool to encourage good corporate citizenship."[56] It is poorly suited for advancing social goals when the corporation's interest and the

---

52. NAT'L ASS'N OF CORP. DIRS. & INTERNET SEC. ALL., CYBER-RISK OVERSIGHT 2020: KEY PRINCIPLES AND PRACTICAL GUIDANCE FOR CORPORATE BOARDS 4, 66 (2020), http://isalliance.org/wp-content/uploads/2020/02/RD-3-2020_NACD_Cyber_Handbook__WEB_022020.pdf [https://perma.cc/VUF5-UF7T] (citing Jamie Smith & Bridget Neill, *What Companies Are Sharing About Cybersecurity Risk and Oversight*, EY CTR. FOR BD. MATTERS (Oct. 1, 2019), https://www.ey.com/en_us/board-matters/what-companies-are-sharing-about-cybersecurity-risk-and-oversight [https://perma.cc/YG5Q-N4UJ]). *See also Firemen's Ret. Sys. of St. Louis v. Sorenson*, No. 2019-0965-LWW, 2021 WL 4593777, at *3 (Del. Ch. Oct. 5, 2021) ("Cybersecurity was viewed by the Board as the second biggest risk facing Marriott for fiscal year 2017.").

53. Richard Alsop, Doreen Lilienfield & Gillian Moldowan, *Corporate Governance & Executive Compensation Survey 2021*, HARV. L. SCH. F. ON CORP. GOV. (Dec. 1, 2021), https://corpgov.law.harvard.edu/2021/12/01/corporate-governance-executive-compensation-survey-2021 [https://perma.cc/9PCG-UVHM].

54. LaCroix also flagged the increased risk of *Caremark* liability. Kevin LaCroix, *The Top Ten D&O Stories of 2021*, D&O DIARY (Jan. 3, 2022), https://www.dandodiary.com/2022/01/articles/director-and-officerliability/the-top-ten-do-stories-of-2021 [https://perma.cc/ELX6-SSHM]; Kevin LaCroix, *The Top Ten D&O Stories of 2020*, D&O DIARY (Jan. 4, 2021), https://www.dandodiary.com/2021/01/articles/director-and-officer-liability/the-top-ten-do-stories-of-2020 [https://perma.cc/YV4G-45CE].

55. *See, e.g.*, Jane Goldstein, Daniel Lim & Kenneth Monroe, *Director Oversight Duties Amidst COVID-19*, HARV. L. SCH. F. ON CORP. GOV. (May 8, 2020), https://corpgov.law.harvard.edu/2020/05/08/director-oversight-duties-amidst-covid-19 [https://perma.cc/ZYD4-D4ME] ("As more employees work remotely and by necessity business is conducted virtually, the board and management should consider whether the company's IT systems have enough capacity to support the growing virtual environment. Should management hire consultants to consider alternative communication platforms? In addition, are proper cybersecurity protection measures, policies, and contingency plans in place? Do the employees working remotely have proper cybersecurity training and are they aware of the company's internal communication protocols and policies? Do those protocols and policies need to be updated?").

56. *Teamsters Loc. 443 Health Servs. & Ins. Plan v. Chou*, No. 2019-0816-SG, 2020 WL 5028065, at *1 (Del. Ch. Aug. 24, 2020).

common interest are not aligned. A reinvigorated *Caremark* doctrine applied to cybersecurity is not *necessarily* in the best interests of either the corporation or society. But an invigorated *Caremark* doctrine will incentivize directors to provide oversight for mission critical operations, and cybersecurity has become mission critical for every large company. Cybersecurity is also strategically important,[57] so the impact on the fundamental board trade-off between strategy and oversight would be mitigated. Cybersecurity is also the subject of increasing public interest; better incentives for corporations to invest in cybersecurity will benefit society. Good faith is especially prosocial relative to other aspects of director fiduciary duty. Though shareholder wealth maximization is the expectation, the board is not allowed to manage the corporation "in an illegal fashion," even if the directors believe "that the illegal activity will result in profits."[58] Cyber incidents have not traditionally resulted in liability for directors on the basis that they failed to provide proper oversight;[59] that may soon change.

This Article makes four key arguments. First, black letter *Caremark* doctrine has not changed, but it is newly reinvigorated, and the risks of *Caremark* liability for directors is greater than just a few years ago. Second, future *Caremark* liability will be centered on failure to provide board-level oversight of mission critical risks. Third, cybersecurity is mission critical to effectively *all* large companies today. Fourth, the risk of *Caremark* liability can be mitigated by taking a few simple steps to ensure that the board addresses cybersecurity. This Article is the first to make these arguments together and the first to make the final argument.

Part I details the increase in cyber risk and attacks over the last several years. Part II details the evolution of *Caremark* doctrine. Part

---

57. *See generally* NAT'L ASS'N OF CORP. DIRS. & INTERNET SEC. ALL, *supra* note 52 (noting "a welcomed and necessary shift [towards] increased emphasis on cybersecurity as a strategic, enterprise-wide risk").

58. *Metro Commc'n Corp. BVI v. Advanced Mobilecomm Techs. Inc.*, 854 A.2d 121, 131 (Del. Ch. 2004); see also Elizabeth Pollman, *Corporate Oversight and Disobedience*, 72 VAND. L. REV. 2013, 2026 (2019) ("The requirement of fidelity to the law aims to protect society's interests, not those of the corporation.").

59. *See, e.g.*, *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, No. 19-md-2879, 2021 WL 2401641, at *14, *19 (D. Md. June 11, 2021) (declining to exercise supplemental jurisdiction and dismissing without prejudice oversight claim under Delaware law tied to data breach); *In re The Home Depot, Inc. S'holder Deriv. Litig.*, 223 F. Supp. 3d 1317, 1325–27 (N.D. Ga. 2016) (dismissing *Caremark* claim under Delaware law that alleged directors failed to appropriately respond to data breach); *In re Target Corp. Deriv. Litig.*, No. 14-cv-203-PAM-JJK (D. Minn. July 7, 2016) (dismissing oversight claim under Minnesota law); *Palkon v. Holmes*, No. 14-cv-01234-SRC, 2014 WL 5341880, at *1, *6 n.1 (D.N.J. Oct. 20, 2014) (dispensing with a *Caremark* claim under Delaware law in a footnote in litigation after Wyndham Worldwide Corporation data breach); *see also* Benjamin P. Edwards, *Cybersecurity Oversight Liability*, 35 GA. ST. U. L. REV. 663, 671–76 (2019) (discussing the Wyndham, Target, Home Depot, and Yahoo data breach derivative lawsuits).

II(a) looks at the *Caremark* decision and the doctrine as originally laid out in that opinion. Part II(b) surveys a decades-long stretch where *Caremark* was "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment"[60] and discusses the evolution of black letter *Caremark* doctrine into its current form in *Stone v. Ritter*.[61] Part II(c) analyzes the Delaware Supreme Court's decision in *Marchand v. Barnhill*,[62] which overturned a Chancery Court decision dismissing a *Caremark* claim[63] and newly reinvigorated *Caremark* doctrine. Part II(d) looks at four subsequent Chancery Court opinions refusing to dismiss a *Caremark* claim. Part III reassesses *Caremark* doctrine after that line of cases. Part IV looks at technological challenges to corporate governance. Part V considers the board-level cybersecurity oversight required under *Caremark*'s good faith standard in the wake of *Marchand*. Part VI concludes with brief thoughts on the potential for *Caremark* liability in the ESG (Environmental, Social, and Governance) context more generally.

I. CYBER RISK AND ATTACKS INCREASE

Reports of cyberattack and ransomware demands have now become almost a daily occurrence.[64] Many excellent accounts of the increased threat are available, and, given the space constraints for any one law review article, we will not replicate them here.[65]

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

61. 911 A.2d 362, 368–70 (Del. 2006).

62. 212 A.3d 805 (Del. 2019).

63. *Marchand v. Barnhill*, No. 2017-0586-JRS, 2018 WL 4657159, at *16–19 (Del. Ch. Sept. 27, 2018).

64. *See, e.g.*, David Uberti, *Iowa Grain Cooperative Hit by Cyberattack Linked to Ransomware Group,* WALL ST. J., (Sept. 20, 2021, 5:22 PM), https://www.wsj.com/articles/iowa-grain-cooperative-hit-by-cyberattack-linked-to-ransomware-group-11632172945 [https://perma.cc/B2J9-SY7R].

65. *See generally 2020 Year End Report*, RISK BASED SECURITY 3 (2021).

A. Recent Assessment

Although COVID-19 during early 2020 may have caused a brief disruption in the "vulnerability landscape, where the number of reported vulnerabilities fell dramatically[,]" by the end of 2020, "the average number of vulnerabilities . . . reached almost 70 per day, with a high of 384 in a single day."[66] In addition, "patches from Microsoft, Oracle, and other major vendors were released on the same day, account[ing] for around 7% of all disclosed vulnerabilities in 2020."[67] Below, Exhibit 1 discloses vulnerabilities from 2013 to 2020.

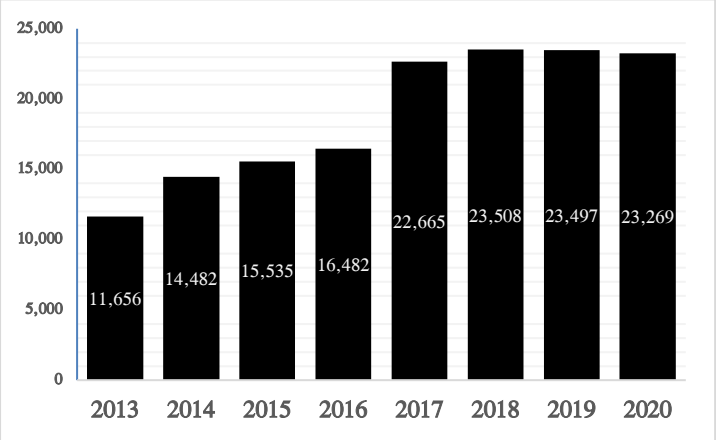

Exhibit 1: Vulnerabilities for the 2013 to 2020 Period.[68]

During the first six months of 2021, "Risk Based Security's VulnDB team aggregated an average of 80 new vulnerabilities per day . . . also updated an average of 200 existing vulnerability entries per day as new solution information, references, and additional metadata became available."[69] We learn that "1,425 vulnerabilities disclosed in the first half of 2021 are remotely exploitable vulnerabilities that have a public exploit and have a mitigating solution. . . . In addition, Risk Based Security has found an additional 849 vulnerabilities that are remotely exploitable but do not have a mitigating solution."[70] The Kaseya and SolarWinds compromises focus attention on the vulnerability of industry

66. *Id.*
67. *Id.*
68. *Id.* at 7.
69. RISKBASED SECURITY, 2021 MID YEAR REPORT: VULNERABILITY QUICKVIEW 2 (2021).
70. *Id.*

to supply chain attacks.[71] Below, Exhibit 2 discloses the number of vulnerabilities reported by Q2 for the 2017 to 2021 period.

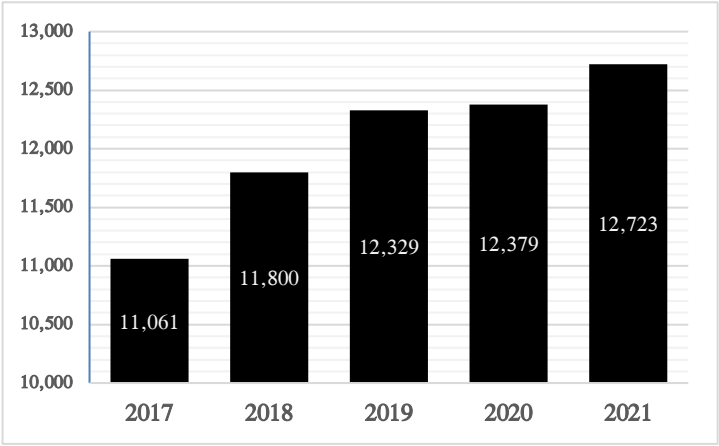

Exhibit 2: Vulnerabilities Reported by Q2 from 2017 to 2021.[72]

II. THE EVOLUTION OF THE *CAREMARK* DOCTRINE

Directors of a corporation owe fiduciary duties to that corporation. Those duties are owed to the corporation itself, not to its shareholders, but shareholders can often bring a suit for breach of duty on behalf of the corporation via a derivative suit.[73] The fiduciary duties owed by directors have traditionally been grouped into a duty of care and a duty of loyalty.[74] Due to the protection afforded by the business judgment rule and Section 102(b)(7), it is only the duty of loyalty that creates any serious risk of liability for directors.[75] Over time, the duty of loyalty doctrine has

71. Martin, *supra* note 41, at 5.

72. 2021 MID YEAR REPORT, *supra* note 69, at 7 fig.1.

73. Roy Shapira, *A New* Caremark *Era: Causes and Consequences*, 98 WASH. U. L. REV. 1857, 1862 n.17 (2021) ("To bring a derivative claim, the plaintiff first has to make a demand on the company's board to pursue that claim. To survive the demand-requirement stage, plaintiffs practically need to convince the courts that a demand is futile because the company's board cannot be trusted to make the right decision—because directors themselves face a significant threat of personal liability, for example.") (first citing *Aronson v. Lewis*, 473 A.2d 805, 811–12 (Del. 1984), *overruled in part by Brehm v. Eisner*, 746 A.2d 244, 253–54 (Del. 2000); then citing *Rales v. Blasband*, 634 A.2d 927, 930 (Del. 1993)).

74. Claire A. Hill & Brett H. McDonnell, Stone v. Ritter *and the Expanding Duty of Loyalty*, 76 FORDHAM L. REV. 1769, 1771 (2007); Lisa M. Fairfax, *Managing Expectations: Does the Directors' Duty to Monitor Promise More than It Can Deliver*, 10 U. ST. THOMAS L.J. 416, 419 (2012) (citing Julian Velasco, *How Many Fiduciary Duties Are There in Corporate Law?*, 83 S. CAL. L. REV. 1231, 1232–33 (2010)).

75. Pace, *supra* note 47, at 6, 8–9.

grown, both as new duties and types of breaches are added[76] and as duties previously thought to reside under the duty of care have been shifted to the duty of loyalty, as was the case with *Caremark* doctrine.[77]

Caremark doctrine, then, is only one piece of what has become quite extensive caselaw governing directors' duties. It has not traditionally been a particularly prominent corner of Delaware corporation law due to the difficulty of bringing a successful *Caremark* claim. But Delaware corporation law continues to evolve, and changes to the *Caremark* doctrine in *Stone v. Ritter* set the stage for it to be newly reinvigorated in *Marchand v. Barnhill*. With the Delaware Supreme Court's opinion in *Marchand* and four opinions out of the Chancery Court allowing *Caremark* claims to survive, we now have enough information to assess where *Caremark* doctrine stands today.

Caremark opinions traditionally come at the motion to dismiss stage of litigation.[78] But the usual procedural posture of *Caremark* claims does

---

76. *See* Hill & McDonnell, *supra* note 74, at 1780–81 (grouping duty of loyalty cases into four categories: "as traditionally conceived" (classic conflict of interest cases), "structural bias" (where the court is concerned about "excessive deference"), "suspect motive[s]" (including doctrines specific to the takeover context), and "conduct involving illegality").

77. *See, e.g.*, Stephen M. Bainbridge, Caremark *and Enterprise Risk Management*, 34 J. CORP. L. 967, 975 (2009) ("In *Guttman*, however, Vice Chancellor Strine ripped the *Caremark* claim from its original home in the duty of care and reinvented it as a duty of loyalty."); Hill & McDonnell, *supra* note 74, at 1769 ("The court also threw in a bit of a shocker in *Stone*, characterizing *In re Caremark International Inc. Derivative Litigation*, until then a paradigmatic duty of care case, as a duty of loyalty case.").

78. *See, e.g.*, *Pettry v. Smith*, No. 2019-0795-JRS, 2021 WL 2644475, at *1 (Del. Ch. June 28, 2021) (deciding the case on demand excusal and thus not reaching arguments under Rule 12(b)(6)); *Richardson v. Clark*, No. 2019-1015-SG, 2020 WL 7861335, at *2 (Del. Ch. Dec. 31, 2020) (dismissing the case for failure to sufficiently plead demand excusal); *Teamsters Local 443 Health Servs. & Ins. Plan v. Chou*, No. 2019-0816-SG, 2020 WL 5028065, at *2 (Del. Ch. Aug. 24, 2020) ("The Defendants have moved to dismiss under Rules 23.1 and 12(b)(6)."); *In re GoPro, Inc. S'holder Deriv. Litig.*, No. 2018-0784-JRS, 2020 WL 2036602, at *2 (Del. Ch. Apr. 28, 2020) (dismissing the case for failure to sufficiently plead demand excusal); *In re Metlife Inc. Deriv. Litig.*, No. 2019-0452-SG, 2020 WL 4746635, at *2 (Del. Ch. Aug. 17, 2020) (dismissing the case because the pled facts "fall[ ] short of a specific pleading of bad faith"); *Hughes v. Hu*, No. 2019-0112-JTL, 2020 WL 1987029, at *2 (Del. Ch. Apr. 27, 2020) ("The defendants also have moved to dismiss the complaint pursuant to Rule 12(b)(6) . . . . That motion is also denied."); *Owens v. Mayleben*, No. 12985-VCS, 2020 WL 748023, at *1 (Del. Ch. Feb. 13, 2020) (dismissing the case for failure to sufficiently plead demand excusal); *In re LendingClub Corp. Deriv. Litig.*, No. 12984-VCM, 2019 WL 5678578, at *2 (Del. Ch. Oct. 31, 2019) (dismissing the case for failure to sufficiently plead demand excusal); *In re Clovis Oncology, Inc. Deriv. Litig.*, No. 2017-0222-JRS, 2019 WL 4850188, at *1 (Del. Ch. Oct. 1, 2019) ("Defendants have moved to dismiss each of Plaintiffs' derivative claims under Court of Chancery Rules 23.1 and 12(b)(6) for failure to plead demand futility with particularity and failure to state viable claims. As explained below, Plaintiffs have well-pled that Defendants face a substantial likelihood of liability under *Caremark* and our Supreme Court's recent explication of

create some important distinctions from, say, your standard-issue commercial litigation in federal court. The distinction is driven by two idiosyncrasies of Delaware corporation law litigation: the demand requirement and Section 220 books and records requests. Because *Caremark* claims are traditionally brought as derivative lawsuits, the dissident shareholder must either make a demand on the board or plead demand excusal.[79] Practically speaking, shareholders will choose the latter option.[80] Demand excusal must be pled with particularity.[81] The Chancery Court has traditionally weighed demand futility for *Caremark* claims under the *Rales* test,[82] but in September 2021, the Delaware Supreme Court replaced the *Aronson*[83] and *Rales* tests with a single, three-part test for demand futility.[84] That new test, though, "is consistent with and enhances *Aronson*, *Rales*, and their progeny" and "cases properly construing *Aronson*, *Rales*, and their progeny remain good law."[85] Where the corporation's certificate of incorporation exculpates

---

Caremark in *Marchand v. Barnhill*."); *Rojas v. Ellison*, No. 2018-0755-AGB, 2019 WL 3408812, at *1 (Del. Ch. July 29, 2019) (dismissing the case for failure to sufficiently plead demand excusal); *Marchand v. Barnhill*, No. 2017-0586-JRS, 2018 WL 4657159, at *1 (Del. Ch. Sept. 27, 2018) (dismissing the case for failure to sufficiently plead demand excusal), *rev'd*, *Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019). The exceptions are *Caremark* itself, which involved a motion to approve a proposed settlement, and *Araneta*, which went to trial. *In re Caremark Int'l Inc. Deriv. Litig.*, 698 A.2d 959, 960 (Del. Ch. 1996); *ATR-Kim Eng Fin. Corp. v. Araneta*, No. 489-N, 2006 WL 3783520 (Del. Ch. Dec. 21, 2006).

79. *Stone v. Ritter*, 911 A.2d 362, 366–67 (Del. 2006) ("[T]he right of a stockholder to prosecute a derivative suit is limited to situations where either the stockholder has demanded the directors pursue a corporate claim and the directors have wrongfully refused to do so, or where demand is excused because the directors are incapable of making an impartial decision regarding whether to institute such litigation.") (citing *Aronson v. Lewis*, 473 A.2d 805, 811 (Del. 1984), *overruled on other grounds by Brehm v. Eisner*, 746 A.2d 244, 253–54 (Del. 2000)).

