THE DUTY TO MONITOR: HOW THE MISSION CRITICAL DOCTRINE IN *MARCHAND* INFORMS DIRECTOR LIABILITY FOR CYBERSECURITY BREACHES

MARY ELLEN KEMPF*

INTRODUCTION

In December of 2014, Altaba, previously known as Yahoo!, experienced one of the largest data breaches in history.[1] Hackers were able to access the personal data of hundreds of millions of users.[2] Although the Yahoo! informational security team had discovered the breach within days of the cyberattack, Yahoo! failed to properly investigate the breach and disclose it to the public until 2016, when Verizon Communications, Inc. was acquiring Yahoo!.[3] For two years, users had no knowledge that their data had been breached. Yahoo! filed several reports in the two years after the breach where it stated that it faced risks of data breaches, but it failed to disclose that one of the largest breaches in history had already happened.[4] Inhibiting the prompt and effective disclosure of cyberattacks, Yahoo! lacked the protocols necessary to properly assess and disclose breaches.[5]

Yahoo! is not the only large company that has suffered a major data breach in recent years. In 2018, Marriott discovered a security breach that exposed 387 million guest records.[6] These records included personal information such as names, addresses, and passport numbers.[7] In 2018, Facebook also discovered a major breach.[8] The breach exposed personal information such as usernames,

---

* Mary Ellen Kempf is a third-year student at Notre Dame Law School, advised by Professor Patrick Corrigan. Juris Doctor Candidate, Notre Dame Law School, 2022; Bachelor of Arts in Spanish and Political Science, Elon University, 2019. Many thanks to Professor Patrick Corrigan for his introduction to the Mission Critical Doctrine and guidance throughout the writing process. Thank you to my family and friends for their support and encouragement. All errors are my own.

1. *See* Press Release, SEC, Altaba, Formerly Known as Yahoo!, Charged with Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay $35 Million, (Apr. 24, 2018), https://www.sec.gov/news/press-release/2018-71 [hereinafter SEC Press Release].
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.*
6. Brandon Vigliarolo, *The Largest Cybersecurity Breaches of the Past Three Years, and Their Effects on Companies*, TechRepublic (May 17, 2019), https://www.techrepublic.com/article/the-largest-cybersecurity-breaches-of-the-past-three-years-and-their-effects-on-companies/.
7. *Id.*
8. *Id.*

email addresses, and the locations of online check-ins.[9] In 2017, Equifax disclosed a cybersecurity breach that compromised the social security numbers, credit card numbers, names, and addresses of customers.[10]

A cybersecurity breach can cost a company around $347 million in legal fees, penalties, and remediation costs.[11] The average stock price loss for these large companies has been around 7.5% which has taken about forty-six days to recover to the market value prior to the cyberattack.[12] These numbers indicate why cybersecurity has become a significant issue for large companies. While these statistics reflect the immediate costs of a major cyberattack, there are also long-term effects such as a loss of customer trust. A loss of trust can result in losing current customers as well as creating difficulties getting new customers.

In light of evolving cybersecurity risks, what do the fiduciary duties under state corporation laws demand of directors and officers? This Note will first provide a background on the role of fiduciary duties within a corporate structure. Part II will introduce *Caremark* claims and the developing Mission Critical Doctrine. Part III will analyze how the Mission Critical Doctrine applies to the fiduciary duties of a corporation's board of directors regarding cybersecurity issues. Finally, Part IV will discuss additional disclosure requirements for public companies subject to federal securities laws.