80. Andrew C.W. Lund, *Rethinking* Aronson*: Board Authority and Overdelegation*, 11 U. PA. J. BUS. L. 703, 712 (2009) ("Demand futility, however, is by far the most popular of these two routes for shareholder-plaintiffs. Indeed, demand futility has been called '*the* critical issue in derivative litigation.'"); *id.* at 712 n.44 ("The general consensus is that it is almost impossible for shareholder plaintiffs to prevail in a 'wrongful refusal' action.") (citing Randall S. Thomas & Kenneth J. Martin, *Litigating Challenges to Executive Pay: An Exercise in Futility?*, 79 WASH. U. L.Q. 569, 576–77 (2001)).

81. DEL. CH. CT. R. 23.1 ("The complaint shall also allege with particularity the efforts, if any, made by the plaintiff to obtain the action the plaintiff desires from the directors or comparable authority and the reasons for the plaintiff's failure to obtain the action or for not making the effort.").

82. *E.g.*, *In re Boeing Co. Deriv. Litig.*, No. 2019-0907-MTZ, 2021 WL 4059934, at *22 (Del. Ch. Sept. 7, 2021) (applying the demand futility standard established in *Rales v. Blasband*, 634 A.2d 927, 934 (Del. 1993)).

83. *Aronson v. Lewis*, 473 A.2d 805 (Del. 1984).

84. *United Food & Com. Workers Union v. Zuckerberg*, 262 A.3d 1034, 1057–59 (Del. 2021).

85. *Id.* at 1059.

directors for breaches of the duty of care (as most do), to show a substantial likelihood of liability under the demand excusal test the plaintiff must adequately plead a duty of loyalty violation, such as under *Caremark*.[86]

Section 220 of the Delaware General Corporation Law provides shareholders with a right to inspect corporate books and records so long as it is not for an improper purpose.[87] The Chancery Court expects litigants to avail themselves of their rights under Section 220 *before* bringing a derivative suit.[88] The Delaware Supreme Court also recently "removed two common defenses that companies use to oppose the production of corporate records to stockholders."[89] The documents produced will be considered on a motion to dismiss; if a document is *not* produced, the court will infer it does not exist.[90] The combination of the two means that facts play a significant role in *Caremark* opinions even at the motion to dismiss stage.

Prior to *Caremark*, the leading Delaware case addressing potential liability for directors after unlawful corporate conduct was *Graham v. Allis-Chalmers Manufacturing Co.*[91] Four employees of Allis-Chalmers

---

86. *See Firemen's Ret. Sys. of St. Louis v. Sorenson (Marriott)*, No. 2019-0965-LWW, 2021 WL 4593777, at *8 (Del. Ch. Oct. 5, 2021) (applying the rule to a derivative action involving *Caremark* claims against Marriott directors).

87. DEL. CODE ANN. tit. 8, § 220 (2022).

88. *Louisiana Mun. Police Emps.' Ret. Sys. v. Pyott*, 46 A.3d 313, 343 (Del. Ch. 2012), *rev'd*, 74 A.3d 612 (Del. 2013) ("The Delaware courts have dismissed a steady stream of *Caremark* claims where the plaintiffs have not first used Section 220 to obtain books and records.") (first citing *Wood v. Baum*, 953 A.2d 136, 144 (Del. 2008); then citing *In re Dow Chem. Co. Deriv. Litig.*, No. 4349-CC, 2010 WL 66769, at *13 (Del. Ch. Jan. 11, 2010); then citing *Desimone v. Barrows*, 924 A.2d 908, 951 (Del. Ch. 2007); then citing *Rattner v. Bidzos*, No. 19700, 2003 WL 22284323, at *14 (Del. Ch. Sept. 30, 2003); then citing *In re Citigroup Inc. S'holders Litig.*, No. 19827, 2003 WL 21384599, at *3 (Del. Ch. June 5, 2003), *aff'd sub nom. Rabinovitz v. Shapiro*, 839 A.2d 666 (Del. 2003); then citing *Guttman v. Huang*, 823 A.2d 492, 493, 504 (Del. Ch. 2003); and then citing *White v. Panic*, 793 A.2d 356, 364–65, 371–72 (Del. Ch. 2000)). *See* John F. Savarese, Sarah K. Eddy & Sabastian V. Niles, *Cybersecurity Oversight and Defense—A Board and Management Imperative*, HARV. L. SCH. F. ON CORP. GOVERNANCE (May 14, 2021), https://corpgov.law.harvard.edu/2021/05/14/cybersecurity-oversight-and-defense-a-board-and-management-imperative [https://perma.cc/M6MH-MK5J] ("Stockholder inspection demands to review a company's books and records, including board- and committee-level minutes, in preparation for litigation are increasingly common and allowed by the courts where legal requirements are met.").

89. Francis Pileggi, *Supreme Court Rejects Two Common Defenses to Section 220 Demands*, DEL. CORP. & COM. LITIG. BLOG (Dec. 14, 2020), https://www.delawarelitigation.com/2020/12/articles/delaware-supreme-court-updates/supreme-court-rejects-two-common-defenses-to-section-220-demands [https://perma.cc/7HLW-CDFC] (relying on *AmerisourceBergen Corp. v. Lebanon Cnty. Emps. Ret. Fund,* 243 A.3d 417 (Del. 2020)).

90. Shapira, *supra* note 73, at 1870–71, 1878.

91. 188 A.2d 125 (Del. 1963).

and the company itself were indicted and pled guilty to charges of violating antitrust law.[92] The plaintiffs alleged that the directors had either actual knowledge of the unlawful corporate conduct or "knowledge of facts which should have put them on notice of such conduct."[93] As a large manufacturer, Allis-Chalmers' operations were heavily decentralized.[94] In contrast with modern *Caremark* claims, *Allis-Chalmers* was decided after depositions, which produced no evidence to support the plaintiffs' allegations.[95] This forced the plaintiffs to argue that the directors should be liable due to "their failure to take action designed to learn of and prevent anti-trust activity."[96] The plaintiffs also argued that the directors were put on notice of potential antitrust problems by two consent decrees entered by the Federal Trade Commission against Allis-Chalmers.[97] But the defendant-directors had not been on the board at the time of the consent decrees, and the company did not admit guilt.[98] According to the Delaware Supreme Court, rather than directors having any obligation to "put into effect a system of watchfulness[,] . . . directors are entitled to rely on the honesty and integrity of their subordinates until something occurs to put them on suspicion that something is wrong."[99] The kernel of what would become a duty to respond to red flags or risk a *Caremark* claim exists in *Allis-Chalmers*, then, but the duty to implement a compliance system or face a *Caremark* claim is missing. The *Allis-Chalmers* opinion was criticized for failing to incentivize boards to implement compliance systems.[100]

A. The Caremark *Doctrine is Born*

At the time of the derivative suit, Caremark International, Inc. (Caremark) was a publicly-traded corporation that was headquartered outside of Chicago but incorporated in Delaware.[101] As a healthcare company, Caremark generated most of its revenue from its patient care

92. *Id.* at 127.
93. *Id.*
94. *Id.* at 128.
95. *Id.* at 127.
96. *Id.*
97. *Id.* at 129.
98. *Id.*
99. *Id.* at 130.
100. *See, e.g.*, Fairfax, *supra* note 74, at 422 (describing *Allis-Chalmers* as setting "the bar of compliance so low as to render the oversight doctrine largely irrelevant"). *But see* Stephen M. Bainbridge, *Don't Compound the* Caremark *Mistake by Extending It to ESG Oversight*, 77 BUS. LAW. 651, 655–60 (2022) (criticizing *Caremark* for effectively overruling the binding precedent of *Allis-Chalmers* from below and for having "ignored the policy concerns that justified the [*Allis-Chalmers*] standard").
101. *In re Caremark Int'l Inc. Deriv. Litig.*, 698 A.2d 959, 961 (Del. Ch. 1996).

business, with a substantial part of that "derived from third party payments, insurers, and Medicare and Medicaid reimbursement programs."[102] The Anti-Referral Payments Law bars healthcare providers from paying referral fees for Medicare and Medicaid patients.[103] Alleged improper payments by Caremark led to multiple criminal indictments against Caremark officers and Caremark itself that ultimately culminated in "a guilty plea to a single count of mail fraud by the corporation, the payment of a criminal fine, the payment of substantial civil damages, and cooperation with further federal investigations."[104]

Shareholders responded by filing five separate derivative actions later consolidated into a single suit.[105] The original complaint characterized the actions (or inaction) by the Caremark board as a breach of the duty of care.[106] The procedural posture of the opinion is unconventional as the issue was not before the Chancery Court on a motion to dismiss. Rather, the court approved a proposed settlement as "fair and reasonable."[107] Caremark only proposed minor changes to its corporate practices, but the court approved the settlement nevertheless for the simple reason that the claims asserted were very weak.[108] The *Caremark* decision both flags a novel claim for breach of fiduciary duty under Delaware corporation law and, at the same time, flags that claim as unlikely to succeed.

The Chancery Court differentiates the claims in *Caremark* from "*a board decision* that results in a loss because that decision was ill-advised or 'negligent.'"[109] The first is safely ensconced within the protective walls of the business judgment rule.[110] The second is what has come to be known as a "*Caremark*" claim: failure to monitor.[111] The first concerns decisions; the second concerns "unconsidered inaction."[112] Unconsidered inaction relates to decisions made by officers and ordinary employees who cause the corporation to violate the law, affecting "the

---

102. *Id.*
103. *Id.* at 961–62.
104. *Id.* at 963–65.
105. *Id.* at 964.
106. *Id.*
107. *Id.* at 970.
108. *Id.* at 970–71.
109. *Id.* at 967 (emphasis in original).
110. *Id.*
111. *Id.* at 967–68. Chancellor Allen first refers to it as a claim for "an *unconsidered failure of the board to act* in circumstances in which due attention would, arguably, have prevented the loss," then later refers to it as "[l]iability for failure to monitor." *Id.* (emphasis in original).
112. *Id.*

welfare of the corporation and its ability to achieve its various strategic and financial goals."[113]

If corporate directors are aware of unlawful corporate behavior due to the decisions of corporate officers and employees, then they have a duty to put a stop to it.[114] But directors can assume integrity on the part of officers and employees "absent grounds to suspect deception."[115] What they cannot do is avoid taking proactive measures to ensure that appropriate monitoring systems are in place.[116]

B. "[T]he most difficult theory in corporation law upon which a plaintiff might hope to win a judgment"[117]

When Chancellor Allen described a *Caremark* claim as "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment,"[118] he was not *only* referring to what are now known as *Caremark* duty-to-monitor claims. He was also referring to the sorts of claims very safely insulated by the business judgment rule.[119] Nonetheless, Chancellor Allen's words proved prescient in the twenty-three years between when *Caremark* and *Marchand* were decided. *Caremark* duty to monitor claims were simply not a viable route to derivative litigation success for disgruntled shareholders, any more than suits challenging an ill-advised board decision. This was by design.[120]

The *Caremark* decision did, however, establish the analytical framework for duty to monitor claims, which themselves came to be known as *Caremark* claims.[121] This was despite the somewhat odd procedural posture of the opinion. The issue before the court was approval of a settlement; the analysis is dicta.[122] The *Caremark* analysis

---

113. *Id.* at 968.

114. *See* Pace, *supra* note 47, at 10 (discussing the application of Delaware corporation law in that situation by the U.S. Court of Appeals for the Seventh Circuit in *In re Abbott Lab'ys Deriv. S'holders Litig.*, 325 F.3d 795, 809 (7th Cir. 2003)).

115. *Caremark*, 698 A.2d at 969 (relying on *Graham v. Allis-Chalmers Mfg. Co.*, 188 A.2d 125, 130–31 (Del. 1963)).

116. *Id.* at 969–70; *see also* Robert C. Bird, Caremark *Compliance for the Next Twenty-Five Years*, 58 AM. BUS. L.J. 63, 71 (2021) (asserting that the world had changed since *Allis-Chalmers* and the time was due for boards "to assume an affirmative obligation, however narrow, to take responsibility for attempting to ensure the existence of a reasonable information and reporting system").

117. *Caremark*, 698 A.2d at 967.

118. *Id.*

119. *Id.* at 967–68.

120. Hill & McDonnell, *supra* note 74, at 1777 ("*Caremark* duties are deliberately structured to make it extremely hard for plaintiffs to win.").

121. Paul E. McGreal, *Corporate Compliance Survey*, 64 BUS. LAW. 253, 272 (2008).

122. *See* Bainbridge, *supra* note 77, at 973.

would remain influential, and the name would stick, but the *Caremark* claim would see important doctrinal development. *Caremark* was "a paradigmatic duty of care case" grouped with other duty of care cases in casebooks.[123] The fiduciary duties owed by directors to the corporation are traditionally bifurcated between the duty of care and the duty of loyalty.[124] The Delaware Supreme Court briefly flirted with dividing corporate fiduciary duties among the duties of care, loyalty, and good faith.[125] The Delaware Supreme Court eventually located good faith firmly *within* the duty of *loyalty*.[126] The Delaware Supreme Court was following the lead of the Chancery Court, which had already "reinvented [*Caremark*] as a duty of loyalty" issue in *Guttman v. Huang*.[127] The Chancery Court noted in *Guttman v. Huang* that, although *Caremark* "is rightly seen as a prod towards the greater exercise of care by directors," it was in fact a matter of the duty of loyalty.[128]

The Delaware courts' moves in 2003 with *Guttman* and 2006 with *Stone* were doctrinally important because, unlike duty of care claims, duty of loyalty claims cannot be exculpated in the corporate charter under Section 102(b)(7).[129] Most corporate charters now include a Section 102(b)(7) exculpatory provision.[130] Removing *Caremark* claims from Section 102(b)(7) exculpation may have been the entire point of the doctrinal shift.[131] If it was, it was unnecessary: Section 102(b)(7) already provides that liability may not be limited for acts by a director that are

---

123. Hill & McDonnell, *supra* note 74, at 1769, 1776 (citing WILLIAM T. ALLEN, REINIER KRAAKMAN & GUHAN SUBRAMANIAN, COMMENTARIES AND CASES ON THE LAW OF BUSINESS ORGANIZATION 282–92 (2d ed. 2007)).

124. *Id.* at 1771.

125. *See* Pace, *supra* note 47, at 65–66 (relying on Stephen M. Bainbridge, Star Lopez, & Benjamin Oklan, *The Convergence of Good Faith and Oversight*, 55 UCLA L. REV. 559, 566 (2008)).

126. *Id.* at 7 (relying on *Stone v. Ritter*, 911 A.2d 362, 369–70 (Del. 2006)*; see also* Andrew C.W. Lund, *Opting Out of Good Faith*, 37 FLA. ST. U. L. REV. 393, 400–06 (2010) (describing good faith as having appeared to "largely breezed into and out of Delaware corporate law without any generally agreed-upon meaning" prior to *Disney* and *Stone*).

127. Bainbridge, *supra* note 77, at 975 (relying on *Guttman v. Huang*, 823 A.2d 482, 506 (Del. Ch. 2003)).

128. *Guttman*, 823 A.2d at 506.

129. Bainbridge, *supra* note 77, at 975 (citing Regina F. Burch, *"Unfit to Serve" Post-Enron*, 42 VAL. U. L. REV. 1081, 1094 (2008)).

130. Hill & McDonnell, *supra* note 74, at 1774.

131. *See, e.g.*, Fairfax, *supra* note 74, at 430 (noting arguments that oversight was shifted from the duty of care to the duty of loyalty in order to remove it from the protection of Section 102(b)(7)) (first citing Stephen M. Bainbridge, Star Lopez & Benjamin Oklan, *The Convergence of Good Faith and Oversight*, 55 UCLA L. REV. 559, 597 (2008); and then citing Robert B. Thompson, *The Short, But Interesting Life of Good Faith as an Independent Liability Rule*, 55 N.Y.L. SCH. L. REV. 543, 551 (2011)).

"not in good faith."[132] And the *Caremark* opinion makes clear that good faith is central to *Caremark* claims.[133]

Stone v. Ritter was also important because it marked the first time the Delaware Supreme Court expressly endorsed the analytical framework from *Caremark*.[134] And it formalized what this Article has referred to as "Type I" and "Type II" *Caremark* claims.[135] Type I applies where "the directors utterly failed to implement any reporting or information system or controls."[136] Type II applies where the board implemented controls but "consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."[137] This framework would have no immediate effect on the viability of *Caremark* claims, which continued to fall at the motion to dismiss stage.

Prior to *Guttman v. Huang*, the Chancery Court appears to have sustained *zero Caremark* claims. During the three-year period from *Guttman* to *Stone*, the Chancery Court sustained *one Caremark* claim,[138] with another sustained shortly after *Stone* was decided.[139] In *Saito v. McCall*,[140] the court, on a second try, "barely" sustained a *Caremark* claim.[141] The board of McKesson Corporation ignored red flags related to "unlawful accounting improprieties" during due diligence of an acquisition target (a Type II claim).[142] In *ATR-Kim Eng Financial Corp. v. Araneta*,[143] the ten-percent shareholders of a corporation sued the ninety-percent shareholder for transferring away the key assets of a

---

132. DEL. CODE ANN. tit. 8, § 102(b)(7) (2016).

133. *See In re Caremark Int'l Inc. Deriv. Litig.*, 698 A.2d 959, 967–68, 971 (Del. Ch. 1996) ("[T]he business judgment rule is process oriented and informed by a deep respect for all *good faith* board decisions. . . . [O]nly a sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exits—will establish the lack of good faith that is a necessary condition to liability.") (emphasis in original).

134. *See* Bainbridge, *supra* note 77, at 976 (citing *Stone v. Ritter*, 911 A.2d 362 (Del. 2006)).

135. *See* Lund, *supra* note 126, at 407 ("After *Stone* then, we are left with at least two types of cases. First, clear *Caremark*/*Stone*, failure-to-monitor claims, for which *Stone* offers a specific disjunctive test—absence of monitoring systems or conscious failure to monitor through such systems.").

136. *Stone*, 911 A.2d at 370.

137. *Id.*

138. *Saito v. McCall*, No. 17132-NC, 2004 WL 3029876 (Del. Ch. Dec. 20, 2004), *overruled on other grounds by Lambrecht v. O'Neal*, 3 A.3d 277 (Del. 2010).

139. *See ATR-Kim Eng Fin. Corp. v. Araneta*, No. 489-N, 2006 WL 3783520, at *19–21 (Del. Ch. Dec. 21, 2006). The opinion in *Araneta* was issued a month after the opinion in *Stone*.

140. 2004 WL 3029876.

141. *Id.* at *1, *6.

142. *Id.* at *6–7.

143. 2006 WL 3783520.

holding company incorporated in Delaware to his family members.[144] The majority shareholder had a traditional duty of loyalty issue.[145] But two other directors, both of whom considered themselves to be employees of the majority shareholder, had a duty of loyalty issue under *Caremark*.[146] No reporting systems were in place and the directors deferred entirely to the majority shareholder.[147] *Araneta* is notable for being the rare *Caremark* claim that made it to trial.[148] Of these two cases, *Araneta* was the earliest to see a *Caremark* claim succeed, with the court describing the directors as "stooges."[149]

Guttman was preceded by the 2002 corporate governance crisis exemplified by Enron and WorldCom.[150] Despite the magnitude of the crisis, there was no surge in successful *Caremark* suits. The Chancery Court dismissed a *Caremark* claim against Citigroup alleging that its board had ignored red flags related to improper transactions by its clients, including Enron and WorldCom.[151] After the first suit failed, in part because of a failure to seek documents under Section 220, another plaintiff remedied the defect and tried again, with an equal lack of success.[152]

Stone was followed two years later by the 2008 financial crisis.[153] Citigroup would again be sued under a *Caremark* theory and again prevail on a motion to dismiss.[154] Goldman Sachs would also face a *Caremark* claim and come away unscathed.[155] Despite the belief of many that poor board oversight helped lead to both crises,[156] neither the 2002 corporate governance crisis nor the 2008 financial crisis resulted in the number of successful *Caremark* claims seen between 2019 and 2021. The financial crisis did result in one successful *Caremark* claim against

144. *Id.* at *1. The underlying venture was based in the Philippines. *Id.* at *3.

145. *Id.* at *15–17.

146. *Id.* at *19–21.