I. BACKGROUND

In any corporation, the stockholders elect the board of the directors to act on their behalf.[13] Often, agency problems arise when the interests of the board and the interests of the stockholders do not align.[14] Misalignment of incentives within this agency relationship can happen in a variety of situations.[15] For example, executive compensation is one area where the executives of a corporation often disagree with stockholders about what a reasonable salary might be.[16] Without any protection, the stockholders would have trouble mitigating these agency problems in situations where ownership is spread among a large, dispersed group.[17] For these reasons, the board of directors must abide by fiduciary duties.[18] These duties include both the duty of loyalty and the duty of care.[19]

---

9. *Id.*
10. *Id.*
11. *Id.*
12. *Id.*
13. Brennan Ackerman, *The Fiduciary Duties of the Board of Directors: Cybersecurity Potential Liability and Preventative Actions*, 2 WAYNE ST. U. J. BUS. L. 12, 14 (2019).
14. *Id.*
15. *Id.*
16. *Id.*
17. *Id.*
18. *Id.*
19. *See id.* at 15 ("A director's fiduciary duty of care involves exercising reasonable business judgment and using ordinary care and prudence in the fulfillment of his or her duties.").

Because the board of directors generally has discretion regarding when the corporation should initiate litigation, directors are unlikely to bring suit against themselves.[20] Instead, stockholders can enforce fiduciary duties by bringing derivative suits.[21] A derivative suit allows the stockholders to sue the board of directors on behalf of the corporation itself.[22]

Even if a derivative plaintiff can survive substantial procedural hurdles, a derivative lawsuit for a breach of the board's duty of care is unlikely to succeed these days in jurisdictions that allow exculpatory clauses.[23] In Delaware, the Delaware General Corporation Law was modified in 1986 to allow exculpatory clauses for breaches of the duty of care under Section 102(b)(7).[24] Section 102(b)(7) has reduced the amount of derivative suits brought for duty of care breaches. However, Section 102(b)(7) is limited to allowing corporations to exculpate breaches of a director's duty of care.[25] It does not allow corporations to exculpate their directors for bad faith actions or violating the duty of loyalty.[26] Even with a 102(b)(7) exculpatory clause in a corporation's foundational documents, stockholders can still bring a derivative lawsuit to enforce the board's fiduciary duty of loyalty.[27]

One particular type of derivative lawsuit that a stockholder may bring against the board for oversight liability of directors is a *Caremark* claim.[28] The facts of *Caremark* generally limited the claims to illegal actions or knowledge of illegal actions by directors.[29] Later, the caselaw developed to encompass a duty to monitor within the directors' preexisting duty of loyalty.[30]

Generally, courts defer to the board of directors when a plaintiff claims that the board breached a fiduciary duty.[31] This same deference would apply if

---

See also id. at 16 ("In general, the duty of loyalty requires directors to act in good faith to advance the best interests of the corporation and, similarly, to refrain from conduct that injures the corporation.").

20. Gerard M. Stegmaier & Courtney E. Fisher, *Caveat Director*, 38 DEL. LAW. 14 (2020).

21. *Id.*

22. *Id.*

23. Derivative suits require a few procedural hurdles. If a stockholder is suing on behalf of the corporation for harm done by the directors' actions, the stockholder "must either (1) make a pre-suit demand by presenting the allegations to the corporation's directors, requesting that they bring suit, and showing that they wrongfully refused to do so, or (2) plead facts showing that demand upon the board would have been futile." *Id.* at 15.

24. DEL. CODE. ANN. tit. 8 § 102(b)(7) (2020); John Armour et al., *Taking Compliance Seriously*, 37 YALE J. ON REGUL. 1, 42 (2020); *see* Ackerman, *supra* note 13, at 15 ("Delaware allows for an exculpatory provision to be included in a corporation's charter. This clause nearly eliminates any personal liability which directors owe to shareholders under the fiduciary duty of care. Exculpatory clauses are authorized under Section 102(b)(7) of the DGCL. If a complaint alleges only a breach of the duty of care, it can be dismissed if the directors are protected by an exculpatory clause.").