147. *Id.* at *20.

148. *See id.* at *5.

149. *Id.* at *19, *21.

150. *See, e.g.*, Fairfax, *supra* note 74, at 426.

151. *In re Citigroup Inc. S'holders Litig.*, No. 19827, 2003 WL 21384599 (Del. Ch. June 5, 2003).

152. *David B. Shaev Profit Sharing Acct. v. Armstrong*, No. 1449-N, 2006 WL 391931, at *1 (Del. Ch. Feb. 13, 2006), *aff'd*, 911 A.2d 802 (Del. 2006).

153. Bernard S. Sharfman, *Enhancing the Efficiency of Board Decision Making: Lessons Learned from the Financial Crisis of 2008*, 34 DEL. J. CORP. L. 813, 816 (2009).

154. *In re Citigroup Inc. S'holder Derivative Litig.*, 964 A.2d 106, 131 (Del. Ch. 2009).

155. *In re Goldman Sachs Grp., Inc. S'holder Litig.*, No. 5215-VCG, 2011 WL 4826104, at *18, *23 (Del. Ch. Oct. 12, 2011).

156. *E.g.*, Fairfax, *supra* note 74, at 425–27.

AIG.[157] The plaintiffs in *AIG* alleged "widespread illegal misconduct" led to financial restatements that wiped out $3.5 billion in shareholder value and resulted in the company paying $1.6 billion in fines and other costs to resolve litigation and regulatory enforcement actions against it.[158] The director defendants "were directly knowledgeable of and involved in much of the wrongdoing," the "diversity, pervasiveness, and materiality" of which was "extraordinary."[159] If that was true, then the directors must have also known that AIG's internal controls were inadequate.[160]

During the thirteen years between *Stone* and *Marchand*, as few as five *Caremark* claims were sustained by the Chancery Court (including *AIG* and *Araneta*).[161] In *Rich ex rel Fuqi International, Inc. v. Yu Kwai Chong*,[162] the court sustained a *Caremark* claim where the "individual Defendants not only failed to respond to the demand over the next two years, but allegedly took actions making meaningful response to the demand unlikely if not impossible."[163] An investigation of "the transfer of $120 million of cash out of the company" ended after the audit committee's advisors were not paid, and all of the corporation's independent directors subsequently resigned.[164] The company also lacked internal controls and had accounting issues.[165] The *Caremark* claim in *Rich* was sustained as a Type II claim.[166] The board ignored red flags, including accounting issues that required a restatement and inadequate internal controls neither of which were remedied.[167] It also ignored known issues bringing internal controls for a Chinese company into accord with U.S. securities laws.[168]

---

157. *Am. Int'l Grp., Inc. v. Greenberg* (*In re Am. Int'l Grp., Inc.*), 965 A.2d 763, 798–99 (Del. Ch. 2009).

158. *Id.* at 774–75.

159. *Id.* at 799.

160. *Id.*

161. *See Stewart v. Wilmington Tr. SP Servs., Inc.*, 112 A.3d 271, 299–301 (Del. Ch. 2015); *In re China Agritech, Inc. S'holder Derivative Litig.*, No. 7163-VCL, 2013 WL 2181514, *18–20 (Del. Ch. May 21, 2013); *Rich ex rel. Fuqi Int'l, Inc. v. Yu Kwai Chong*, 66 A.3d 963, 975 (Del. Ch. 2013); *In re Am. Int'l Grp., Inc.*, 965 A.2d 763, 798–99; *ATR-Kim Eng Fin. Corp. v. Araneta*, No. 489-N, 2006 WL 3783520, *19–21 (Del. Ch. Dec. 21, 2006).

162. 66 A.3d 963 (Del. Ch. 2013).

163. *Id.* at 965–66.

164. *Id.* at 966.

165. *Id.* at 970, 982–83.

166. *See id.* at 983–85.

167. *Id.* at 983–84.

168. *Id.*

Stewart v. Wilmington Trust SP Services, Inc.[169] involved accounting irregularities.[170] *Stewart* is procedurally distinct from a standard *Caremark* claim. Rather than a shareholder-plaintiff, the Delaware Insurance Commissioner prosecuted the claims of four Delaware captive insurance companies as receiver in liquidation.[171] Under the facts of the case, Wilmington Trust SP Services, Inc. (Wilmington Trust) was a Delaware corporation that provided management and administrative services to four captive insurance companies (SPI Entities).[172] Wilmington Trust struggled to produce audited financial statements for the SPI Entities.[173] An investigation by the Insurance Commissioner discovered that, contrary to their financial statements, the assets of the SPI Entities were minimal.[174] The court sustained a *Caremark* claim because the SPI "[E]ntities' boards approved the audited financial statements with little or no substantive discussion, despite warnings that significant irregularities occurred and the companies' procedures needed to be changed."[175]

In *China Agritech*,[176] a Chinese manufacturer and seller of fertilizer accessed U.S. securities markets through an inactive Delaware corporation with a NASDAQ listing.[177] Like the company in *Rich*, China Agritech disclosed inadequate internal controls but did not remedy them.[178] Problems were in fact substantial, with little to no manufacturing, fictional revenue, and ghost factories.[179] Although the disclosed but inadequate and unremedied internal controls in *Rich* served as red flags for a Type II claim, the *China Agritech* court instead appeared to sustain a *Caremark* claim under a Type I analysis because China Agritech had "an Audit Committee that existed in name only."[180] Notably, both *Rich* and *China Agritech* involved Chinese companies.[181]

---

169. 112 A.3d 271 (Del. Ch. 2015).

170. *See id.* at 282–86.

171. *Id.* at 278.

172. *Id.* at 279–80.

173. *Id.* at 282–86.

174. *Id.* at 289.

175. *Id.* at 299–300.

176. *In re China Agritech, Inc. S'holder Deriv. Litig.*, No. 7163-VCL, 2013 WL 2181514 (Del. Ch. May 21, 2013).

177. *Id.* at *1.

178. *Id.* at *2–4, 8.

179. *Id.* at *5–6.

180. *Id.* at *18–19.

181. There have been as few as eleven successful *Caremark* claims in the doctrine's history. Three involved Chinese companies. *Id.* at *1; *Rich ex rel. Fuqi Int'l, Inc. v. Yu Kwai Chong*, 66 A.3d 963, 966–67 (Del. Ch. 2013); *Hughes v. Hu*, No. 2019-0112-JTL, 2019 WL 1987029, at *2 (Del. Ch. Apr. 27, 2020). Audit issues have also recently become a major issue for Chinese companies listed on the New York Stock Exchange. Kiuyan Wong & Benjamin Bain, *What's Driving US-China Spat Over Audits,*

Also of note is the Chancery Court's decision in *Massey Energy*.[182] The plaintiff framed one of their claims as a *Caremark* claim, but the court ruled that rather than allow unlawful corporate action through inadequate oversight, the board instead "knowingly caus[ed] it to seek profit by violating the law."[183] A claim that the board directed the corporation to violate the law or knew that it was doing so and turned a blind eye is conceptually and doctrinally distinct from a *Caremark* claim.[184]

The highest profile *Caremark* case in the years immediately preceding *Marchand* involved defective ignition switches in General Motors Company (GM) vehicles.[185] GM recalled 28 million vehicles via forty-five recalls over the course of several months.[186] The defective ignition switches sometimes inadvertently resulted in the vehicle's engine, power steering, power breaks, and airbags becoming disabled while driving.[187] Recall costs alone led to $1.5 billion in charges against earnings and GM set up a fund to compensate accident victims.[188] GM violated the National Traffic and Motor Vehicle Safety Act of 1996 by not reporting the defect after becoming aware of it within five days.[189] GM subsequently paid $35 million in fines to the government.[190]

Certain GM employees had known about the ignition switch defect for years; the GM board had not, but plaintiffs argued that they *should have* known.[191] More precisely, the plaintiffs argued that the board prevented the issue from reaching it by not implementing appropriate policies and procedures.[192] Notably in light of *Marchand* and its progeny, GM did not have a specific committee responsible for vehicle safety issues, although it did initially have a finance and risk committee.[193] The finance and risk committee was eliminated during the relevant time period and its risk management oversight responsibilities were

---

Delistings, BLOOMBERG, https://www.bloomberg.com/news/articles/2022-07-28/what-s-driving-us-china-spat-over-audits-delistings-quicktake [https://perma.cc/5PPT-BHEU] (Aug. 26, 2022, 10:56 PM).

182. *In re Massey Energy Co. Deriv. & Class Action Litig.*, No. 5430-VCS, 2011 WL 2176479 (Del. Ch. May 31, 2011).

183. *Id.* at *19–20.

184. *See* Pace, *supra* note 47, at 6–8 (distinguishing the duty of loyalty doctrine from the *per se* standard that applies to knowing violations of law).

185. *In re General Motors Co. Deriv. Litig.*, No. 9627-VCG, 2015 WL 3958724, at *1 (Del. Ch. June 26, 2015).

186. *Id.* at *2.

187. *Id.*

188. *Id.*

189. *Id.* at *9.

190. *Id.* at *2.

191. *Id.*

192. *Id.* at *9.

193. *Id.* at *4–5.

transferred to the audit committee.[194] On the management side, the chief risk officer position was eliminated and its responsibilities combined with that of the general auditor.[195] The Chancery Court dismissed the *Caremark* claim because there were no red flags alerting the board to the issue, and the board *did* have a compliance system in place, even if it was poorly designed or did not cause the revelation of the ignition switch defect.[196]

The reputation of *Caremark* claims for being tough to win surely affected litigation strategy. Plaintiffs' lawyers are less likely to pursue a litigation strategy with a long history of repeated failure, instead exploring other avenues to recovery. For example, the plaintiff in a suit alleging directors of Google parent Alphabet breached their fiduciary duties in their handling of sexual harassment claims was careful to specify in the complaint that "[t]his is not a 'failure to supervise' case."[197]

C. Caremark *Newly Invigorated in Wake of* Marchand *(Blue Bell)*

Observers could be forgiven for failing to recognize the Blue Bell ice cream listeria outbreak as the harbinger of a major change in the reception *Caremark* claims would receive before Delaware judges. It got off to an inauspicious start. Vice Chancellor Slights dispensed with the plaintiffs' *Caremark* claim in just eight paragraphs in an unpublished opinion.[198] The Vice Chancellor rejected the plaintiffs' arguments, finding "no allegation that Blue Bell failed to implement [] mandated monitoring and reporting systems" in regards to a Type I *Caremark* claim while also being "unable to discern whether Plaintiff actually intends to advance a [Type II] *Caremark* claim."[199] The plaintiff would fare better before the Supreme Court of Delaware.[200]

The facts leading to the listeria outbreak and Blue Bell's subsequent emergency, dilutive injection of cash are integral to understanding why this suit ended differently than so many previous suits that advanced

194. *Id.* at *7.

195. *Id.* at *6.

196. *Id.* at *11–17. *See generally* Marianne Jennings & Lawrence J. Trautman, *Ethical Culture and Legal Liability: The GM Switch Crisis and Lessons in Governance*, 22 B.U. J. SCI. & TECH. L. 187 (2016) (looking at the ignition switch defect debacle in great depth).

197. Shareholder Derivative Complaint ¶ 12, *Martin v. Page*, No. 19-CIV-00164 (Cal. Super. Ct. Jan. 10, 2019); *see also* Pace, *supra* note 47, at 45–46 (discussing whether a *per se* standard might apply on the theory that the board knew of and failed to prevent the unlawful activity).

198. *Marchand v. Barnhill*, No. 2017-0586-JRS, 2018 WL 4657159, at *16–19 (Del. Ch. Sept. 27, 2018).

199. *Id.* at *17–19.

200. *See Marchand v. Barnhill*, 212 A.3d 805, 807–08 (Del. 2019).

Caremark claims. The facts are equally integral to understanding the viability of *Caremark* claims going forward. Blue Bell makes and sells ice cream.[201] That is what they do—nothing more, nothing less. This subjects them to both heavy FDA and state regulation.[202]

Despite food safety being mission critical, Blue Bell had a history of quality issues. The Delaware Supreme Court opinion detailed six separate run-ins with regulators from 2009 to 2012 and multiple infractions per run-in, noting multiple positive listeria tests from 2013 to 2015.[203] Listeria can have lethal consequences. *Listeria monocytogenes* is a bacterium that can be passed through contact with diseased animals or via contaminated food.[204] Listeriosis commonly manifests as meningitis in adults, which has a high mortality rate.[205] With mortality rates between thirteen and thirty-four percent, "listeriosis may well be the leading fatal food-borne infection in the United States."[206] The bacteria has been found in a variety of dairy products, and requires careful quality assurance in food production because it is difficult to prevent.[207]

Blue Bell responded to positive listeria tests in early 2015 with a limited recall,[208] but it was too late. Within a month, listeria was discovered in Blue Bell products in South Carolina and was linked to a listeria outbreak in Kansas.[209] Blue Bell responded with another limited recall.[210] Within a month, the second recall had grown to cover *all* Blue Bell products.[211] Three people in Kansas died from listeria complications after eating contaminated Blue Bell products.[212]

For three Kansans, the consequences of lax food safety were fatal. For Blue Bell, the legal and financial consequences were just beginning. The Center for Disease Control and Prevention (CDC) launched an

---

201. *Id.* at 809.

202. *Id.* at 810.

203. *Id.* at 811–13 (citations omitted).

204. J.M. Farber & P.I. Peterkin, Listeria monocytogenes, *a Food-Borne Pathogen*, 55 MICROBIOLOGICAL REVS. 476, 477–78 (1991).

205. *Id.* at 479.

206. *Id.*

207. *Id.* at 488–89, 500.

208. *Marchand*, 212 A.3d at 813.

209. *Id.* at 813–14.

210. *Id.* at 814.

211. *Id.* Blue Bell employees were at one point directed to "explain simply that there were unspecified quality issues or manufacturing irregularities" when removing Blue Bell ice cream from store shelves. Michael W. Peregrine & David S. Rosenbloom, *The Blue Bell Dairy CEO Indictment and its Implications for Executive Liability*, HARV. L. SCHOOL FORUM CORP. GOV. (May 26, 2020), https://corpgov.law.harvard.edu/2020/05/26/the-blue-bell-dairy-ceo-indictment-and-its-implications-for-executive-liability [https://perma.cc/8H56-Z5VH].

212. *Marchand*, 212 A.3d at 814.

investigation and issued its own recall order.[213] The FDA inspected all three Blue Bell production facilities and found major issues at each.[214] Former Blue Bell employees detailed poor food safety practices to news outlets.[215]

Remember, Blue Bell was a monoline company. All they made and sold was ice cream. Due to the positive listeria test, all of Blue Bell's ice cream products were recalled from store shelves. Understandably, this led to a liquidity crisis.[216] Sid Bass' fund Moo Partners injected cash into Blue Bell via "a $125 million credit facility and . . . a $100 million warrant to acquire 42% of Blue Bell at $50,000 per share."[217] This not only diluted the ownership of existing shareholders, but also shifted control. In return for the cash infusion, Blue Bell gave Moo Partners one-third of the voting power on the board.[218]

What was the board doing during all of this? Not enough, according to the Delaware Supreme Court. "[T]he Blue Bell board failed to implement *any* system to monitor Blue Bell's food safety performance or compliance."[219] This was fatal for a "monoline company that makes a single product," making food safety a central compliance issue.[220] Management saw red flags (and failed to respond appropriately); the board was not presented with the red flags, preventing them from fulfilling their responsibilities.[221] Reports on listeria in Blue Bell plants went to management but did not find their way to the board.[222] In fact, until Blue Bell made its first recall, the only board-level discussion in the record concerned a third-party audit of sanitation issues in 2014.[223] Even then, the Blue Bell board met two days after the first recall and continued to rely on management rather than scheduling additional emergency board meetings to provide oversight for Blue Bell's response.[224]

The Delaware Supreme Court held that the plaintiff met the pleading requirement for a Type I *Caremark* claim.[225] Type I claims apply when a board fails to put in place any compliance systems or controls.[226] How could the Blue Bell directors have failed to meet this standard? Blue Bell

213. *Id.*
214. *Id.*
215. *Id.* at 815.
216. *Id.*
217. *Id.*
218. *Id.*
219. *Id.* at 809 (emphasis added).
220. *Id.*
221. *Id.*
222. *Id.* at 812.
223. *Id.* at 812–13.
224. *Id.* at 813–14.
225. *Id.* at 809.
226. *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006).

complied with various state and federal food safety regulations, and management took various steps to oversee food safety.[227] The answer lies in recognizing that the pertinent duty is a *director* duty.[228] It concerns *board* action, not the action of officers and other corporate employees. Blue Bell's failures were *board* failures, whatever management did. The *board* failed to implement any *board-level* food safety compliance system.[229] There was no *board committee* for food safety.[230] There were no protocols requiring management report food safety issues to the *board*.[231] The positive listeria results and other food safety issues—the sort of thing that might serve as a "red flag" for a Type II *Caremark* claim—were never relayed to the *board*.[232] *Board* minutes were devoid of evidence that the *board* discussed food safety issues.[233]

Accordingly, the Delaware Supreme Court reversed the Chancery Court's decision dismissing the plaintiff's claims.[234] More recently, a separate action against the operating limited partnership settled.[235] The CEO of Blue Bell was indicted on seven federal felony counts, and Blue Bell itself pled "guilty to misdemeanor charges of distribution of adulterated food."[236]

D. Four Subsequent Cases Show Marchand *was No Fluke*

After *Marchand* was decided, two questions remained. One, was *Marchand* a one-off or did it signal a real change in the viability of *Caremark* claims going forward? Two, were the implications of *Marchand* limited to its facts—a monoline company with a "mission critical"[237] compliance issue—or would *Caremark* start to bite more broadly? Four subsequent decisions by the Chancery Court provide answers.

---

227. *Marchand*, 212 A.3d at 822–23.

228. *See Stone*, 911 A.2d at 372.

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

230. *Id.* at 822.

231. *Id.*

232. *Id.*

233. *Id.*

234. *Id.* at 824.

235. Stipulation & [Proposed] Order, *Wenske v. Blue Bell Creameries, Inc.*, No. 2017-0699-JRS (Del. Aug. 17, 2020); Order & Final Judgment, *Wenske v. Blue Bell Creameries, Inc.*, No. 2017-0699-JRS (Del. Aug. 17, 2020).

236. Peregrine & Rosenbloom, *supra* note 211.

237. *Marchand*, 212 A.3d at 824 ("In Blue Bell's case, food safety was essential and mission critical.").

1. *IN RE CLOVIS ONCOLOGY, INC.*[238]

Delaware court watchers would not have to wait long. The Delaware Supreme Court decided *Marchand* on June 19, 2019;[239] the Chancery Court decided *In re Clovis Oncology, Inc.* on October 1, 2019.[240] Clovis Oncology, Inc. (Clovis) was a pharmaceutical start-up, which had developed a promising cancer drug.[241] This drug, Roci, was the most promising of the three drugs Clovis had in development.[242] Clovis did not have any drugs on the market.[243] With an estimated $3 billion annual market, Roci had the potential to be a blockbuster drug.[244] That potential return was balanced by countervailing risk. Not only was there a risk Roci would not receive FDA approval, but Clovis was locked in a race for FDA approval with AstraZeneca, which was developing a competing drug.[245]

Objective response rate (ORR) is an industry-standard metric for assessing the success of a new drug during clinical trials.[246] While Clovis reported an ORR similar to that of AstraZeneca's competing drug, the board knew by mid-2014 that the reported ORR was improperly calculated.[247] Clovis reported the improperly calculated ORR to the FDA in mid-2015.[248] Clovis disclosed an ORR of 60% in the prospectus for a secondary offering around the same time.[249] Properly calculated, the ORR was only 42%.[250] There were a number of other issues with the Roci clinical trials.[251] Even after disclosing an ORR of between 28% and 34 % to the FDA in October 2015, Clovis continued to publicly announce an improperly calculated ORR.[252]

It would soon all fall apart. The FDA noticed the discrepancy and started asking hard questions in late 2015.[253] One week later, Clovis issued a press release disclosing the accurate, much lower ORR.[254] Its

238. No. 2017-0222-JRS, 2019 WL 4850188, at *1 (Del. Ch. Oct. 1, 2019).
239. *Marchand*, 212 A.3d at 805.
240. *Clovis*, 2019 WL 4850188.
241. *Id.* at *1.
242. *Id.* at *2.
243. *Id.*
244. *Id.* at *4.
245. *Id.*
246. *Id.* at *4–5.
247. *Id.* at *5–6.
248. *Id.* at *7.
249. *Id.*
250. *Id.*
251. *Id.* at *8–9.
252. *Id.* at *7.
253. *Id.* at *8.
254. *Id.*

stock price promptly dropped 70%, erasing over $1 billion in market capitalization.[255] In April 2016, the FDA voted to delay action on Roci, dropping Clovis' stock price another 17%.[256] The next month, Clovis withdrew its application for FDA approval and ended clinical trials.[257]

Legal consequences followed. Securities fraud class action lawsuits and an SEC enforcement action led to payments of over $160 million.[258] Further, the FDA opened an investigation,[259] and a derivative lawsuit was filed that included a *Caremark* claim.[260] Despite a similar result, the posture of the *Caremark* claim was quite different than in *Marchand*: *Marchand* involved a Type I *Caremark* claim, whereas *Clovis* involved a Type II *Caremark* claim.