25. Ackerman, *supra* note 13, at 15.

26. *Id.*

27. *Id.*

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

29. Armour et al., *supra* note 24, at 42.

30. *Id.*

31. Ackerman, *supra* note 13, at 14.

a plaintiff brought an action against the board of directors for a breach of fiduciary duties after a cyberattack.[32] The plaintiff would have to overcome the business judgment rule in which the courts defer to decisions made by a corporation's board of directors by presuming that the directors made the business decision "on an informed basis, in good faith and in the honest belief that the action was taken in the best interests of the company."[33] This standard applies unless the plaintiff can show that the board "acted in reckless indifference or deliberate disregard of the stockholders or took actions which are outside the bounds of reason."[34] The next Part will assess a board's fiduciary duty of loyalty regarding *Caremark* claims and cybersecurity.

II. CAREMARK CLAIMS

A. Background

In order to bring a successful *Caremark* claim for a breach of the fiduciary duty of loyalty, the stockholder must show "a sustained or systematic failure of the board to exercise oversight."[35] This *Caremark* test requires that "(1) the director knew or should have known of the risk; (2) the director declined to make a good faith effort to prevent the violation; and (3) the lack of action was the proximate cause of damages."[36]

There are two avenues for the stockholder to plead a *Caremark* claim. As Gregory Watts categorizes it, the stockholder must plead either "(1) that 'directors utterly failed to implement any reporting or information system or controls' or (2) that the directors, '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.'"[37] The standard for a *Caremark* claim is higher than mere negligence. To find the directors liable, the court must find that the directors "knew of and consciously disregarded their fiduciary duties."[38] This was a difficult standard for plaintiffs to meet, so *Caremark* claims were not frequently successful shortly after *Caremark* was decided.[39] However, the standard is fact intensive, so "there is no safe harbor for a board member to avoid liability" either.[40] The fact intensive inquiry makes it difficult for a company to

32. *See id.* ("To date, no courts have found a director to have breached his or her fiduciary duties following the occurrence of a cyberattack.").

33. *Id.* at 15.

34. *Id.*

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

36. Ackerman, *supra* note 13, at 17.

37. Gregory L. Watts, *"I Got a Bad Feeling About This": Are* Caremark*'s Walls Closing in on Directors?*, A.B.A. 15 (Dec. 10, 2019), https://www.americanbar.org/groups/litigation/committees/class-actions/articles/2019/fall2019-are-caremarks-walls-closing-in-on-directors/.

38. *Id.*

39. *Id.*

40. Ackerman, *supra* note 13, at 17.

completely avoid the possibility of *Caremark* liability even if the standard is so difficult for plaintiffs to meet.

B. Prong 1

In 2019, the Delaware Supreme Court decided another key case, *Marchand v. Barnhill*.[41] In *Marchand*, the Delaware Supreme Court interpreted Prong 1, that directors utterly failed to implement any reporting or information system or controls, in a more plaintiff-friendly opinion. This case signaled a shift in *Caremark* claims.[42] *Marchand* established the Mission Critical Doctrine, expanding *Caremark* from claims about illegality to finding director liability for a lack of oversight if that oversight regarded something so central to the survival of the corporation that it is considered "mission critical."[43] In *Marchand*, Blue Bell Creamery had one product: ice cream.[44] Because this was the only source of revenue for Blue Bell, the court determined that food safety was mission critical to the business strategy.[45] When Blue Bell failed to comply with FDA regulations, resulting in a listeria outbreak, stockholders brought a derivative lawsuit against the directors of Blue Bell for the ensuing costs.[46] The court found the directors liable for a failure to oversee food safety because this was mission critical to the success of Blue Bell.[47] Even though there were monitoring systems in place at the management level, the court found the directors liable because the board of directors had neither discussed food safety nor had a system in place to report food safety issues to the board level.[48]

C. Prong 2

In another plaintiff-friendly decision, the Delaware Court of Chancery decided *In re Clovis*,[49] analyzing Prong 2—that the directors, having implemented such a system of controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention. In *In re Clovis*, the stockholders brought a lawsuit against the board of directors for breaching their fiduciary duty by misleading the market as to the efficacy of a drug in clinical trials.[50] Following this case, plaintiffs may be more equipped to plead a board's conscious failure to oversee operations and ignorance of red flags.[51]

As the range of successful *Caremark* claims continues to expand, it raises concerns in the academic community. The usual standard of business judgment

41. Marchand v. Barnhill, 212 A.3d 805 (Del. 2019).
42. Watts, *supra* note 37, at 15.
43. *Marchand*, 212 A.3d 805, 824.
44. *Id.* at 807.
45. *Id.*
46. *Id.*
47. *Id.* at 824.
48. *Id.*
49. *In re* Clovis Oncology, Inc. Derivative Litig., 2019 WL 4850188 (Del. Ch. Oct. 1, 2019).
50. *Id.*
51. Watts, *supra* note 37, at 15.

review emphasizes deference to decisionmakers in order to promote stockholder value maximization and minimize the risk that directors will pass over opportunities due to a fear of personal liability.[52] However, this goal may be overshadowed by the wider societal impacts of the decisions being made.[53] An emerging area of *Caremark* claims concerns cybersecurity and the degree of monitoring that *Caremark* may require of a board of directors.

III. CYBERSECURITY

A. Background

While *Marchand* and *In re Clovis* both widened the scope of *Caremark* claims, the facts of both cases involved Food and Drug Administration regulations regarding food safety and drug safety, respectively. The future is uncertain for *Caremark* claims regarding other areas of director oversight, including cybersecurity. Stockholder derivative suits have the potential to hold a board of directors accountable for cybersecurity breaches by bringing a lawsuit on behalf of the corporation.[54] These types of cybersecurity claims have "historically based their claims on an organization's alleged bad faith and oversight failures arising out of the duty of loyalty. This strategy can be traced back to the *Caremark* case."[55]

For companies trying to address cybersecurity risks, the facts of *Marchand* and *In re Clovis* can be helpful guideposts regarding what information a board can rely on and also to what extent and depth the board itself must understand the cybersecurity risks and protection options.[56] The court in *In re Clovis* explained that "[a]s *Marchand* makes clear, when a company operates in an environment where externally-imposed regulations govern its 'mission critical' operations, the board's oversight function must be more rigorously exercised."[57] *In re Clovis* showed that even if a system of monitoring is established, the board's failure "to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention" was enough to find *Caremark* liability in a mission critical regulatory area.[58]

Even though the facts of both *Marchand* and *In re Clovis* deal with food and drug safety, a court could consider cybersecurity to be mission critical to a corporation as well and interpret the same forms of monitoring. While there is no authoritative answer to the question of when cybersecurity is considered mission critical to a company, *Marchand* provides helpful guidance. In *Marchand*, the court found that food safety was mission critical to a monoline ice cream company.[59] Analogizing to the narrow scope of services provided by

52. Armour et al., *supra* note 24, at 44.
53. *Id.*
54. Stegmaier & Fisher, *supra* note 20, at 15.
55. *Id.* at 16.
56. *Id.* at 19.
57. *Id.* at 20.
58. *Id.* at 16.
59. Marchand v. Barnhill, 212 A.3d 805 (Del. 2019).

Blue Bell and the severity of the consequences regarding a potential food safety concern, cybersecurity could be considered mission critical for banks and other financial institutions that safeguard client's sensitive financial information. Additionally, as food safety is regulated by the FDA which enforces industry best practices, likewise banking is a heavily regulated industry which reflects the importance of protecting the clients' data. In determining if cybersecurity is mission critical, "directors should understand their company's cybersecurity risk profile, which is a combination of how likely it is a company will suffer a cyberattack combined with the severity of the consequences that may flow from an attack."[60] No action is needed if the risk of a cyber breach is negligible. Risks from a cyberattack "include the loss of customer confidence, harm to the company's reputation, impact on the stock price, potential regulatory action, potential litigation, and an interruption to the course of business."[61]