Clovis had controls in place and two board committees were tasked with overseeing relevant issues.[261] The Clovis board was also well aware of the issues with the Roci clinical trials. In fact, the Chancery Court described it as "hyper-focused on the drug's development and clinical trial."[262] The drug's development was a regular point of discussion at board meetings, often eating up hours of precious board time.[263] The board was well aware of the importance of ORR.[264] The board knew that ORR was being improperly calculated almost a year and a half before the issue was disclosed to the public, repeatedly receiving reports that flagged the issue.[265] For months and months, the board was aware that the ORR discrepancy was a deadly threat to one of just three Clovis drugs in development and to its stock price but did nothing.[266] The defendant directors signed Clovis' 2014 Annual Report, which included the inflated, improperly calculated ORR.[267] The board was aware both that clinical trial protocols were being violated and that side effects were being underreported.[268] Given the rampant issues and the board's extensive knowledge and appreciation of their severity, the Chancery

255. *Id.*
256. *Id.*
257. *Id.*
258. *See id.* at *9.
259. *Id.*
260. *Id.* at *10.
261. *See id.* at *2 ("The Nominating and Corporate Governance Committee is charged with developing and overseeing the effectiveness of Clovis' legal, ethics and regulatory compliance matters. The Audit Committee oversees typical audit functions and, importantly, reviews earnings reports with management before release to the market.").
262. *Id.* at *4.
263. *Id.*
264. *Id.* at *5.
265. *Id.* at *5–8.
266. *Id.* at *6.
267. *Id.* at *7.
268. *Id.* at *8.

Court ruled that the defendant directors "consciously ignored red flags," denying their motion to dismiss the Type II *Caremark* claim against them.[269]

Clovis is important because successful *Caremark* claims are always noteworthy. It is important because it is a Chancery Court decision; *Clovis* signaled that the Chancery Court would not fight the Delaware Supreme Court's decision in *Marchand* or even attempt to implicitly overrule it from below. It is important because it shows that there is renewed viability for Type II *Caremark* claims, not just Type I *Caremark* claims.

But it does not mark a drastic change in doctrine, or even any change at all. The board had more red flags waved in its face than a Spanish fighting bull.[270] In fact, analytically *Clovis* was not a *Caremark* claim at all.[271] It is more properly viewed as involving a failure by the board to stop known unlawful corporate conduct, which is treated as the equivalent of the board *directing* unlawful corporate conduct under Delaware law and reviewed under a *per se* standard.[272] *Clovis* also did not provide clarity as to whether *Marchand* should be viewed as limited to mission critical risks to a company with limited products operating in a highly regulated industry.[273]

2. *HUGHES V. HU*

Clovis would not be the last time Chancery Court let a *Caremark* claim survive a motion to dismiss. Barely half a year later, the Chancery Court sustained another *Caremark* claim in *Hughes v. Hu*.[274] Kandi Technologies Group, Inc. (Kandi) is a Delaware corporation but is based in China.[275] Kandi entered into a fifty-fifty joint venture with Geely Automobile Holdings Ltd. (Geely).[276] Kandi sold parts to the joint venture, which then used the parts in the manufacture of electric

269. *Id.* at *13–15.

270. The Chancery Court characterized the directors as acting "[w]ith hands on their ears to muffle the alarms." *Id.* at *7.

271. *Procedurally*, both the complaint and the Chancery Court opinion treat it as a *Caremark* claim. *See id.* at *1, *10.

272. *See* Pace, *supra* note 47, at 10 (relying on *In re Abbott Lab'ys Deriv. S'holders Litig.*, 325 F.3d 795, 803, 809 (7th Cir. 2003)) (discussing a case that applied Illinois law but nonetheless reviewed Delaware law and indicated the result would be the same under either).

273. *See Clovis*, 2019 WL 4850188, at *12–13 (noting that compliance is context- and industry-specific, the importance of the business's regulatory environment, and "'mission critical' regulatory compliance risk").

274. No. 2019-0112-JTL, 2020 WL 1987029, at *2 (Del. Ch. April 27, 2020).

275. *Id.* at *1.

276. *Id.* at *2.

vehicles.[277] The joint venture wholesaled the finished electric vehicles to another company, Zhejiang ZuoZhongYou Electric Vehicle Service Co., Ltd. (Zhejiang), which then sold or leased the vehicles.[278]

Kandi raised some eyebrows with how it structured its business.[279] Kandi owned 9.5% of Zhejiang.[280] Xiaoming Hu, CEO of Kandi and chair of its board, owned another 13% of Zhejiang, along with his 28.4% ownership stake in Kandi.[281] His son owned Kandi USA, one of Kandi's five largest customers.[282] The complex joint venture and service company structure was allegedly designed to allow Kandi to secure both subsidies provided by China to producers of electric vehicles and subsidies provided by China to purchasers of electric vehicles.[283] AWC (CPA) Limited (AWC), Kandi's auditor, had no other clients.[284]

Kandi was rife with accounting issues over a several year period. Kandi "parked large amounts of cash in the personal bank accounts of its officers and employees," which included the CEO.[285] AWC neither verified that the cash actually existed nor *why* it was parked in personal accounts.[286] While AWC discovered $3 million in such cash, Kandi did not disclose another $4.1 million.[287] With $37.9 million in notes receivable, a single note was outstanding for $33.1 million and the borrower had made zero interest payments in the prior year.[288] "AWC did not evaluate the creditworthiness of the borrower."[289]

Related-party transactions were an ongoing issue. Kandi did extensive business with both Kandi USA and Zhejiang.[290] Transactions with Kandi USA were recorded under another name.[291] Remarkably, AWC rebooked the transactions to another customer's account at Kandi's suggestion and erased Kandi USA from its audit trail.[292] Kandi did not disclose that it had engaged in material related-party transactions with

277. *Id.*

278. *Id.*

279. All of this is based on the allegations in the complaint, taken as true at the relevant state of litigation. *Id.*

280. *Id.*

281. *Id.*

282. *Id.* at *3.

283. *Id.* at *2.

284. *Id.* at *3.

285. *Id.*

286. *Id.*

287. *See id.*

288. *Id.*

289. *Id.*

290. *See, e.g.*, *id.* at *3, *6 (noting Kandi USA was one of Kandi's five largest customers and that at one point the audit committee signed off on $42 million in related-party transactions with Zhejiang).

291. *Id.* at *3.

292. *Id.*

Kandi USA (totaling almost $10 million) until 2016.[293] Kandi also did not disclose until 2016 that Zhejiang had owed it over $40 million in 2014 and still owed it $10 million.[294]

AWC reported multiple key internal control weaknesses to the audit committee.[295] Kandi's securities disclosures also identified material control weaknesses.[296] At other times, Kandi described its controls as "effective."[297] Announcing its financials would have to be restated, Kandi also announced that it was "reassessing its internal controls."[298] The audit committee was largely asleep at the wheel during all this. They "never met for longer than one hour and typically only once per year."[299] Kandi failed to make determinations that it should have made prior to filing its 2014 10-K with the SEC.[300]

Things came to a head in 2016. The Public Company Accounting Oversight Board sanctioned AWC for its handling of Kandi's audits in 2010, 2011, and 2012.[301] Kandi responded by firing AWC as its auditor.[302] The sanctions attracted the attention of NASDAQ.[303] The Chinese government investigated Kandi and first delayed subsidy payments, then decided to phase them out altogether—the same subsidies that Kandi had structured its business to take advantage of.[304] The next spring, Kandi "announced that its financial statements from 2014 through the third quarter of 2016 could not be relied upon and needed to be restated."[305] Hughes, a Kandi shareholder, brought a derivative suit on Kandi's behalf against Hu and other directors and officers.[306]

Interestingly, the Chancery Court treated the *Caremark* claim in *Hughes* as a Type I claim rather than a Type II claim.[307] The case followed in the wake of *Marchand*, not *Clovis*. From one perspective, this made sense. A Type I claim was off the table in *Clovis*, because the record was clear that the board was sharply attentive to the Roci clinical

293. *Id.* at *7.
294. *Id.* at *8.
295. *Id.* at *3.
296. *Id.* at *4, *8.
297. *Id.* at *6.
298. *Id.* at *8.
299. *Id.* at *16.
300. *Id.* at *6.
301. *Id.* at *7.
302. *Id.*
303. *Id.*
304. *Id.*
305. *Id.* at *8.
306. *Id.* at *1.
307. *See id.* at *16 ("The complaint's allegations support a pleading-stage inference that the board never established its own reasonable system of monitoring and reporting, choosing instead to rely entirely on management.").

trials.[308] But the facts of *Hughes* were different from *Marchand*. There, the board delegated food safety entirely to management with no board committee responsible for food safety and no reports made on or discussion of food safety at full board meetings.[309] The audit committee in *Hughes* met and allegedly reviewed relevant policies, but they "never met for longer than one hour and typically only once per year" and did not produce the relevant policies.[310] *Hughes* fits better as a Type II *Caremark* claim; the Chancery Court's muddled approach shows that the doctrinal distinction between Type I and Type II will not be sharply applied.

Hughes is notable because a second vice chancellor responded positively to the Delaware Supreme Court's signal in *Marchand*.[311] *Caremark*'s reinvigoration is not the private crusade of a single vice chancellor. *Hughes* is important because the plaintiff's claim survived a motion to dismiss despite four previously dismissed securities class actions filed in the United States District Court for the Southern District in New York.[312] Entrepreneurial plaintiffs' lawyers will likely shift from securities class actions to derivative lawsuits if the latter proves more viable than the former,[313] and "plaintiffs' lawyers have struggled to get traction with cybersecurity-related securities suits."[314] If a *Caremark* claim can succeed where securities claims have failed, it may be time to ask whether *Caremark* is still "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment."[315] Nor will all securities claims fail. Directors have to worry about *Caremark* liability *in addition to* securities claims, not instead of. Finally, *Hughes* is important because: "Once is happenstance. Twice is coincidence. The third time it's enemy action."[316] This is the third time.

---

308. *See In re Clovis Oncology, Inc. Derivative Litig.,* No. 2017-0222-JRS, 2019 WL 4850188, at *1 (Del. Ch. Oct. 1, 2019) ("Clovis conducted its clinical trial of Roci subject to strict protocols and associated FDA regulations.").

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

310. *Hughes,* 2020 WL 1987029, at *16.

311. *Clovis* was decided by Vice Chancellor Slights. *Clovis*, 2019 WL 4850188; *Hughes* was decided by Vice Chancellor Laster. *Hughes*, 2020 WL 1987029, at *1.

312. *Hughes,* 2020 WL 1987029, at *8 (citing *In re Kandi Techs. Grp. Inc. Sec. Litig.*, No. 17 Civ. 1944, 2019 WL 4918649, at *9 (S.D.N.Y. Oct. 4, 2019)).

313. *See* Pace, *supra* note 47, at 66 ("Entrepreneurial plaintiffs' lawyers are always on the hunt for the next viable theory of liability against corporate directors, after all.").

314. Kevin LaCroix, *Cybersecurity-Related Securities Suit Dismissed*, D&O DIARY (Sept. 27, 2021), https://www.dandodiary.com/2021/09/articles/securitieslitigation/cybersecurity-related-securities-suit-dismissed [https://perma.cc/KNH5-YHD6].

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

316. IAN FLEMING, GOLDFINGER 177 (Thomas & Mercer ed. 2012) (1959).

3. *TEAMSTERS LOCAL V. CHOU* (AMERISOURCEBERGEN)

The fourth case in which Delaware courts refused to dismiss a *Caremark* claim is *Teamsters Local v. Chou*.[317] *Chou* involved Medical Initiatives, Inc. (Medical Initiatives), an indirect but wholly-owned subsidiary of AmerisourceBergen Corporation (AmerisourceBergen).[318] Like *Caremark* itself, *Chou* involved kickbacks in the healthcare context.[319]

Medical Initiatives systematically removed the manufacturer overfill from vials of oncology drugs, used them to fill additional syringes, and sold them.[320] This was an unsterile process that left the drugs "so grossly contaminated that particulates were visible to the naked eye."[321] In addition to the kickbacks and the pooling of overfill, Medical Initiatives sought to avoid FDA oversight through the use of sham prescriptions.[322] The scheme was profitable, with Medical Initiatives at its height selling over one million pre-filled syringes per year and netting over $14 million in profit for AmerisourceBergen per year.[323]

Much as in *Marchand*, the facilities and practices used by Medical Initiatives were unsanitary and dangerous. The vials were designed and approved by the FDA to be opened and used once, but Medical Initiatives staff frequently opened them several times.[324] To remedy the problem, the FDA instructed Medical Initiatives to not use vials containing visible particulates; however, Medical Initiatives instead filtered the particulates and sold the drugs to the tune of 32,000 syringes in a six-year period.[325] What is more, "syringes tested positive for bacteria," equipment "in the cleanroom tested positive for bacteria in excess of acceptable levels," and "air in the cleanrooms tested positive for fungal contamination and/or bacterial contamination."[326] Medical Initiatives responded with cleaning efforts but did not test to confirm their success or even stop operations during the cleaning.[327] Employees routinely violated basic cleanroom

317. No. 2019-0816-SG, 2020 WL 5028065 (Del. Ch. Aug. 24, 2020).

318. *Id.* at *1. AmerisourceBergen owned ASD Specialty Healthcare, LLC d/b/a Oncology Supply, which owned Medical Initiatives. *Id.* at *3.

319. *Id.* at *2.

320. *Id.* at *1.

321. *Id.* at *2.

322. *Id.*

323. *Id.* at *5.

324. *Id.*

325. *Id.*

326. *Id.* at *6.

327. *Id.*

protocols.[328] Medical Initiatives did not notify its customers of any issues.[329] Medical Initiatives shut down its operations in 2014.[330]

Unsurprisingly, these practices created compliance issues. The plaintiffs alleged that four of the compliance issues were "red flags" under the *Caremark* framework.[331] First was the 2006 board vote on the capital expenditure necessary to expand Medical Initiative's facility.[332] The board did not discuss any compliance issues related to the facility.[333] But the Chancery Court saw no red flag at that time; not asking enough questions does not alone establish a claim under *Caremark*.[334] The second alleged red flag was a report prepared by the Davis Polk & Wardwell (Davis Polk) law firm.[335] Davis Polk assessed compliance at AmerisourceBergen and reported its findings to the audit committee.[336] The Davis Polk report flagged that Medical Initiatives was not integrated into AmerisourceBergen's compliance program.[337] It never was, and the audit committee never received reports on compliance specific to Medical Initiatives.[338] The Chancery Court saw the Davis Polk report as a red flag that could trigger *Caremark* liability when viewed in conjunction with other red flags, even if it would not trigger *Caremark* liability by itself.[339]

The third alleged red flag was concerns raised by Michael Mullen, the former COO of the AmerisourceBergen subsidiary that was the parent of Medical Initiatives.[340] Mullen raised concerns about regulatory exposure to other senior managers and the then-CEO but was let go without his concerns being addressed.[341] The board was not informed of either Mullen's concerns nor his termination despite all severance agreements requiring the approval of the compensation committee.[342] After his termination, Mullen filed a *qui tam* action under seal that AmerisourceBergen management did not initially disclose to the board.[343] Under a *qui tam* action, a whistleblower brings a false claims action on behalf of the government, typically receiving a cut of the recovery if the

328. *Id.*
329. *Id.*
330. *Id.* at *8.
331. *Id.* at *19.
332. *Id.* at *10.
333. *Id.*
334. *Id.* at *19.
335. *Id.* at *10, *19.
336. *Id.* at *10.
337. *Id.* at *10, *19.
338. *Id.* at *20.
339. *Id.*
340. *Id.* at *11, *21.
341. *Id.* at *11–12.
342. *Id.* at *12.
343. *Id.* at *13.

action is successful.[344] Mullen's *qui tam* complaint, which was inadvertently disclosed publicly, alleged mission critical compliance issues that included overfill by Medical Initiatives.[345] The board failed to respond, allowing Medical Initiatives to continue to operate for another four years.[346] As the board knew about the *qui tam* action but did not take any remedial action, it was a red flag for *Caremark* purposes.[347]

The fourth alleged red flag was a search warrant that the FDA executed at Medical Initiative's facility and a subpoena AmerisourceBergen received from federal prosecutors.[348] The search warrant could not have been a red flag, because the *board* did not know about it.[349] The subpoena, on the other hand, was disclosed in AmerisourceBergen's 10-K.[350] Since it did not appear in the board's minutes, the Chancery Court inferred the board knew there was an issue but did not take remedial action.[351]

The United States Department of Justice (DOJ) filed a criminal complaint against AmerisourceBergen in 2017, alleging that it violated the Food and Drug Commission Act by operating an illegal operation "known to and approved at the highest levels" of AmerisourceBergen.[352] An AmerisourceBergen subsidiary pled guilty, paying the DOJ $260 million.[353] One month later, the subsidiary settled "civil claims under the False Claims Act for $625 million."[354]

In *Chou*, a third vice chancellor allowed a *Caremark* claim to survive a motion to dismiss.[355] Notably, Vice Chancellor Glasscock dismissed *Caremark* claims both shortly before and shortly after deciding *Chou*,[356] further confirming the lack of a split on the court when it came

344. Press Release, U.S. Dep't of Just., Justice Department Recovers over $2.2 Billion from False Claims Act Cases in Fiscal Year 2020 (Jan. 14, 2021), https://www.justice.gov/opa/pr/justice-department-recovers-over-22-billion-false-claims-act-cases-fiscal-year-2020 [https://perma.cc/LNJ7-NFQA]*; see also* Peter C. Ormerod, *Privacy Qui Tam,* 98 NOTRE DAME L. REV. (forthcoming 2023).

345. *Chou*, 2020 WL 5028065, at *21.

346. *Id.*

347. *Id.* at *22–24.

348. *Id.* at *24.

349. *Id.*

350. No. 2019-0907-MTZ, 2021 WL 4059934, at *1 (Del. Ch. Sept. 7, 2021).

351. *Id.*

352. *Id.* at *6–7.

353. *Id.* at *7–8.

354. *Id.* at *8.

355. *Chou* was decided by Vice Chancellor Glasscock, and the previous two successful *Caremark* suits were decided by Vice Chancellor Slights and Vice Chancellor Laster, respectively. *Chou*, 2020 WL 5028065; *see supra* note 311.

356. *See Richardson v. Clark*, No. 2019-1015-SG, 2020 WL 7861335 (Del. Ch. Dec. 31, 2020); *In re MetLife, Inc. Deriv. Litig.*, No. 2019-0452-SG, 2020 WL 4746635 (Del. Ch. Aug. 17, 2020).

to *Caremark* claims.[357] *Chou* is important because it demonstrates that red flags are cumulative.[358] Chou is interesting because the plaintiffs simultaneously advanced both Type I and Type II claims.[359] Given their nature, the claims are typically mutually exclusive; to allege both should be rare. [360] In fact, *Chou* may not have fit analytically as a *Caremark* claim at all. To the extent that the plaintiffs argued that AmerisourceBergen was operating an illegal business with the knowledge of the board, a much stricter *per se* standard would apply rather than either *Caremark* test.[361]

4. *IN RE THE BOEING COMPANY DERIVATIVE LITIGATION*

The fifth and most recent case in which the Chancery Court allowed a *Caremark* claim to survive was *In re The Boeing Co. Derivative Litigation*. That case was the result of an even bigger corporate disaster disaster than the Blue Bell listeria outbreak—the fatal crashes of two Boeing 737 MAX airplanes.[362] "Boeing is a global aerospace corporation" and "the largest manufacturing exporter in the United States" with over $100 billion in revenue and $8 billion in profit in 2018.[363] But Boeing began falling behind Airbus, its primary competitor, when Airbus introduced the A320neo.[364] To rush a competing airplane into production, Boeing chose to develop a "derivative plane," the 737 MAX, that would only require Federal Aviation Administration (FAA)

---

357. Vice Chancellor Slights, who sustained a *Caremark* claim in *Clovis*, would dismiss two *Caremark* claims less than one year later. *In re GoPro, Inc. S'holder Deriv. Litig.*, No. 2018-0784-JRS, 2020 WL 2036602 (Del. Ch. Apr. 28, 2020); *Pettry v. Smith*, No. 2019-0795-JRS, 2021 WL 2644475 (Del. Ch. June 28, 2021), *aff'd,* 273 A.3d 750 (Del. 2022).