Further, the facts of *Marchand* and *In re Clovis* could inform the level of involvement required of the board in cybersecurity oversight. Courts will still review a board's actions according to the business judgment standard, but "these cases indicate that board members who passively rely on the presence of a compliance program to satisfy their oversight obligations in 'intrinsically critical' areas may face higher litigation risk."[62] The current standard is "reasonable" security, but this has been largely undefined and difficult to implement.[63] The Federal Trade Commission ("FTC") provides some guidance for which corporations may be liable for cybersecurity breaches. The FTC Act which empowers the agency has specified that corporations could be held liable for "unfair or deceptive acts or practices in or affecting commerce."[64] Unfair and deceptive practices include the failure to maintain reasonable data security regarding consumer information.[65]

Facebook failed this standard of reasonable data security in 2019 when it failed to protect user privacy.[66] As a result, the FTC fined Facebook $5 billion for data misuse, and required Facebook's corporate governance to the issue.[67] Equifax also had to pay a large settlement of $575 million due to a breach of consumer data.[68] These significant fines for data breaches ultimately harm the shareholders who bear the cost,[69] so boards of directors should be informed of possible *Caremark* claims regarding data security. While corporations should satisfy FTC-required controls at a minimum, executives are "increasingly turning to experts or committees with specific expertise to avoid liability."[70]

60. Ackerman, *supra* note 13, at 25.
61. *Id.* at 27.
62. Stegmaier & Fisher, *supra* note 20, at 20.
63. *Id.*
64. *Id.*
65. *Id.*
66. Stegmaier & Fisher, *supra* note 20, at 21.
67. *Id.*
68. *Id.*
69. *Id.*
70. *Id.*

With cybersecurity breaches becoming more common,[71] it is important for corporations to be aware of the level of monitoring that is required of a board of directors to avoid *Caremark* derivative lawsuits. *Caremark* does not require implementation of a perfect system that avoids cybersecurity breaches altogether; it just requires a certain level of effort by the board of directors to monitor cybersecurity in a good faith effort to prevent security breaches.[72]

B. Potential Caremark Liability for Cybersecurity Risks

To demonstrate how potential cybersecurity risks can create *Caremark* liability, this Note will first explain the Mission Critical framework that *Marchand* detailed. After elaborating on this foundation, this Note will then apply the framework to cybersecurity risks to examine how the liability that was related to food safety in *Marchand* applies in the cybersecurity context.

1. The Mission Critical Framework

As discussed earlier in this Note, *Caremark* claims can be difficult to plead.[73] *Marchand* and the accompanying Mission Critical Doctrine opened the door for liability if the directors breach their duty to monitor when the failure to monitor relates to an area that is "mission critical" or essential to the success of the company.[74] In *Marchand*, Chief Judge Strine found *Caremark* liability for a failure to monitor the food safety risks that led to a listeria outbreak.[75] Blue Bell Creameries was liable under a new branch of *Caremark* claims because the business only sold one product, making food safety "mission critical" to the success of the company.[76] Ferrillo et al. presented a six-prong framework for these mission critical *Caremark* claims.[77]

In a complaint, the plaintiff needs to plead facts alleging an utter failure by the board of directors to monitor risks to an essential aspect of the enterprise.[78] Among others, plaintiffs might plead one or several failures on the part of the board of directors:

Committees.[79] In *Marchand*, the board of directors had not created a committee to address food safety.[80] Because ice cream was the sole source of revenue for Blue Bell Creameries, the court found that food safety was mission critical to the success of the company.[81] To comply with fiduciary duties, the

71. *Id.*
72. *Id.*
73. *See infra* Part I.
74. Marchand v. Barnhill, 212 A.3d 805 (Del. 2019).
75. *See generally id.*
76. *Id.* at 824.
77. Paul Ferrillo et al., *Boards Should Care More About Recent "*Caremark*" Claims and Cybersecurity*, HARV. L. SCH. F. CORP. GOV. (Sept. 15, 2020), https://corpgov.law.harvard.edu/2020/09/15/boards-should-care-more-about-recent-caremark-claims-and-cybersecurity/.
78. *Id.*
79. *Id.*
80. Marchand v. Barnhill, 212 A.3d 805, 809 (Del. 2019).
81. *Id.*

board should have had a committee that specifically monitored food safety and FDA standards to protect this sole source of revenue.[82]

Processes and Protocols.[83] The board of directors in *Marchand* did not have established processes and protocols in place to inform the directors of food safety compliance reports.[84] There were no requirements for management to inform the board of the practices in place.[85] In fact, the FDA had sent multiple warnings to Blue Bell Creameries of food safety deficiencies, but these were not discussed with the board of directors.[86]

Regularity.[87] In *Marchand*, the board did not evaluate food safety risks on a regular basis.[88] The court in *Marchand* called for regularly scheduled evaluations of risks that are mission critical, such as quarterly or biannual reports.[89]

Yellow and Red Flags.[90] The management in *Marchand* had received reports that would amount to red or yellow flags before the three customer deaths occurred.[91] The court found that there should be a reporting system or requirements to disclose these reports to the board in order to keep the board informed of large threats to what is considered mission critical to the company.[92]

Full Reports.[93] In *Marchand*, the board of directors had received favorable food safety reports by management, but they did not receive information regarding the growing risks and deviations from compliance standards.[94] In the reporting mechanisms that a company may have, the board should be receiving both the favorable and unfavorable updates.[95]

Board Meetings.[96] During the board meetings in *Marchand*, the board of directors did not have regular food safety discussions.[97] In order to meet the *Caremark* duty to monitor, boards should have regularly scheduled portions of the board meetings to discuss those issues considered mission critical to the company's success.[98]

The aim of these six considerations is to show that there is consistent monitoring and reporting on those issues considered mission critical at the *board* level.[99] Where Blue Bell Creameries went wrong was relying on the

82. *Id.*
83. Ferrillo et al., *supra* note 77.
84. *Marchand*, 212 A.3d at 814.
85. *Id.*
86. *Id.*
87. Ferrillo et al., *supra* note 77.
88. *Marchand*, 212 A.3d at 817.
89. *Id.*
90. Ferrillo et al., *supra* note 77.
91. Marchand v. Barnhill, 212 A.3d 805, 811 (Del. 2019).
92. *Id.*
93. Ferrillo et al., *supra* note 77.
94. *Marchand*, 212 A.3d at 812.
95. *Id.*
96. Ferrillo et al., *supra* note 77.
97. *Marchand*, 212 A.3d at 812.
98. *Id.*
99. *Id.*

mechanisms that reported to management.[100] Even though management had access to information regarding compliance, FDA reports, and other resources, the court found liability because there was not sufficient monitoring and reporting at the board level.[101] Next, this Note will analyze how these six considerations would apply to cybersecurity in a potential *Caremark* claim.

2. Applying the Mission Critical Framework to Cybersecurity

As previously discussed, the Delaware courts have applied the Mission Critical Doctrine in *Marchand* and *In re Clovis* to issues of food and drug safety, respectively.[102] In order to apply this doctrine to cybersecurity, it is important to address the limitations that the Delaware courts have applied in the past when plaintiffs have asked the courts to expand the doctrine.

In *In re Citigroup*, the Delaware Court of Chancery specified that the Mission Critical Doctrine does not apply to business decisions to take on excessive financial risk.[103] The court found that red flags regarding the state of the subprime mortgage market and the "staggering losses" that soon followed were business decisions that were protected under the business judgment rule, and these decisions did not amount to misconduct by the board of directors.[104] A board of directors will not be liable for *Caremark* claims arising from bad business decisions and taking on too much financial risk, even if that risk threatens the very existence of the company.[105] The court is reluctant to engage in this sort of judicial second-guessing.[106]

Another hurdle that plaintiffs will have to overcome is showing that the defendant did not have an adequate reporting system in place. In *In re General Motors Co.*, the court dismissed the plaintiff's claim that the defendant's system was inadequate because General Motors had established a system to report risks.[107] The court was hesitant to second-guess a board's decision of what type of reporting system was appropriate for the corporation. In this case, the court granted the motion to dismiss, finding that a poorly managed reporting system does not imply bad faith by the directors.[108] In fact, "[s]o long as some board-level system exists, and without 'red flags' or other bases from which the court can infer knowledge on the part of the board that its system was inadequate, the complaint will be dismissed."[109] This deference will be difficult for plaintiffs