358. *Chou*, 2020 WL 5028065, at *20 ("[T]he Davis Polk Report serves as a backdrop against which the other pled red flags must be viewed.").

359. *Id.* at *17. The Chancery Court ultimately ruled that the Type II claims survived and thus there was no need to reach the Type I claim. *Id.* at *26.

360. *Id.* at *21 ("[T]he Plaintiffs plead mutually exclusive occurrences, that is, the Board was not informed of Mullen's allegations (supporting a 'prong one' *Caremark* claim) *and* that the Board consciously ignored Mullen's allegations (supporting a 'prong two' *Caremark* claim)."); *see also* Lund, *supra* note 126, at 407 (referring to the post-*Stone* test as "disjunctive").

361. *See* Pace, *supra* note 47, at 10 (discussing the application of Delaware corporation law in that situation by the U.S. Court of Appeals for the Seventh Circuit in *In re Abbott Lab'ys Derivative S'holders Litig.*, 325 F.3d 795 (7th Cir. 2003)).

362. *Id.* at *1.

363. *Id.* at *2, *11; David Gelles, *'I Honestly Don't Trust Many People at Boeing': A Broken Culture Exposed*, N.Y. TIMES, https://www.nytimes.com/2020/01/10/business/boeing-737-employees-messages.html [https://perma.cc/KU7H-STFN] (Oct. 15, 2021).

364. *Boeing*, 2021 WL 4059934, at *7.

certification for changes from the base plane, not the entire plane.[365] That proved to be a fatal error.

The larger engine on the 737 MAX shifted the airplane's center of gravity, causing the plane to tend to tilt up during flight.[366] Boeing responded with a software solution that incorrectly pushed the plane down if a single, temperamental sensor failed.[367] This was a known issue, but a proposed fix was rejected "due to additional cost and pilot training."[368] The pilot could prevent catastrophic results but only if they responded within ten seconds.[369] Boeing convinced the FAA to allow flight training for the 737 MAX on a tablet computer rather than a flight simulator, a policy it would later use in its sales pitch for the 737 MAX.[370] The issue was raised in neither "airplane manuals [or] pilot training materials for U.S.-based airlines."[371]

In October 2018, a new 737 MAX crashed in the Java Sea off "Indonesia, killing all 189 passengers and crew."[372] In March 2019, another new 737 MAX crashed in Ethiopia "shortly after taking off, killing all 157 passengers and crew."[373] Both crashes were caused by the known software issue.[374] Within three days, every major aviation regulator had grounded the 737 MAX, and the 737 MAX would stay grounded for the better part of two years.[375] The board responded by firing the Boeing CEO.[376]

Any scapegoating aside, the financial cost to Boeing was enormous. With litigation ongoing, Boeing estimated in 2020 "that it had incurred non-litigation costs of $20 billion, and litigation-related costs in excess of $2.5 billion."[377] Boeing also "consented to the filing of a criminal information charging [it] with conspiracy to defraud the United States."[378] Boeing directors settled the *Caremark* claims against themselves for $237.5 million, "the largest settlement ever in Delaware

365. *Id.*
366. *Id.* at *8.
367. *Id.*
368. *Id.* at *9.
369. *Id.*
370. *Id.* at *9–10.
371. *Id.* at *10.
372. *Id.* at *12.
373. *Id.* at *16.
374. *Id.* at *12, *16.
375. *Id.* at *16–17, *20.
376. *Id.* at *19.
377. *Id.* at *20.
378. *Id.*

of a *Caremark*/breach of the duty of oversight case" (all of which was paid by D&O insurance).[379]

The plaintiffs' careful pleading avoids muddling the distinction between Type I and Type II *Caremark* claims, arguing that the board's inaction prior to the first crash constituted a Type I claim and that its inaction between the first and second crash constituted both a Type I and Type II claim.[380] Boeing's board fell short in a number of ways, resulting in "a sustained or systematic failure of the board to exercise oversight."[381] Boeing did not have a board directly responsible for monitoring airplane safety, and "the Audit Committee did not regularly or meaningfully address or discuss airplane safety."[382] The board as a whole did not devote meaningful time to monitoring safety either.[383] Its first formal meeting to address the first crash, two months after the crash occurred, only concerned the "restoration of profitability and efficiency, but not product safety."[384]

Boeing did not have an internal reporting system for whistleblowers that reached the board.[385] The board did not "expect or demand that management would deliver safety reports or summaries" to it on a regular basis.[386] The board's reliance on management to report on safety at their discretion continued after the first crash.[387] The Chancery Court interpreted emails between directors—suggesting the devotion of a full board meeting to safety and on the value of management safety briefings during prior service on another board—as showing the directors knew their current efforts were inadequate.[388]

After four cases, another *Caremark* claim surviving a motion to dismiss should have hardly come as a surprise, but *Boeing* remains important for a number of reasons. It confirms that *Caremark* remains reinvigorated in 2021. It confirms that the logic of *Marchand* is not limited to monoline companies[389] and emphasizes that *Caremark* liability

---

379. Kevin LaCroix, *Boeing Air Crash Derivative Lawsuit Settles for $237.5 Million*, D&O DIARY (Nov. 7, 2021), https://www.dandodiary.com/2021/11/articles/shareholders-derivativelitigation/boeing-air-crash-derivative-lawsuit-settles-for-237-5-million [https://perma.cc/LD6R-U6L3].

380. *Boeing*, 2021 WL 4059934, at *25.

381. *Id.* (quoting *In re Citigroup Inc. S'holder Deriv. Litig.*, 964 A.2d 106, 122 (Del. Ch. 2009)).

382. *Id.* at *27.

383. *Id.* at *27–28.

384. *Id.* at *28.

385. *Id.* at *7, *27.

386. *Id.* at *29.

387. *Id.* at *30.

388. *Id.* at *32.

389. Boeing's commercial airplane division accounted for "approximately 61.7% of the Company's revenue in 2017 and 45% of its revenue in 2019," but Boeing

threatens where risks are "mission critical,"[390] a term the opinion used six times.[391] *Boeing* is important for its careful parsing of when *both* a Type I and a Type II *Caremark* claim could successfully be brought together, even if the opinion does not reach the Type II claim.[392] *Boeing* is important because it shows that *Caremark*'s reinvigoration does not mean that *all* bad faith claims are similarly reinvigorated: the Chancery Court dismissed claims related to the compensation paid to the ousted Boeing CEO.[393] *Boeing* also leaves open the question of whether *officers* can be liable under the *Caremark* doctrine.[394] The *Boeing* decision was written by yet another vice chancellor; four of the seven sitting chancery judges have now written opinions sustaining *Caremark* claims.[395]

III. REASSESSING *CAREMARK* DOCTRINE AFTER *MARCHAND*

None of the opinions from the 2019 to 2021 *Caremark* quintet of cases purported to change *Caremark* doctrine, nor can they be said to have changed black letter law. *Caremark* doctrine is the same today as it was before *Marchand*. But it is a doctrine with considerably more bite today than it had before *Marchand*. The five successful *Caremark* claims in a short interval after twenty-five years as "the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment" signals a newly invigorated doctrine.[396] At the same time, *Caremark* claims have not become an easy route to establish director liability. At least seven *Caremark* claims have been dismissed since the Delaware Supreme Court decided *Marchand*.[397] The question, then, is what fact

---

has other divisions and sells commercial airplanes other than the 737 MAX. *Id.* at *2, *11.

390. *Id.* at *26, *33. (quoting *Marchand v. Barnhill*, 212 A.3d 805, 824 (Del. 2019)).

391. *Id.* at *1, *26, *29, *33.

392. *Id.* at *25, *33–34.

393. *Id.* at *35–36.

394. *Id.* at *36.

395. *Boeing*, 2021 WL 4059934 (decided by Vice Chancellor Zurn); *Teamsters Loc. 443 Health Servs. & Ins. Plan v. Chou*, No. 2019-0816-SG, 2020 WL 5028065 (Del. Ch. Aug. 24, 2020) (decided by Vice Chancellor Glasscock); *Hughes v. Hu*, No. 2019-0112-JTL, 2020 WL 1987029 (Del. Ch. Apr. 27, 2020) (decided by Vice Chancellor Laster); *In re Clovis Oncology, Inc. Deriv. Litig.*, No. 2017-0222-JRS, 2019 WL 4850188 (Del. Ch. Oct. 1, 2019) (decided by Vice Chancellor Slights).

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

397. *Pettry v. Smith*, No. 2019-0795-JRS, 2021 WL 2644475 (Del. Ch. June 28, 2021); *Richardson v. Clark*, No. 2019-1015-SG, 2020 WL 7861335 (Del. Ch. Dec. 31, 2020); *In re GoPro, Inc. S'holder Deriv. Litig.*, No. 2018-0784-JRS, 2020 WL 2036602 (Del. Ch. Apr. 28, 2020); *In re MetLife Inc. Derivative Litig.*, No. 2019-0452-SG, 2020 WL 4746635 (Del. Ch. Aug. 17, 2020); *Owens v. Mayleben*, No. 12985-VCS, 2020 WL 748023 (Del. Ch. Feb. 13, 2020); *In re LendingClub Corp. Deriv. Litig.*, No.

patterns can we expect to result in successful *Caremark* claims in the future?

A. Mission Critical Risk is Caremark *Risk*

There are three possibilities. The first is that successful *Caremark* claims will be limited to monoline companies. The Delaware Supreme Court's *Marchand* opinion stresses that Blue Bell only sold ice cream.[398] Clovis was a pharmaceutical start-up with only three drugs in development,[399] and Medical Initiatives' entire business was putting drugs from vials into syringes.[400] But it was AmerisourceBergen that was the nominal defendant in the *Chou* derivative lawsuit, not AmerisourceBergen's indirect subsidiary Medical Initiatives.[401] Medical Initiatives was only a small part of AmerisourceBergen's total business,[402] although, as a large pharmaceutical company, compliance with FDA regulations was still a "primary regulatory concern" for AmerisourceBergen.[403] And the *Hughes* court never mentions whether Kandi was a monoline company,[404] implying that it was not relevant. It is unlikely that *Marchand* would have been decided differently had Blue Bell also sold Pez dispensers so long as the financial impact of the listeria outbreak was the same. Blue Bell's reliance on a single product made it vulnerable, but it was ultimately the scale of the impact that mattered. This logic was reaffirmed by the Chancery Court in *Boeing*, where the 737 MAX was only one of several commercial airplanes sold by Boeing, with commercial airplanes as a whole accounting for between two- and three-fifths of company revenue.[405]

The second possibility is that successful *Caremark* claims will be limited to highly regulated industries or maybe even only industries regulated by the FDA. Blue Bell, Clovis, Medical Initiatives were all regulated by the FDA.[406] The DOJ is particularly active in pursuing

---

12984-VCM, 2019 WL 5678578 (Del. Ch. Oct. 31, 2019); *Rojas v. Ellison*, No. 2018-0755-AGB, 2019 WL 3408812 (Del. Ch. July 29, 2019).

398. *See Marchand v. Barnhill*, 212 A.3d 805, 809 (Del. 2019) ("As 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.").

399. *Clovis*, 2019 WL 4850188, at *2.

400. *Chou*, 2020 WL 5028065, at *1.

401. *Id.*

402. *Id.* at *2.

403. *Id.* at *18.

404. *Hughes v. Hu*, No. 2019-0112-JTL, 2020 WL 1987029 (Del. Ch. Apr. 27, 2020).

405. *In re The Boeing Co. Deriv. Litig.*, No. 2019-0907-MTZ, 2021 WL 4059934, at *2 (Del. Ch. Sept. 7, 2021).

406. *See Marchand v. Barnhill*, 212 A.3d 805, 810 (Del. 2019) (noting that the FDA regulates food safety and that Blue Bell was required to comply with FDA

healthcare companies, with $2.6 billion out of $3 billion total in 2019 DOJ civil litigation fraud and false claims recoveries coming from healthcare companies.[407] But the FDA is far from the only active regulator, and the food and drug industries are far from the only heavily regulated industries. Kandi was not regulated by the FDA.[408] Boeing is highly regulated by the FAA and the National Transportation Safety Board,[409] which at least dispenses with the possibility that successful *Caremark* claims will be limited to industries regulated by the FDA.

The third and most plausible possibility is that successful *Caremark* claims will be limited to mission critical operations. As a "monoline company that makes a single product, . . . food safety was an essential and *mission critical*" compliance risk for Blue Bell.[410] For Clovis, the improperly calculated ORR and failure to follow clinical trial protocols was "a *mission critical* failure to comply."[411] For AmerisourceBergen, compliance with FDA regulations was "*absolutely critical* to its business."[412] The Chancery Court in *Chou* did not say that the AmerisourceBergen board must *always* "actively exercise its oversight duties," but rather that it must do so "when regulations governing drug health and safety are at issue," because compliance with those regulations is mission critical.[413] The Chancery Court in *Boeing* quotes the term "mission critical" six times.[414]

The final remaining question is whether the 2019 to 2021 *Caremark* quintet provides any clarity as to whether the *Caremark* doctrine requires underlying unlawful conduct. The doctrine does not *require* by its own terms unlawful corporate conduct.[415] Nevertheless, the application of

---

regulations); *Chou*, 2020 WL 5028065, at *2 (noting that Medical Initiatives used sham prescriptions to avoid FDA oversight); *In re Clovis Oncology, Inc. Deriv. Litig.*, No. 2017-0222-JRS, 2019 WL 4850188, at *1 (Del. Ch. Oct. 1, 2019) ("Clovis conducted its clinical trial of Roci subject to strict protocols and associated FDA regulations. Yet, assuming the pled facts are true, the Board ignored red flags that Clovis was not adhering to the clinical trial protocols, thereby placing FDA approval of the drug in jeopardy.").

407. Press Release, U.S. Dep't of Just., Justice Department Recovers over $3 Billion from False Claims Act Cases in Fiscal Year 2019 (Jan. 9, 2020), https://www.justice.gov/opa/pr/justice-department-recovers-over-3-billion-false-claims-act-cases-fiscal-year-2019 [https://perma.cc/55ET-8NC3].

408. *Hughes*, 2020 WL 1987029.

409. *Boeing*, 2021 WL 4059934, at *4, *28.

410. *Marchand*, 212 A.3d at 809, 824 (emphasis added).

411. *Clovis*, 2019 WL 4850188, at *15 (emphasis added).

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

413. *Id.*; *see also* Shapira, *supra* note 73, at 1866 ("Following *Marchand* and *Clovis*, *Chou* implies an enhanced oversight duty for 'mission critical' risks.").

414. *Boeing*, 2021 WL 4059934, at *1, *26, *29, *33.

415. *See* Bainbridge, *supra* note 77, at 968 ("There is no doctrinal reason that *Caremark* claims should not lie in cases in which the corporation suffered losses, not due to a failure to comply with applicable laws, but rather due to lax risk management.").

Caremark doctrine shows that the presence of unlawful corporate conduct really does matter.[416] All five cases from the 2019 to 2021 *Caremark* quintet involved unlawful conduct.[417] Again, black letter *Caremark* doctrine has not changed. But as to this particular aspect, at least, the application remains the same. It seems unlikely that a claim not tied to underlying unlawful corporate conduct could succeed.

Success on a *Caremark* claim remains hard enough to find even *with* unlawful corporate conduct. But mission criticality will be determined based on overall impact, not just on the direct impact of the unlawful corporate conduct. Blue Bell would have suffered severe customer backlash after the listeria outbreak even if it had not been legally obligated to recall its products. Clovis' business was devastated because its most promising drug did not work; this would have been the case regardless of whether they faced FDA sanction.

The bottom line is that the black letter law is the same, but its application is much more vigorous. The *Caremark* standard may not quite be the great hurdle it has traditionally been, but nor is it easily surmounted. The conscious disregard standard remains.[418] All five cases from the 2019 to 2021 *Caremark* quintet qualify as egregious.[419] But it does not necessarily follow that a newly reinvigorated *Caremark* doctrine

---

416. *See* Pollman, *supra* note 58, at 2031 ("[C]ourts have drawn a line between the oversight of business risk and legal risk—the former given wide allowance and the latter deemed improper.").

417. *See Marchand v. Barnhill*, 212 A.3d 805, 813–15 (Del. 2019) (noting that the FDA was involved in the recall process and also found food contamination and other issues when it inspected Blue Bell's production facilities); *Boeing*, 2021 WL 4059934, at *15–17 (noting that DOJ "opened a criminal investigation into whether Boeing had defrauded the FAA" resulting in a total payment by Boeing of over $2.5 billion and that all major aviation regulators grounded the 737 MAX); *Chou*, 2020 WL 5028065, at *6–8 (noting that the DOJ filed a criminal information against an AmerisourceBergen subsidiary for violating the Food and Drug Commission Act and that it subsequently pled guilty to violations); *Hughes v. Hu*, No. 2019-0112-JTL, 2020 WL 1987029, at *8 (Del. Ch. Apr. 27, 2020) (noting that the company faced four *unsuccessful* securities class actions); *In re Clovis Oncology, Inc. Deriv. Litig.*, No. 2017-0222-JRS, 2019 WL 4850188, at *8–10 (Del. Ch. Oct. 1, 2019) (noting that the FDA voted to delay action on the drug in question and that both an SEC complaint and securities class action were filed against Clovis and its CEO and CFO).

418. *Compare Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006) ("Where directors fail to act in the fact of a known duty to act, thereby demonstrating a *conscious disregard* for the responsibilities, they breach their duty of loyalty by failing to discharge that fiduciary obligation in good faith.") (emphasis added) (first citing *In re the Walt Disney Co. Deriv. Litig.*, 906 A.2d 27, 67 (Del. 2006); and then citing *Guttman v. Huang*, 823 A.2d 492, 506 (Del. Ch. 2003)), *with Marchand*, 212 A.3d at 821.

419. The one possible exception is *Chou*. What happened at Medical Initiatives was egregious, but Medical Initiatives was a mere indirect subsidiary of AmerisourceBergen and only accounted for a small part of its overall business. *Chou*, 2020 WL 5028065, at *1. It may not have been egregious (or mission critical) when considered at the level of the parent company.

will continue to lead to two or more successful *Caremark* claims every year. *Caremark* has more bite than it used to, but avoiding *Caremark* liability is entirely within a board's power. Just as "*Caremark* spurred the development of corporate internal control systems,"[420] the 2019 to 2021 *Caremark* quintet will spur greater board attention to internal controls.

B. An Invigorated Caremark *and Cybersecurity*

One area where issues of inadequate controls can be especially acute is cybersecurity. The newly invigorated *Caremark* doctrine has already been tested in the cybersecurity context, with inconclusive results. Directors of Marriott International, Inc. (Marriott) were sued in a derivative action filed on December 3, 2019, after discovery of "a data security breach that had exposed the personal information of up to 500 million guests."[421] Not only was this "one of the biggest data breaches in history," it exposed the "names, passport numbers, birth dates, email and mailing addresses, [and] payment card details" of hotel guests.[422]

Marriott had continued to run the allegedly deficient reservation system of Starwood Hotels and Resorts (Starwood) after acquiring Starwood in 2016.[423] Marriott was alerted "that an unknown user had run a query in Starwood's guest reservation database" on September 7, 2018.[424] Marriott's outside investigators discovered malware on the Starwood system ten days later.[425] CEO Arne Sorenson notified the board the next day, just eleven days after Marriott's first inklings of a data breach.[426] Both the audit committee and the full board would receive regular updates from management as the investigation continued.[427] Marriott publicly announced the data breach on November 30, 2018.[428] The legal fallout was significant. Marriott faced investigations by state attorneys general (all of them), the SEC, the FTC, Congress, and "class action lawsuits for violations of federal securities laws, violations of state and federal consumer protection laws, and violations of state disclosure laws."[429]

---

420. Fairfax, *supra* note 74, at 439.

421. *Firemen's Ret. Sys. of St. Louis v. Sorenson (Marriott)*, No. 2019-0965-LWW, 2021 WL 4593777, at *1, *5–6 (Del. Ch. Oct. 5, 2021).

422. *Id.* at *4

423. *Id.* at *1.

424. *Id.* at *4.

425. *Id.*

426. *Id.*

427. *Id.*

428. *Id.*

429. *Id.* at *5.

The Chancery Court dismissed the *Caremark* claims against the Marriott directors because they "were 'routinely apprised' on cybersecurity risks and mitigation, provided with annual reports . . . that specifically evaluated cyber risks, and engaged outside consultants to improve and auditors to audit corporate cybersecurity practices."[430] Red flags were reported to the board, and management took a number of steps to remediate those failures, even if those efforts were ultimately unsuccessful.[431]

Another *Caremark* suit related to two cyber incidents was filed in April 2020 against directors of Laboratory Corporation of America Holdings (LabCorp) and bears watching.[432] The first exposed names and addresses, social security numbers, medical information, and credit card information for over ten million LabCorp patients, and the second exposed over ten thousand documents, often including social security numbers and medical information.[433] LabCorp disclosed the first breach only after disclosure by another company and news reports and disclosed the second in a press release rather than directly to affected customers or in an SEC filing.[434]

LabCorp was subsequently sued in a class action for "negligence, negligence per se, unjust enrichment, breach of contract, and multiple violations of state health care information acts, privacy acts, and identify theft protection acts."[435] The data breaches have been expensive for LabCorp. Legal fees and settlement or judgment costs associated with the class action, this derivative lawsuit, and subsequent government enforcement actions caused LabCorp to "spen[d] $11,500,000 during 2019 for response and remediation costs" for the first breach alone.[436]

LabCorp had both an audit committee (with cybersecurity responsibilities) and a quality and compliance committee.[437] Management reported regularly to the audit committee and full board on cybersecurity.[438] The plaintiff alleged both Type I and Type II *Caremark* violations.[439] Per the complaint, the directors "failed to implement . . . effective internal controls," failed to monitor legal compliance, failed "to ensure that [LabCorp] utilized proper cybersecurity safeguards," and

---

430. *Id.* at *6, *13.

431. *Id.* at *13.

432. Verified Shareholder Derivative Complaint, *Eugenio v. Berberian*, No. 2020-0305-PAF (Del. Ch. 2020).

433. *Id.* ¶¶ 2, 5, 8–9, 12.

434. *Id.* ¶¶ 9, 11, 109–12, 200.

435. *Id.* ¶¶ 13–14 (citing Transfer Order, *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, No. 19-md-2904 (D.N.J. July 31, 2019)).

436. *Id.* ¶¶ 16, 209.

437. *Id.* ¶¶ 78–80, 82, 235.

438. *Id.* ¶¶ 191–92, 232.

439. *Id.* ¶¶ 18, 246.

failed "to have a sufficient incident response plan to immediately respond to the Data Breaches" (allegations of a Type I claim).[440] But the complaint further alleged that the directors "refused to act in the face of numerous red flags demonstrating the insufficient data security practices of its vendor . . . and the internal [LabCorp] practices, and failed to implement controls designed to protect against a data breach" (allegations of a Type II claim).[441]

The third, and perhaps the most important, cyber incident-related *Caremark* claim was lodged against technology company SolarWinds. SolarWinds sells "information technology ('IT') infrastructure management software" to clients that include "499 of the Fortune 500, major U.S. technology companies such as Intel and Microsoft, all of the top ten U.S. telecommunications companies, all of the top five U.S. accounting firms" and multiple government agencies, including the Departments of "Defense, State, Treasury, Justice, and Energy."[442] The nature of SolarWinds software gave it valuable (to hackers) access to its clients' most sensitive systems.[443] Russian hackers used SolarWinds software to gain access into the systems of as many as "18,000 of [SolarWinds'] clients, including numerous U.S. national security agencies and leading technology companies."[444] The complaint stresses that SolarWinds is a "*monoline* provider of information technology" with only one "line of business" and that its "directors had a fiduciary duty to monitor and oversee [SolarWinds'] known *mission critical* cybersecurity risks."[445]

The cyber incident resulted in SolarWind's stock losing almost forty percent of its value, its license revenue declining by twenty-seven percent, and it incurring direct expenses of $34 million.[446] The DOJ,

---

440. *Id.* ¶ 85.

441. Such allegations were a Type II claim. *Id.* ¶ 237. A *Caremark* claim was also recently filed in federal court against T-Mobile USA, Inc. directors. Verified Stockholder Derivative Complaint, *Litwin v. Sievert*, No. 2:21-cv-01599 (W.D. Wash. filed Nov. 21, 2022). *See also* Kevin LaCroix, *Data Breach-Related Derivative Suit Filed Against T-Mobile USA Board*, D&O DIARY (Nov. 30, 2021), https://www.dandodiary.com/2021/11/articles/cyber-liability/data-breach-related-derivative-suit-filed-against-t-mobile-usa-board [https://perma.cc/XTU9-JQMJ] (noting that "[a]lthough the plaintiff's complaint does not expressly use the words 'breach of the duty of oversight' or refer to 'Caremark duties,' the complaint does refer to the board's alleged 'failure to monitor' and to the board's alleged failure 'to heed red flags'— the very kind of allegations that are at the heart of breach of the duty of oversight claims").

442. Verified Shareholder Derivative Complaint ¶¶ 2, 33, *Constr. Indus. Laborers Pension Fund v. Bingle*, No. 2021-0940-SG, 2022 WL 4102492 (Del. Ch. Sept. 6, 2022) [hereinafter *Bingle* Complaint].

443. *Id.* ¶ 3.

444. *Id.* ¶ 4.

445. *Id.* ¶¶ 1–2, 13 (emphasis added).

446. *Id.* ¶¶ 107–08.

SEC, and state attorneys general launched investigations, and private plaintiffs filed multiple class action lawsuits.[447] All of this took place against "the context of affirmative SEC regulatory guidance imposing cybersecurity oversight and disclosure obligations on boards" and "increasingly positive legal requirements promulgated by the SEC that reflect the mission critical nature of cybersecurity oversight."[448] The complaint alleged that "SolarWinds suffered from internal cybersecurity deficiencies that defied elementary cybersecurity standards for any modern company, let alone one with a heightened risk of cyberattack."[449] In doing so, the complaint raised a Type I *Caremark* claim, alleging that the SolarWinds directors utterly failed "to monitor or oversee any aspect" of SolarWinds known, fundamental cybersecurity risks.[450]

The Chancery Court dismissed the *Caremark* claim against the SolarWinds directors but, in doing so, did not reject the possibility of a successful cyber-related *Caremark* claim entirely.[451] Indeed, it accepted that cybersecurity is mission critical, at least for online service providers.[452] Any Type I claim failed because SolarWinds had two committees, the audit committee and the nominating and corporate governance committee, with cyber risk as a part of their portfolios, and the nominating and corporate governance committee received a management presentation on cybersecurity, discussed cybersecurity afterward, and the committee charter was amended to explicitly include cyber and data security shortly thereafter.[453] Any Type II claim failed because the alleged red flags were either not red flags or the complaint did not allege the *board* (or the relevant board committees) were aware of red flags.[454] More problematic is the Chancery Court's analysis of the positive law predicate. The opinion mentioned "warnings by government agencies" and interpretative guidance from the SEC but ignored the loose

447. *Id.* ¶ 109; *see also In re SolarWinds Corp. Sec. Litig.*, 1:21-CV-138-RP, 2022 WL 958385 (W.D. Tex. Mar. 30, 2022) (denying, substantially, a motion to dismiss securities class action).

448. *Bingle* Complaint, *supra* note 442, ¶¶ 58, 61.

449. *Id.* ¶ 11.

450. *Id.* ¶ 13; *see also* Leo E. Strine, Jr., Kirby M. Smith & Reilly S. Steel, Caremark *and ESG, Perfect Together: A Practical Approach to Implementing an Integrated, Efficient, and Effective* Caremark *and EESG Strategy*, 106 IOWA L. REV. 1885, 1906–07 (2021) (referencing oversight claims after data breaches filed in federal court).

451. *See Constr. Indus. Laborers Pension Fund v. Bingle*, No. 2021-0940-SG, slip op. at 18 (Sept. 6, 2022) (echoing *Firemen's Ret. Sys. of St. Louis v. Sorenson (Marriott)*, No. 2019-0965-LWW, 2021 WL 4593777 (Del. Ch. Oct. 5, 2021), in suggesting that a failure of cybersecurity oversight may lead to a successful *Caremark* claim).

452. *Id.* at 3.

453. *Id.* at 7–9, 29–31.

454. *Id.* at 26–28.

approach taken in *Marchand* and the allegations in the complaint of investigations by "the DOJ, SEC, and state Attorneys General" and "several private class action lawsuits."[455]

IV. TECHNOLOGICAL CHALLENGES TO CORPORATE GOVERNANCE

Within the last two decades alone, rapid technological change has created a daily struggle to keep pace by both corporate boards,[456] and regulators alike.[457] New technologies such as those based on the blockchain,[458] the Internet of Things (IoT),[459] growth in adoption of virtual currencies and payment systems,[460] privacy issues,[461] and

455. *Id.* at 24; *Marchand v. Barnhill*, 212 A.3d 805, 823 (2019) ("[T]he 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."); *Bingle* Complaint, *supra* note 442, ¶ 109.

456. *See* Lawrence J. Trautman, *Rapid Technological Change and U.S. Entrepreneurial Risk in International Markets: Focus on Data Security, Information Privacy, Bribery and Corruption*, 49 CAP. U. L. REV. 67, 70 (2021).

457. *See* Neal F. Newman & Lawrence J. Trautman, *Securities Law: Overview and Contemporary Issues*, 16 OHIO STATE BUS. L.J. 149, 149, 209 (2021); Lawrence J. Trautman & George P. Michaely, Jr., *The SEC and the Internet: Regulating the Web of Deceit*, 68 CONSUMER FIN. L.Q. REP. 262, 262, 281 (2014); Lawrence J. Trautman & Neal F. Newman, *A Proposed SEC Cyber Data Disclosure Advisory Commission*, 50 SEC. REGUL. L.J. (forthcoming 2022).

458. *See generally* Brian Elzweig & Lawrence J. Trautman, *When Does a Nonfungible Token (NFT) Become a Security?*, GA. STATE U.L. REV. (forthcoming); Lawrence J. Trautman & Mason J. Molesky, *A Primer for Blockchain*, 88 UMKC L. REV. 239 (2019); Lawrence J. Trautman, *Virtual Art and Non-Fungible Tokens*, 50 HOFSTRA L. REV. 361 (2022).

459. *See generally* Lawrence J. Trautman, Mohammed T. Hussein, Louis Ngamassi & Mason J. Molesky, *Governance of the Internet of Things (IoT)*, 60 JURIMETRICS J. 315 (2020); Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 U. MIA. L. REV. 761 (2018); *see generally* Lawrence J. Trautman & Mohammed T. Hussein, *The Internet of Things (IoT) in a Post-Pandemic World*, JURIMETRICS J. (forthcoming).

460. *See generally* Lawrence J. Trautman & Alvin C. Harrell, *Bitcoin Versus Regulated Payment Systems: What Gives?*, 38 CARDOZO L. REV. 1041 (2017); Lawrence J. Trautman, *E-Commerce, Cyber, and Electronic Payment Systems Risks: Lessons from PayPal*, 16 UC DAVIS BUS. L.J. 261 (2016); Lawrence J. Trautman, *Bitcoin, Virtual Currencies, and the Struggle of Law and Regulation to Keep Pace*, 102 MARQ. L. REV. 447 (2018); Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?*, 69 CONSUMER FIN. L.Q. REP. 232 (2016); Lawrence Trautman, *Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 13 (2014).

461. *See* Lawrence J. Trautman, *Governance of the Facebook Privacy Crisis*, 20 PITT. J. TECH. L. & POL'Y 43 (2020). *See generally* Lawrence J. Trautman, *How Google Perceives Customer Privacy, Cyber, E-Commerce, Political and Regulatory Compliance Risks*, 10 WM. & MARY BUS. L. REV. 1 (2018).

cybersecurity vulnerabilities[462] are responsible for consuming considerable board attention and resources.[463] Following the highly disruptive COVID-19 pandemic,[464] to be expected, board nominating committees are challenged to recruit experienced talent having backgrounds and experience in computer science and cybersecurity issues.[465] Recently, many boards assign cyber risk oversight to the audit committee,[466] while others have a designated "risk" committee.[467]

V. GOOD FAITH CYBERSECURITY

Cyberthreats have become so pervasive and dangerous that cybersecurity is now mission critical to *every* publicly traded U.S. company.[468] *Caremark* litigation brings attention to its creation of liability

462. *See* Lawrence J. Trautman, Mohammed T. Hussein, Emmanuel U. Opara, Mason J. Molesky & Shahedur Rahman, *Posted: No Phishing*, 8 EMORY CORP. GOVERNANCE & ACCOUNTABILITY REV. 39, 41–42 (2021); David D. Schein & Lawrence J. Trautman, *The Dark Web and Employer Liability*, 18 COLO. TECH. L.J. 49, 51, 64–65 (2020).

463. *See* Lawrence J. Trautman, *The Board's Responsibility for Crisis Governance*, 13 HASTINGS BUS. L.J. 275, 337 (2017); Lawrence J. Trautman, *Managing Cyberthreat*, 33 SANTA CLARA HIGH TECH. L.J. 230, 232–33 (2016).

464. *See* Eddie Bernice Johnson & Lawrence J. Trautman, *The Demographics of Death: An Early Look at Covid-19, Cultural and Racial Bias in America*, 48 HASTINGS CONST. L.Q. 357, 440–41 (2021).

465. *See* Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment*, 11 FLA. STATE U. BUS. REV. 75, 99, 112–13 (2012); Mohammed T. Hussein, Lawrence J. Trautman & Reginald Holloway, Technology Employment, Information and Communications in the Digital Age (Nov. 4, 2021), (unpublished manuscript) (http://ssrn.com/abstract=3762273).

466. *See* Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?,* 11 DEPAUL BUS. & COM. L.J. 205, 233 (2013); Lawrence J. Trautman, *Who Sits on Texas Corporate Boards? Texas Corporate Directors: Who They Are and What They Do,* 16 HOUS. BUS. & TAX L.J. 44, 76–77 (2016).

467. *See* Lawrence J. Trautman, Seletha Butler, Frederick R. Chang, Michele Hooper, Ron McCray & Ruth Simmons, *Corporate Directors: Who They Are, What They Do, Cyber and Other Contemporary Challenges*, 70 BUFFALO L. REV. 459, 506–07 (2022).

468. *See Firemen's Ret. Sys. of St. Louis v. Sorenson (Marriott)*, No. 2019-0965-LWW, 2021 WL 4593777, at *11 (Del. Ch. Oct. 5, 2021) ("Cybersecurity [] is an area of consequential risk that spans modern business sectors."); Roy Shapira, *Mission Critical ESG and the Scope of Director Oversight Duty*, COLUM. BUS. L. REV. (forthcoming 2022) (manuscript at 5) (SSRN) [hereinafter, *Mission Critical ESG*] ("[C]ybersecurity risks are likely to count as 'mission critical' across business sectors."); Mary Galligan & Carey Oven, *A New Chapter in Cyber*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Aug. 1, 2022), https://corpgov.law.harvard.edu/2022/08/01/a-new-chapter-in-cyber [https://perma.cc/Y6PJ-2YJA] (relying on *NACD Director's Handbook on Cyberrisk Oversight*, NAT'L ASS'N OF CORP. DIRECTORS (Feb. 25, 2020)) ("Boards should understand and approach cybersecurity as a risk management issue for the entire enterprise and not just a technology or IT issue. Cybersecurity may have begun as

against directors of companies that maintain poor cybersecurity.[469] For publicly traded U.S. companies incorporated in Delaware—and over two-thirds of the Fortune 500 share are[470]—the reinvigoration of *Caremark* and the rise of cyberthreats combine to threaten director liability. Directors who fail to ensure that the corporation addresses cybersecurity *at the board level* are exposing themselves to liability. Luckily for directors, the *Marchand* opinion lays out a roadmap for directors asking what it means for a board of directors to act in "good faith."

A. Roadmap to Avoiding Liability

The first and most important principle to avoiding liability is cybersecurity oversight is too important to delegate entirely to management, even if management is competent and puts extensive processes and protocols in place. The board must take an active hand, even if management remains the primary actors in the space. Just what that active hand looks like is "context and industry specific,"[471] but Blue Bell's deficiencies translate well to lessons for the cybersecurity context.

A board committee should either be devoted entirely to cybersecurity or have cybersecurity as a significant part of its portfolio.[472] Though it is common to give responsibility over cybersecurity to the audit

primarily a technology-centric risk, but it has evolved to become a multifaceted business issue. The ability to manage cyber risk is integral to every aspect of business operations.").

469. *See* Shapira, *supra* note 73, at 1887 ("[S]takeholders of company X cannot punish the company for misbehaving if all of the company's competitors face similar allegations (they cannot take their business elsewhere). Private *Caremark* litigation helps in ferreting out who among the industry players fared worse.").

470. DEL. DIV. CORPS., 2020 ANNUAL REPORT STATISTICS (2020), https://corpfiles.delaware.gov/Annual-Reports/Division-of-Corporations-2020-Annual-Report.pdf [https://perma.cc/4ABF-KVZW]. *Caremark* doctrine is specific to Delaware, but the influence of Delaware corporation law and its courts means that changes to *Caremark* doctrine can affect the law in other states as well. *See, e.g.*, *In re Cardinal Health Inc. Deriv. Litig.*, 518 F. Supp. 3d 1046, 1066–67, 1072 (S.D. Ohio 2021) (denying a motion to dismiss claims under Ohio law against directors for failing to provide good faith oversight by responding to red flags related to the opioid epidemic and violations of the Controlled Substances Act). *But see* Keith Paul Bishop, *Still No California Caremark?*, CAL. CORP. & SECS. LAW (Jan. 28, 2021), https://www.calcorporatelaw.com/still-no-california-caremark [https://perma.cc/Q38G-92L9] ("Although a quarter century has passed, the California courts have yet to adopt *Caremark* as the standard of liability for directors of California corporations.").

471. *Marchand v. Barnhill*, 212 A.3d 805, 821 (Del. 2019).

472. *Cf. id.* at 822 ("[N]o board committee that addressed food safety existed."); *see also Guttman v. Huang*, 823 A.2d 492, 506–07 (Del. Ch. 2003) (noting that a contention such as the lack of an audit committee is vital to a *Caremark* claim).

committee,[473] this is probably a mistake. Cybersecurity is too technical to give to a committee with an existing need for a different set of skills and expertise.[474] An audit committee will already have a substantial portfolio unrelated to cybersecurity.[475] An audit committee that is responsible for cybersecurity but does not discuss cybersecurity on a regular basis invites a *Caremark* claim.[476] But very few corporations (less than ten percent) have a compliance or cybersecurity committee.[477] Even if multiple committees have cybersecurity responsibilities, a court is likely to focus on the committee with the most significant cybersecurity responsibilities.[478] Creating a dedicated cybersecurity committee "can help communicate that the board hears [cybersecurity] concerns and takes them seriously."[479]

---

473. Savarese, Eddy & Niles, *supra* note 88; *see also* Armour, *Board Compliance*, *supra* note 49, at 1198 ("One approach towards formalizing board oversight of compliance is for boards to add compliance to the remit of their audit committees."); *Cf. Constr. Indus. Laborers Pension Fund v. Bingle*, No. 2021-0940-SG, slip op. at 7–8 (noting the SolarWinds board split cybersecurity oversight between the Nominating and Corporate Governance Committee and the Audit Committee, with the audit committee having responsibility for cybersecurity as a "major financial risk exposure").