100. *Id.*
101. *Id.*
102. *See infra* Part I.
103. Elizabeth Pollman, *Corporate Oversight and Disobedience*, 72 VAND. L. REV. 2013, 2033 (2019).
104. *Id.*
105. Pollman, *supra* note 103.
106. *Id.*
107. *Id.* at 2034; In re Gen. Motors Co. Derivative Litig., No. 9627-VCG, 2015 WL 3958724 (Del. Ch. June 26, 2015), aff'd, 133 A.3d 971 (Del. 2016).
108. *Id.* at 2034; In re Gen. Motors Co. Derivative Litig., No. 9627-VCG, 2015 WL 3958724 (Del. Ch. June 26, 2015), aff'd, 133 A.3d 971 (Del. 2016).
109. Pollman, *supra* note 103 at 2034.

to overcome so long as the defendant has any type of reporting system to the board level implemented.

As both the *In re Citigroup* and *In re General Motors Co.* cases show, courts are very hesitant to second guess what is considered a business judgment by the board of directors.[110] As long as the board has "*some* system and *some* response" in place, the courts likely will not fault the board for inadequacies in the monitoring systems or for poor business choices regarding the level of financial risk the board decides to assume.[111] It seems to take a complete lack of monitoring by the board or egregious facts to overcome this deference.[112]

The cases in which a plaintiff was able to overcome a motion to dismiss pled facts that indicate a legal or compliance risk, as opposed to a business risk, that the board of directors implicated.[113] This distinction is clear in a quick comparison between *In re Citigroup* and *Marchand*. The court in *In re Citigroup* deferred to the board's decision to take on an incredible amount of financial risk that had the potential to bankrupt the corporation because these types of financial risks are decisions that are subject to the business judgment rule.[114] Under the business judgement rule, the court does not second-guess strategic business decisions made by a board of directors.[115] The court in *In re Citigroup* would not allow *Caremark* to create a backdoor around the business judgement rule.[116] However, because the category of risk that Blue Bell Creameries took on in *Marchand* was a legal or compliance risk, the court did not defer to the decision not to monitor the food safety standards.[117] In this way, the legal risk of enforcement of regulatory law is clearly distinguished from the materialization of financial risk.[118]

Another category of cases in which a plaintiff is more likely to overcome a motion to dismiss would be a case in which red flags are disclosed to the board. This would remain the same for cases of cybersecurity. If the monitoring systems that the board has put in place raise any red flags, the board must address those concerns immediately.[119] For example in the *In re Clovis* case, "the directors of a biopharmaceutical company 'did nothing' after repeatedly receiving signals from management that the company was violating the FDA's clinical trial protocol for its most promising drug under review."[120] Because the company did not have any drugs on the market, this drug trial was mission critical to the success of the company, and the board was complicit in the

110. *Id.* at 2035.
111. *Id.*
112. *Id.*
113. *Id.* at 2036.
114. *Id.* at 2037; *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 113 (Del. Ch. 2009).
115. Pollman, *supra* note 103, at 2036.
116. *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d at 113.
117. Pollman, *supra* note 103, at 2036.
118. *Id.*
119. *Id.* at 2041.
120. *Id.*

wrongdoing which allowed the case to survive a motion to dismiss.[121] To survive the motion to dismiss, the plaintiffs pled "factual allegations that suggested defendant directors not only ignored red flags, but had gone farther down a path of participation or complicity in wrongdoing."[122]

While there is no specific action that currently serves as a safe harbor, "factors that courts will consider when assessing a board's liability include organizational structure, budgetary review, board education and third-party audits."[123] Because of the emphasis on these formalities in a corporation's ability to end *Caremark* claims on a motion to dismiss, this Note will now apply the Mission Critical Framework from Ferrillo et al. to a potential cybersecurity claim.[124]