474. Cybersecurity is too important for the full board to avoid altogether. *But see Bingle*, slip op. at 28–33 (refusing to sustain a *Caremark* claim where cybersecurity oversight happened only at the committee, not full board, level, in part because directors must "exercise business judgment in determining what issues should be brought from the subcommittee to the full Board").

475. *See Hughes v. Hu*, No. 2019-0112-JTL, 2020 WL 1987029, at *5 (Del. Ch. Apr. 27, 2020) (inferring that "there was no possible way that the Audit Committee could have fulfilled all of the responsibilities it was given under the Audit Committee Charter" when it met for less than an hour a year after its last meeting); *see also* Strine, Smith & Steel, *supra* note 450, at 1915 ("[A]udit committees' core responsibilities in accounting and financial compliance, prudence, and integrity have grown even more challenging, complex, and time consuming.").

476. *Cf. Teamsters Local 443 Health Servs. & Ins. Plan v. Chou*, No. 2019-0816-SG, 2020 WL 5028065, at *9 (Del. Ch. Aug. 24, 2020) (noting that the full board "did not set aside a portion of Board meetings devoted to drug safety and compliance"); *see also* Strine, Smith & Steel, *supra* note 450, at 1917 ("By putting a critical function in a committee that cannot perform it effectively, the board risks missing issues [and] limits communications between the directors and a more diverse set of company officers.").

477. Armour, *Board Compliance*, *supra* note 49, at 1225; Gartner Jan. 28, 2021 Press Release, *supra* note 49; *see also* Ryan McManus, *A Special Board Committee Can Help Drive Corporate and Transformational Success*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Aug. 31, 2021), https://corpgov.law.harvard.edu/2021/08/31/a-special-board-committee-can-help-drive-corporate-and-transformational-success [https://perma.cc/MT6Q-JE9P] ("11.2 percent of Fortune 500 companies have committees dedicated to science, technology, and innovation.").

478. *Cf. Chou*, 2020 WL 5028065, at *9 (noting that all board committees but the executive committee had risk oversight responsibility but otherwise focusing on the audit committee in its analysis).

479. Paul DeNicola, *Questions to Ask Before Forming a New Board Committee*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Oct. 10, 2021),

The responsible committee must meet on a regular basis for sufficient durations and—if the committee's portfolio also includes unrelated issue—devote sufficient time during those meetings to cybersecurity.[480] The members of the responsible committee must have sufficient expertise to monitor the company's cybersecurity efforts,[481] and the effectiveness of the committee should be reviewed by the full board on an annual basis.[482] The "mere existence" of a committee responsible for cybersecurity is insufficient to defeat liability.[483] Furthermore, as Boeing found when it created an Aerospace Safety Committee only after two fatal crashes, establishing a board committee *after* a major data breach may be too little, too late.[484] Companies may be sluggishly rising to the challenge, with one technology consultancy predicting that, "[b]y 2025, 40% of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member."[485]

Protocols should be set to require management to regularly update the board on cybersecurity "compliance practices, risks, or reports."[486] In *Stone v. Ritter*, for example, the board "enacted written policies and procedures designed to ensure compliance with . . . regulations."[487] In *Hughes v. Hu*, the audit committee allegedly approved a number of policies and procedures but did not produce them in response to a Section

---

https://corpgov.law.harvard.edu/2021/10/10/questions-to-ask-before-forming-a-new-board-committee [https://perma.cc/64KQ-NH2C].

480. *See Hughes*, 2020 WL 1987029, at *16 ("[T]he Audit Committee never met for longer than one hour and typically only once per year. . . . The plaintiff is entitled to the inference that the board was not fulfilling its oversight duties."); *Guttman v. Huang*, 823 A.2d 492, 507 (Del. Ch. 2003) (noting that an allegation that "the company had an audit committee that met only sporadically and devoted patently inadequate time to its work" can sustain a *Caremark* claim).

481. *See Hughes*, 2020 WL 1987029, at *15 (noting that the audit committee "lacked the expertise necessary to" provide the required oversight, forcing it to instead defer to management); *see also* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590, 16593 (proposed Mar. 9, 2022) (to be codified at 17 C.F.R. pts. 229, 232, 239, 240, 249) (suggesting "to require disclosure of whether any member of [a publicly traded company's] board has expertise in cybersecurity, and if so, the nature of such expertise").

482. *See Hughes*, 2020 WL 1987029, at *4 (listing weaknesses disclosed in the company's 10-K, which included not evaluating the effectiveness of the audit committee).

483. *See id.* at *14 (noting the same in the context of an audit committee and accounting irregularities) (comparing *Ash v. McCall*, No. Civ. A. 17132, 2000 WL 1370341, at *15 n.57 (Del. Ch. Sept. 15, 2000), with *Rich ex rel. Fuqi Int'l, Inc. v. Yu Kwai Chong*, 66 A.3d 963, 983 (Del. Ch. 2013)).

484. *In re The Boeing Co. Deriv. Litig.*, No. 2019-0907-MTZ, 2021 WL 4059934, at *19 (Del. Ch. Sept. 7, 2021).

485. Gartner Jan. 28, 2021 Press Release, *supra* note 49. *But see* Strine, Smith & Steel, *supra* note 450, at 1919 ("[I]n general, it is important not to proliferate committees.").

486. *Marchand v. Barnhill*, 212 A.3d 805, 822 (Del. 2019).

487. *Stone v. Ritter*, 911 A.2d 362, 372 (Del. 2006).

220 request leading the Chancery Court to infer they did not exist.[488] In *Boeing*, the board relied on "intermittent, management-initiated communications" about safety.[489] In *Chou*, neither the audit committee nor the full board received reports on compliance at Medical Initiatives,[490] in contrast with both the audit committee and the full board in *Marriott* receiving regular reports on cybersecurity.[491] Compliance officers are reporting to the board more often,[492] but they must report specifically on cybersecurity.[493] The board should receive reports from multiple members of management rather than rely exclusively on a compliance officer.[494]

The board must discuss cybersecurity on a regular basis.[495] It should discuss cybersecurity during or after any serious cyber incident. But the board must also discuss cybersecurity issues on a regular basis regardless

---

488. *See Hughes*, 2020 WL 1987029, at *4–5 (inferring that the "sales contract entered into with Eliteway [Kandi USA]," "Approval Procedures for Relationship Transaction," "Internal Audit Activity Charter," and "Management Policy on Related-Party Transactions" did not exist because Kandi did not produce them). Kandi may have hoisted itself on its own petard. It did not produce an "Audit Committee Charter," but that charter did in fact exist and was available publicly, so the Chancery Court credited its existence. *Id.*, at *5. It may be that the Chancery Court punished Kandi for the other documents that did in fact exist because Kandi failed to produce them.

489. *Boeing*, 2021 WL 4059934, at *29.

490. *Teamsters Local 443 Health Servs. & Ins. Plan v. Chou*, No. 2019-0816-SG, 2020 WL 5028065, at *10 (Del. Ch. Aug. 24, 2020).

491. *Firemen's Ret. Sys. of St. Louis v. Sorenson (Marriott)*, No. 2019-0965-LWW, 2021 WL 4593777, at *13 (Del. Ch. Oct. 5, 2021).

492. *See* Shapira, *supra* note 73, at 1879 ("The proliferation of compliance personnel within organizations, and the credible threat of liability they face, have gradually increased the chances that these compliance officers will report to the board on thorny aspects of the company's compliance.").

493. *See Marriott*, 2021 WL 4593777, at *1 ("Cybersecurity has increasingly become a central compliance risk deserving of board level monitoring."); *see also* Antony Kim, Aravind Swaminathan & Daniel Dunne, *The Risks to Boards of Directors and Board Member Obligations*, *in* NAVIGATING THE DIGITAL AGE: THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS 51, 54 (Matt Rosenquist ed., 2015) ("Operationally, a board can exercise its oversight in a number of ways, including by [] devoting board meeting time to presentations from management responsible for cybersecurity and discussions on the subject."); Galligan & Oven, *supra* note 468 (relying on *Director's Handbook on Cyber-Risk Oversight*, *supra* note 468) ("Boards should set an expectation for management to establish an enterprise-wide risk management framework that is adequately resourced.").

494. *See* Joyce, Dobrygowski & Van der Oord, *supra* note 52 ("Directors, recognizing that cyber risk is an enterprise-wide concern, should look to a variety of executives and managers in order to ascertain the full impact of cyber risk on the organization. Each member of the management team has a responsibility to understand the impact of cyber risk within her or his remit and can therefore support the board's effort to develop a holistic view.").

495. *See Marchand v. Barnhill*, 212 A.3d 805, 822 (Del. 2019) ("[T]he board meetings are devoid of any suggestion that there was any regular discussion of food safety issues.").

of whether there was a recent cyber incident.[496] Generic discussion of compliance is not enough; the board and relevant committees must discuss cybersecurity discretely and document the same.[497] Regular time should be set aside to discuss cybersecurity.[498] In *Stone v. Ritter*, for example, the audit committee oversaw the Bank Secrecy Act and anti-money laundering regulation compliance quarterly and received training on it annually.[499] The board cannot simply defer to management on mission critical matters such as cybersecurity.[500]

Red flags should be reported up to the board.[501] Type II *Caremark* claims can result in liability where directors ignore red flags.[502] After *Marchand*, Type I *Caremark* claims can result in liability where directors do not ensure that they see red flags.[503] Focus is on board action, not management action.[504] Management may hide red flags from the board, but the board must take steps to attempt to prevent that. One option is for the officer charged with cybersecurity to report directly to the relevant

---

496. *Id.* (highlighting that there was "no schedule for the board to consider on a regular basis, such as quarterly or biannually, any key food safety risks existed").

497. *Cf. Teamsters Loc. 443 Health Servs. & Ins. Plan v. Chou*, No. 2019-0816-SG, 2020 WL 5028065, at *20 (Del. Ch. Aug. 24, 2020) (discounting discussion of a report on compliance and efforts to increase oversight over compliance because it was unclear whether it "targeted the mission critical compliance risk that undergirds the Complaint").

498. *Cf. id.* at *9 ("[T]he Board did not set aside a portion of Board meetings devoted to drug safety and compliance.").

499. *Stone v. Ritter*, 911 A.2d 362, 372 (Del. 2006).

500. *See Hughes v. Hu*, No. 2019-0112-JTL, 2020 WL 1987029, at *16 (Del. Ch. Apr. 27, 2020) ("*Caremark* envisions some degree of board-level monitoring system, not blind deference to and complete dependence on management."). Recent *Caremark* decisions, then, resurrect the suspicion of excessive board deference to management discussed in *Smith v. Van Gorkom*, 488 A.2d 858 (Del. 1985). *See* Hill & McDonnell, *supra* note 74, at 1780 ("An excellent example is *Van Gorkom*, (the duty of care case that prompted the legislature to enact section 102(b)(7)), in which the facts strongly implicated excessive deference by the officers and directors to the chief executive officer (CEO).").

501. *See Marchand v. Barnhill*, 212 A.3d 805, 822 (Del. 2019) (noting that management received reports containing "red, or at least yellow, flags" that were not "disclosed to the board").

502. *Stone*, 911 A.2d at 370 ("*Caremark* articulates the necessary conditions predicate for director oversight liability: (a) the directors utterly failed to implement any reporting or information system or controls; *or* (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.").

503. *Marchand*, 212 A.3d at 822 ("Under *Caremark*, a director may be held liable if she acts in bad faith in the sense that she made no good faith effort to ensure that the company had in place any 'system of controls.'").

504. *See id.* at 821 ("*Caremark* does have a bottom-line requirement that is important: the board must make a good faith effort—*i.e.*, try—to put in place a reasonable board-level system of monitoring and reporting.").

board committee rather than to the CEO or another officer.[505] That officer should at the very least have board-level reporting obligations.[506] Red flags that are "numerous, serious, directly in front of the directors, and indicative of a corporate-wide problem" trigger liability under *Caremark*.[507] The third requirement—"directly in front of the directors"—cannot be circumvented by the board simply not getting reports from management. The board must also respond to and follow up on red flags, not just passively receive reports on them.[508] And it must respond to red flags that it learns of outside of normal management channels.[509] Red flags should also be considered cumulatively.[510]

Board reports on cybersecurity must include both favorable information and unfavorable information.[511] Again, management might hide unfavorable information, but the board must take steps to ensure they receive the bad with the good, including by asking hard questions of members of management presenting on cybersecurity.[512] Nor can the board receive unfavorable information passively.[513] The board must take appropriate action when presented with mission critical compliance

505. *See Hughes,* 2020 WL 1987029, at *4 ("[T]he head of the Company's internal audit department reported to [the CEO] rather than to the Audit Committee, which 'impaired the independence and objectivity of the internal control audit department.'"); *see also* Armour, Garrett, Gordon & Min, *Board Compliance*, *supra* note 49, at 1218 ("Moreover, it is increasingly thought that a direct channel of reporting from compliance to the board is a means of fostering not only autonomy within the compliance program but also an open upward transmission of information.") (citing U.S. DEP'T OF JUST., CRIM. DIV., EVALUATION OF CORP. COMPLIANCE PROGRAMS (2020), https://www.justice.gov/criminal-fraud/page/file/937501/download [https://perma.cc/6Q57-DBJY]).

506. *Cf. Marchand*, 212 A.3d at 813 (noting that the "board had made no effort at all to implement a board-level system of mandatory reporting of any kind").

507. *See* Regina F. Burch, *Director Oversight and Monitoring: The Standard of Care and the Standard of Liability Post-Enron*, 6 WYO. L. REV. 481, 498 (2006).

508. *See id.* ("Defendants have not pointed to any part of the Section 220 production that refers to actions taken with regard to the shortcomings at [Medical Initiatives] concerning mission critical drug health and safety regulations.").

509. *See In re The Boeing Co. Deriv. Litig.*, No. 2019-0907, 2021 WL 4059934, at *34 (Del. Ch. Sept. 7, 2021) ("[T]he Board did not require an internal system to learn about the Lion Air Crash and the attendant MCAS failures[,] . . . a red flag . . . that the Board should have heeded but instead ignored.").

510. *See Teamsters Loc. 443 Health Servs. & Ins. Plan v. Chou*, No. 2019-0816-SG, 2020 WL 5028065, at *20 (Del. Ch. Aug. 24, 2020) ("[T]he Davis Polk Report serves as a backdrop against which the other pled red flags must be viewed.").

511. *See Marchand*, 212 A.3d at 822 ("[T]he board was given certain favorable information about food safety by management, but was not given important reports that presented a much different picture."); *see also Boeing*, 2021 WL 4059934, at *31 ("Management's *ad hoc* reports were also one-sided at best and false at worst.").

512. *See Boeing*, 2021 WL 4059934, at *29 (faulting the board for "not press[ing] for further information" when management reported on safety).

513. *See id.* (faulting the board for "passively accept[ing] management's assurances and opinions").

issues.[514] The board should follow up on remediation efforts[515] rather than simply direct management to do so.[516] As with reports and red flags, an invigorated *Caremark* doctrine shifts the board's activities in favor of its underappreciated role of engaging in "information governance"—taking an active hand in shaping the flow of information from management to the board.[517]

The board should make "use of third-party monitors, auditors, or consultants."[518] It will necessarily rely on those third parties, but it cannot display "blind deference to and complete dependence on" them.[519] The Delaware courts have a long history of encouraging boards to make use of third parties; "more reliance on and more fees for lawyers, investment bankers, accountants, management consultants, and economists" was, after all, one of the lessons from *Smith v. Van Gorkom*.[520] Similarly, the Chancery Court in *Marriott* specifically credited the directors for leveraging outside consultants and auditors to improve company cybersecurity practices.[521] Third-party reports that the board would be unwilling to produce in an attempt to protect attorney-client privilege would be of limited use in defending a *Caremark* claim, though.[522]

---

514. *See Chou*, 2020 WL 5028065, at *25 ("The Defendants have put forth nothing from the Section 220 production showing a tangible reaction to—as opposed to a review of—the mission critical compliance failures at [Medical Initiatives].").

515. *See id.* at *21–25 (ruling that red flags triggered *Caremark* in part because the Audit Committee and full board did not present documentation of remediation efforts or of otherwise following up to confirm issues were addressed).

516. *See id.* at *12 (noting that the Audit Committee directed management to follow up on recommendations in a law firm report on compliance deficiencies).

517. *See* Faith Stevelman & Sarah C. Haan, *Boards in Information Governance*, 23 U. PA. J. BUS. L. 179, 181–82, 268–70 (2020) (defining "information governance" and discussing it in the context of *Marchand* and *Caremark*).

518. *Marchand v. Barnhill*, 212 A.3d 805, 823 (Del. 2019).

519. *Hughes v. Hu*, No. 2019-0112-JTL, 2020 WL 1987029, at *16 (Del. Ch. Apr. 27, 2020).

520. 488 A.2d 858 (Del. 1985); *see* Leo Herzel & Leo Katz, Smith v. Van Gorkom: *The Business of Judging Business Judgment*, 41 BUS. LAW. 1187, 1191 (1986) (criticizing *Smith v. Van Gorkom* for imposing greater formalism on boards and thus incentivizing board reliance on experts); *see also* Bainbridge, *supra* note 100, at 27 (criticizing the invigoration of *Caremark* for "incentiviz[ing] directors to overinvest in lawyers and experts").

521. *Firemen's Ret. Sys. of St. Louis v. Sorenson (Marriott)*, No. 2019-0965-LWW, 2021 WL 4593777, at *13 (Del. Ch. Oct. 5, 2021); *see also* Kim, Swaminathan & Dunne, *supra* note 493 ("Business judgment rule protection is strengthened by ensuring that board members . . . have access to cyber experts whose expertise and experience the board members can rely on in making decisions about what to do (or not to do) to address cybersecurity risks."); *see also* Galligan & Oven, *supra* note 468 (suggesting "[p]resentations at board meetings by internal and external cyber risk experts" to increase the board's understanding of cybersecurity issues).

522. *See Teamsters Loc. 443 Health Servs. & Ins. Plan v. Chou*, No. 2019-0816-SG, 2020 WL 5028065, at *23 (Del. Ch. Aug. 24, 2020) ("It is unclear what Ober Kaler's recommendations were because the report was withheld as privileged. . . .

Board minutes should reflect the above. *Marchand* was decided on a motion to dismiss, settling before trial.[523] The Chancery and Supreme Court decisions, then, were made on the basis of board minutes and other board documents appended to the complaint.[524] Board discussion of cybersecurity not reflected in the minutes is of limited to no value at the motion to dismiss stage, and it is on that ground that *Caremark* battles will continue to be fought. Dissident shareholders will have access to board minutes and supporting materials under Section 220 of the Delaware General Corporation Law, and Delaware courts will expect them to take full advantage.[525] Supporting materials may be substantial, as in *Boeing*, where the plaintiff-shareholders gained access to 44,000 internal documents.[526] In *Stone v. Ritter*, for example, the plaintiffs requested books and records, which produced a company-wide, board-enacted Bank Secrecy Act and anti-money laundering regulation policy that was appended to the plaintiff's complaint.[527] Conversely, if the corporation fails to produce relevant documents, the Chancery Court will assume that these do not exist.[528] This includes where documents are

---

Consequently, without knowing what these recommendations were, it is not possible at this time to draw an inference regarding the extent of the measures implemented.").

523. *Marchand*, 212 A.3d at 824; *see also* Roger A. Cooper & Mark E. McDonald, Caremark *Claims on the Rise Fueled by Section 220 Demands*, CLEARY GOTTLIEB (Jan. 11, 2021), https://www.clearygottlieb.com/news-and-insights/publication-listing/caremark-claims-on-the-rise-fueled-by-section-220-demands [https://perma.cc/JF84-4BNU]) (noting that "Delaware courts in the past 'routinely dismissed *Caremark* claims at the motion to dismiss stage, even in the face of substantial "corporate traumas,"'" which is typical for many *Caremark* claims).

524. *See* Kevin M. LaCroix, *A "New Era" of Caremark Claims?*, D&O DIARY (Jan. 20, 2021), https://www.dandodiary.com/2021/01/articles/director-and-officer-liability/a-new-era-of-caremark-claims [https://perma.cc/283E-ZB3Q] ("At a minimum, the recent *Caremark* duty decisions represent developments about which boards must be aware . . . . Not only must boards establish monitoring mechanisms, particularly with respect to mission critical operations, but they must also be able to show that they were monitoring the mechanisms and responding to red flags and other alerts.").

525. *See, e.g.*, Savarese, Eddy & Niles, *supra* note 85 ("Stockholder inspection demands to review a company's books and records, including board- and committee-level minutes, in preparation for litigation are increasingly common and allowed by the courts where legal requirements are met."); *see also* Kim, Swaminathan & Dunne, *supra* note 493, at 51, 54 ("Boards should . . . make sure that these actions are clearly documented in board and committee packets, minutes, and reports.").

526. Roy Shapira, *Max Oversight Duties: How* Boeing *Signifies a Shift in Corporate Law*, 48 J. CORP. L. (forthcoming 2022) (manuscript at 21).

527. *Stone v. Ritter*, 911 A.2d 362, 372 (Del. 2006).

528. *See Hughes v. Hu*, No. 2019-0112-JTL, 2020 WL 1987029, at *2 (Del. Ch. Apr. 27, 2020) ("Given this stipulation [that materials requested either do not exist or are withheld on privilege grounds], if the Company failed to produce a document that it would reasonably be expected to possess if a particular event had occurred, then the plaintiff is entitled to a reasonable inference that the event did not occur.") (citing *Morrison v. Berry*, 191 A.3d 268, 275 n.20 (Del. 2018)).

referenced in board documents but not produced.[529] For this reason, books and records requests have been an important step in successful *Caremark* claims.[530]

Compliance with prophylactic government regulations alone is not enough. The Delaware Supreme Court rejected the defense that Blue Bell complied with FDA regulations.[531] Nor did compliance with FAA regulations save the Boeing directors, because it does not evidence board-level oversight, which is exactly what *Caremark* measures.[532] Government regulations are a floor, not a ceiling. Corporate conduct can satisfy prophylactic regulation but still result in legal liability after the fact, as was the case for both Blue Bell and Boeing.[533] And, again, there is a laser focus on the board that may not have been present in *Caremark* opinions before *Marchand*.

Boards must respond appropriately to cybersecurity incidents *and* known cybersecurity vulnerabilities. *Marchand* involved a Type I *Caremark* claim. After *Marchand*, "keeping your head in the sand" is no longer a viable strategy for directors seeking to avoid liability. The specter of Type II claims remains, though. Directors must take steps to ensure red flags are raised to the board; once they have been, they cannot be ignored without risking a Type II claim.

B. The Role of Positive Law in Caremark *Claims*

Under both the original analytical framework in *Caremark* and as revised and restated in *Stone v. Ritter*, underlying unlawful corporate activity is not a predicate to *Caremark* liability.[534] But underlying

529. *See, e.g.*, *id.* at *4 ("The Audit Committee also purportedly reviewed a document titled 'Approval Procedures of Relationship Transaction.' The Company failed to produce this document in response to the plaintiff's inspection demand. It is reasonable to infer that the Audit Committee did not receive or review this document.") (cleaned up).

530. *Teamsters Loc. 443 Health Servs. & Ins. Plan v. Chou*, No. 2019-0816-SG, 2020 WL 5028065, at *2 (Del. Ch. Aug. 24, 2020); *Hughes*, 2020 WL 1987029, at *2; *In re Clovis Oncology, Inc. Deriv. Litig.*, No. 2017-0222, 2019 WL 4850188, at *9–10 (Del. Ch. Oct. 1, 2019).

531. *Marchand v. Barnhill*, 212 A.3d 805, 823 (Del. 2019).

532. *In re The Boeing Co. Deriv. Litig.*, No. 2019-0907-MTZ, 2021 WL 4059934, at *28 (Del. Ch. Sept. 7, 2021) (relying on *Marchand*, 212 A.3d at 823).

533. *Marchand*, 212 A.3d at 824; *Boeing*, 2021 WL 4059934, at *28.

534. *See* Bainbridge, *supra* note 77, at 968 ("There is no doctrinal reason that *Caremark* claims should not lie in cases in which the corporation suffered losses, not due to a failure to comply with applicable laws, but rather due to lax risk management."). *But see Firemen's Ret. Sys. of St. Louis v. Sorenson (Marriott)*, No. 2019-0965-LWW, 2021 WL 4593777, at *12 (Del. Ch. Oct. 5, 2021) ("Delaware courts have not broadened a board's *Caremark* duties to include monitoring risk in the context of business decisions."); Pollman, *supra* note 58, at 2031 ("[C]ourts have drawn a line between the oversight of business risk and legal risk—the former given wide allowance and the latter

unlawful corporate activity has been ubiquitous to high-profile *Caremark* claims, whether successful or unsuccessful. The Chancery Court in *Clovis* emphasized the importance of the presence of a regulatory scheme and relevant positive law to a successful *Caremark* claim.[535]

A *Caremark* claim remains highly unlikely to survive a motion to dismiss without an allegation of underlying unlawful corporate conduct. But damages for a successful *Caremark* claim will not be limited to the direct injury from, say, an SEC enforcement action. Other monetary harm and reputational harm can also be recovered.[536] While there must be "a causal nexus between the breach of fiduciary duty and the corporate trauma,"[537] it is only the breach of fiduciary duty that must be tied to unlawful corporate conduct. The corporate trauma can and has reached much further. The claim in *Marchand* survived a motion to dismiss because food safety is heavily regulated in the United States,[538] but Blue Bell would have suffered a massive, negative fallout regardless, simply because customers will avoid a product that recently killed multiple people. The same is true for Boeing. Under Delaware Supreme Court precedent, damages for a breach of fiduciary duty are to be calculated liberally.[539] Damage models can include incidental damages such as the cost to fix the issue, reputational harm, and the cost to defend resulting lawsuits.[540]

The Chancery Court's recent decision in *Marriott*[541] would seem to undercut much of the above. Investigations by dozens of government bodies and multiple class actions on multiple theories were not enough for the court.[542] The court refused to consider pending lawsuits against Marriott in part because they were not brought against the directors

---

deemed improper."); Fairfax, *supra* note 74, at 427–28 ("[I]n . . . *Citigroup* . . . , the Delaware Supreme Court appeared to indicate that oversight liability could not be extended to board inattentiveness related to business risks.") (citing *In re Citigroup Inc. S'holder Deriv. Litig.*, 964 A.2d 106, 123 (Del. Ch. 2009)).

535. *In re Clovis Oncology, Inc. Deriv. Litig.*, No. 2017-0222-JRS, 2019 WL 4850188, at *12 (Del. Ch. Oct. 1, 2019).

536. *Id.* at *15; *Hughes v. Hu*, No. 2019-0112-JTL, 2020 WL 1987029, at *17 (Del. Ch. Apr. 27, 2020).

537. *Clovis*, 2019 WL 4850188, at *15.

538. *Marchand*, 212 A.3d at 822–23.

539. *Thorpe ex rel. Castleman v. CERBCO, Inc.*, 676 A.2d 436, 445 (Del. 1996) ("Delaware law dictates that the scope of recovery for a breach of the duty of loyalty is not to be determined narrowly.").

540. *Hughes*, 2020 WL 1987029, at *17 (citing *Thorpe*, 676 A.2d at 445).

541. *Firemen's Ret. Sys. of St. Louis v. Sorenson (Marriott)*, No. 2019-0965-LWW, 2021 WL 4593777 (Del. Ch. Oct. 5, 2021).

542. *Id.* at *1, *5.

personally.[543] The court stated that, "[s]imply listing statutes 'in vague, broad terms' without alleging what law was violated and how is insufficient to state a *Caremark* claim."[544] Perhaps the plaintiffs in *Marriott* were victims of sloppy pleading. But the approach taken by the court in *Marriott* is hard to square with *Marchand* and its progeny, and the decisions it cites do not involve *Caremark* claims. However, because *Marriott* is a Chancery Court decision, it cannot overturn *Marchand*, a Delaware Supreme Court decision. More bluntly, *Marriott* should not be relied on uncritically.

C. Existing Cybersecurity Regulatory Framework

Cybersecurity is already regulated in the United States,[545] and it is only going to become more regulated.[546] The Cyber Incident Notification Act of 2021 provides some protection from legal liability for certain companies that disclose a cyberbreach to the Department of Homeland Security Cybersecurity and Infrastructure Security Agency.[547] The carrot is paired with a stick: the proposed statutory language provides for civil penalties of up to 0.5 percent of the company's gross revenue *each day* a violation continues.[548]

The SEC has published guidance on how publicly traded companies should disclose cybersecurity risks and incidents.[549] Of particular note in

---

543. *Id.* at *18 (first citing *In re Marriott Int'l, Inc. Customer Data Security Breach Litig.*, 440 F. Supp. 3d 447, 487, 490 (D. Md. 2020); and then citing *Pfeiffer v. Toll*, 989 A.2d 683, 690 (Del. Ch. 2010)).

544. *Id.* at *14 (first quoting *Wilkin v. Narachi*, No. CV 12412, 2018 WL 1100372, at *12 (Del. Ch. Feb. 28, 2018); and then citing *Desimone v. Barrows*, 924 A.2d 908, 928 (Del. Ch. 2007)).

545. KOSSEFF, *supra* note 22, at xxiv–xxv ("[C]ybersecurity law [consists] of six broad areas of law: private sector data security laws, anti-hacking laws, public-private cybersecurity efforts, government surveillance laws, cybersecurity requirements for government contractors, [and] privacy law.") (cleaned up).

546. *See Firemen's*, 2021 WL 4593777, at *11 ("Regulators in the United States and abroad have become more active in issuing cybersecurity guidance and undertaking enforcement activities in response.") (first citing CAL. CIV. CODE §§ 1798.110, 1798.150 (West 2021); then citing Council Regulation 2016/679, 2016 O.J. (L 119) 1, General Data Protection Regulation (EU); then citing Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166, 8,166 (Feb. 26, 2018); and then citing Jared Ho, *Corporate Boards: Don't Underestimate Your Role in Data Security Oversight*, FED. TRADE COMM'N (Apr. 28, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/corporate-boards-dont-underestimate-your-role-data-security-oversight [https://perma.cc/U7TS-XPLH]).

547. *Senators Introduce Cyber Incident Notification Act*, SECURITY (July 22, 2021), https://www.securitymagazine.com/articles/95693-senators-introduce-cyberincident-notification-act [https://perma.cc/WG2L-KCXW].

548. *Id.*

549. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. at 8,166–67.

the *Caremark* context, the SEC states that the board's role in providing oversight of cybersecurity should be disclosed if cybersecurity risks are material.[550] The SEC recently announced that it had settled with First American Financial Corporation (First American) for "inadequate disclosure controls and procedural violations."[551] The First American settlement is notable both because it did not involve a cybersecurity breach, only a vulnerability, and because it was based on inadequate controls, not fraud.[552] As cyber incidents grow in scale, they are more and more likely to prove material to a company's financials and the relevance of SEC regulation will grow. Today, publicly traded companies "must disclose material cybersecurity lapses, breaches, and vulnerabilities just like they must disclose any other material corporate events."[553] The SEC announced that its 2021 regulatory agenda would include rulemaking related to cybersecurity risk disclosure.[554] Cybersecurity looks to be a major enforcement priority after SEC Chairman Gary Gensler's first one hundred days,[555] and President Biden has named it a "top priority and essential to national and economic security."[556] The SEC issued a proposed rule "to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting" in March 2022 that

550. Vivek Mohan, David Simon & Richard Rosenfeld, *SEC Increasingly Turns Focus Toward Strength of Cyber Risk Disclosures*, HARV. L. SCH. F. ON CORP. GOVERNANCE (July 25, 2021), https://corpgov.law.harvard.edu/2021/07/25/sec-increasingly-turns-focus-toward-strength-of-cyber-risk-disclosures [https://perma.cc/NP76-DYZV] (relying on Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. at 8,166).

551. William Johnson, Scott Ferber & Matthew Hanson, *SEC Returns Spotlight to Cybersecurity Disclosure Enforcement*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Aug. 1, 2021), https://corpgov.law.harvard.edu/2021/08/01/sec-returns-spotlight-to-cybersecurity-disclosure-enforcement [https://perma.cc/6WGJ-AMH4].

552. John F. Savarese, Wayne M. Carlin & Sabastian V. Niles, *A New Angle on Cybersecurity Enforcement from the SEC*, HARV. L. SCH. F. ON CORP. GOVERNANCE (June 26, 2021), https://corpgov.law.harvard.edu/2021/06/26/a-new-angle-on-cybersecurity-enforcement-from-the-sec [https://perma.cc/3ENC-76EP].

553. Johnson, Ferber & Hanson, *supra* note 551.

554. Press Release, U.S. Sec. and Exch. Comm'n Off. Of Info. And Regul. Affairs, SEC Announces Annual Regulatory Agenda, (June 11, 2021), https://www.sec.gov/news/press-release/2021-99 [https://perma.cc/T337-YHK7].

555. *See* Randall R. Lee, Julianne Landsvik & Michael Welsh, *Early SEC Enforcement Trends from Chairman Gensler's First 100 Days*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Aug. 11, 2021), https://corpgov.law.harvard.edu/2021/08/11/early-sec-enforcement-trends-from-chairman-genslers-first-100-days [https://perma.cc/G6Y7-9NNX] (identifying cybersecurity as one of five early enforcement priority areas).

556. Exec. Order No. 14,208, 86 Fed. Reg. 26,633, 26,633 (May 12, 2021).

attracted almost one hundred fifty comment letters and is expected to be finalized in late 2022.[557]

Regulated industries frequently have their own cybersecurity requirements. SEC-regulated broker-dealers and investment advisors, for example, have to follow SEC requirements in handling client data.[558] Health care providers must conform to the standards for patients' electronic health information in the HIPAA Security Rule.[559] The Federal Energy Regulatory Commission promulgated a rule in 2008 setting cybersecurity reliability standards for power companies.[560]

The Wall Street Journal reported that, "[r]ansomware is likely to remain a threat to U.S. economic and national security for years to come, the country's top military cyber official said."[561] And according to Army General Paul Nakasone, the director of the National Security Agency, "[r]ansomware attacks won't end anytime soon."[562] Ransomware payments can implicate an array of laws. Ransomware payments may violate laws setting economic sanctions.[563] Ransomware payments may also run afoul of the Patriot Act and other anti-money laundering laws and regulations.[564] Companies must comply with a patchwork of state laws setting data breach notification obligations.[565] So, while Alabama

---

557. Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16,590 (proposed Mar. 23, 2022); Galligan & Oven, *supra* note 468.

558. Johnson, Ferber & Hanson, *supra* note 551.

559. HIPAA Security Rule, 45 C.F.R. pts. 160, 164 (2021).

560. 18 C.F.R pt. 40 (2008).

561. James Rundle, *NSA Chief Says Ransomeware Threat to Remain for Years*, WALL ST. J. (Oct. 5, 2021, 2:49 PM), https://www.wsj.com/articles/nsa-chief-says-ransomware-threat-to-remain-for-years-11633459763 [https://perma.cc/J9L5-PRDD].

562. *Id.*

563. DEP'T OF THE TREASURY OFF. OF FOREIGN ASSETS, ADVISORY ON POTENTIAL SANCTION RISKS FOR FACILITATING RANSOMWARE PAYMENTS (2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf [https://perma.cc/4USR-98SF].

564. Antonia M. Apps, Adam Fee & Matthew Laroche, *What Companies Need to Know About Modern Ransomware Attacks and How to Respond*, HARV. L. SCH. F. ON CORP. GOVERNANCE. (July 14, 2021), https://corpgov.law.harvard.edu/2021/07/14/what-companies-need-to-know-about-modern-ransomware-attacks-and-how-to-respond [https://perma.cc/3ED2-U5N7]; *see also* Press Release, U.S. Dep't of The Treasury, Treasury Takes Robust Actions to Counter Ransomware, (Sept. 21, 2021) [hereinafter *Dep't of The Treasury Sept. 21, 2021 Press Release*], https://home.treasury.gov/news/press-releases/jy0364 [https://perma.cc/R6RZ-M32E] ("The United States has been a leader in applying its anti-money laundering/countering the financing of terrorism (AML/CFT) framework in the virtual currency area, including with zthe Financial Crimes Enforcement Network (FinCEN) publishing guidance regarding the application of Bank Secrecy Act rules in this area in 2013 and 2019.").

565. *See The 50 State Data Breach Notification Laws by State*, IT GOVERNANCE, https://www.itgovernanceusa.com/data-breach-notification-laws

law requires a company to notify its customers of a breach "as expeditiously as possible and without unreasonable delay,"[566] a similar Florida law requires action within thirty days,[567] and Connecticut requires action within sixty days of discovering the breach.[568] Legislators in at least four states have proposed laws banning ransomware payments.[569]

In discussing federal contractors, on October 6, 2021, "Deputy Attorney General Lisa Monaco unveiled the new policy . . . saying, 'For too long, companies have chosen silence under the mistaken belief that it's less risky to hide a breach than to bring it forward and to report it. Well, that changes today.'"[570] Ms. Monaco continues, "[w]here those who are entrusted with government dollars . . . to work on sensitive government systems fail to follow required cybersecurity standards, we're going to go after that behavior and extract very hefty [] fines."[571]

CONCLUSION

This Article makes four key arguments. First, black letter *Caremark* doctrine has not changed, but it is newly reinvigorated, and the risks of *Caremark* liability for directors is greater than it was just a few years ago. Second, future *Caremark* liability will be centered on failure to provide board-level oversight of mission critical risks. Third, cybersecurity is mission critical to effectively *all* large companies today. Fourth, the risk of *Caremark* liability can be mitigated by taking a few simple steps to ensure that the board is addressing cybersecurity. Scholars and other commentators are still in the early stages of assessing what the *Marchand* line of cases mean for *Caremark* doctrine, and cybersecurity in the *Caremark* context has been heretofore underappreciated. This Article takes valuable steps in both those areas.

[https://perma.cc/FZC8-KZ42] (last visited Sept. 19, 2021) (surveying data breach notification laws in all 50 states).

566. *See, e.g.*, ALA. CODE § 8-38-5 (2022).

567. *See, e.g.*, FLA. STAT. § 501.171. (2022)

568. *See, e.g.*, CONN. GEN. STAT. § 36a-701b (2022).

569. Cynthia Brumfield, *Four States Propose Laws to Ban Ransomware Payments*, CSO (June 28, 2021, 2:00 AM), https://www.csoonline.com/article/3622888/four-states-propose-laws-to-ban-ransomware-payments.html [https://perma.cc/PT49-DAVL].

570. James Rundle & Kim S. Nash, *U.S. Contractors Must Report Breaches*, WALL ST. J. (Oct. 7, 2021, 5:30 AM), https://www.wsj.com/articles/justice-department-to-fine-contractors-for-not-reporting-cyber-incidents-11633599001 [https://perma.cc/2U3E-SXE3].

571. *Id.* Cybersecurity regulation is also attracting international attention. *See Dep't of The Treasury Sept. 21, 2021 Press Release*, *supra* note 564. ("At the Group of Seven (G7) meeting in June, participants committed to working together to urgently address the escalating shared threat from criminal ransomware networks. The G7 is considering the risks surrounding ransomware, including potential impacts to the finance sector.").

Cybersecurity is one of many issues included under the broad rubric "ESG" (Environmental, Social, and Governance) and is typically categorized under the "G."[572] Each of the many issues under the "E," the "S," and the "G" have the potential to lead to *Caremark* liability if five factors are present: underlying law or regulation, mission critical risk, unlawful corporate conduct, large-scale negative consequences for the corporation, and conscious disregard by the directors. Examination of each is contextual and issue- and company-specific, because determining which risks are mission critical is a contextual effort. With greater attention paid to and regulation of ESG along with an invigorated *Caremark* doctrine, ESG brings greater risks for directors. Scholars are starting to take notice, with a number of other post-*Marchand* legal journal articles considering *Caremark* in the context of ESG or specific ESG issues.[573] The area remains fertile ground for future research.

572. Peter Yapp, *ESG and Cybersecurity: Governance is Key*, SCL (May 11, 2022), https://www.scl.org/articles/12579-esg-and-cybersecurity-governance-is-key [https://perma.cc/E84E-7VUY].

573. *See, e.g.*, H. Justin Pace & Lawrence J. Trautman, *Climate Change and* Caremark *Doctrine, Imperfect Together*, U. PA. J. BUS. L. (forthcoming); Strine, Smith & Steel, *supra* note 450; Cynthia A. Williams, *Fiduciary Duties and Corporate Climate Responsibility*, 74 VAND. L. REV. 1875 (2021); Bainbridge, *supra* note 100; Shapira, *supra* note 468.