Committees.[125] If cybersecurity is mission critical for the corporation's success, then the board of directors should designate a committee to evaluate the corporation's cybersecurity risks and to create a plan to address potential cybersecurity breaches. The committee that evaluates cybersecurity is not a formalistic requirement. In *In re Home Depot*, the:

> infrastructure committee, which had managed cybersecurity, was disbanded and the audit committee, which was supposed to assume those responsibilities, had not amended its charter accordingly. The court saw past this formalism, explaining that "the [a]udit [c]ommittee received regular reports from management on the state of Home Depot's data security, and the [b]oard in turn received briefings from both management and the [a]udit [c]ommittee."[126]

As long as there is a committee that oversees cybersecurity, the court will not adhere to overly formalistic standards.[127]

Processes and Protocols.[128] The board should have an established process and protocol in place to inform the board of cybersecurity breaches and vulnerabilities. These processes should require the management to inform the board of any breaches. A court will "show deference to directors in judging the adequacy of the actions taken by them to prevent a cybersecurity breach when the corporation has a clearly defined plan and reporting chain for cyber breaches."[129] The board of directors should have discussions with those involved in this system of reporting. "Of potential safeguards, courts will show the most deference to cyber breach response plans" and even "a flawed and slowly implemented response plan may still be sufficient."[130] In determining

121. *In re* Clovis Oncology, Inc. Derivative Litig., 2019 WL 4850188 (Del. Ch. Oct. 1, 2019).
122. Pollman, *supra* note 103, at 2036.
123. Ackerman, *supra* note 13, at 13.
124. Ferrillo et al., *supra* note 77.
125. *Id.*
126. Ackerman, *supra* note 13, at 22.
127. *Id.*
128. Ferrillo et al., *supra* note 77.
129. Ackerman, *supra* note 13, at 12.
130. *Id.* at 30–31.

what the best response plan may be for a cyberattack, courts are more likely to defer to third party investigations over in-house investigations.[131]

Regularity.[132] The board should evaluate cybersecurity risks on a regular basis in quarterly or biannual reports. Additionally, the board should have a working knowledge of cybersecurity sufficient to comprehend these risks and make informed business decisions regarding the risks and exposure.[133]

Yellow and Red Flags.[134] The reporting system should require management to disclose red or yellow flags to the board in order to keep the board informed of large threats to cybersecurity that are considered mission critical to the company. The board must then respond by promptly addressing the risks or red flags that were raised. The board must not facilitate or be complicit in the wrongdoing that is reported.

Full Reports.[135] In any reporting mechanism, the board should be receiving both the favorable and unfavorable updates on breaches of cybersecurity. As to the content of the report,

> [t]he specifics of what should be reported and how much detail should be included in the reports has not been specified by the courts. According to some experts, an ideal reporting system would consist of the board receiving regular briefings from the CIO and a yearly internal report on the cybersecurity program.[136]

At a minimum, known cyber breaches should be included in the reports.

Board Meetings.[137] In order to meet the *Caremark* duty to monitor,[138] the board of directors should regularly schedule a portion of the board meetings to discuss cybersecurity. Courts have not clarified how frequently a board must discuss cybersecurity, but "dicta suggest it is necessary that cyber breaches be discussed by the full board of directors. Periodic updates to a board regarding the state of a corporation's cybersecurity framework as well as any new risks may be also required."[139] The board of directors should document discussions of cybersecurity that take place at board meetings, including the review of reports, updates from management, and other potential safeguards.[140] If none of the directors have a working knowledge of cybersecurity and modern cyberattack issues,

> a court could hold that the board is incapable of properly weighing the magnitude of risks, taking advantage of the reporting system, or putting the necessary controls in place. Thus, the board should receive some level of education on cybersecurity and should

131. *Id.* at 31.
132. Ferrillo et al., *supra* note 77.
133. Ackerman, *supra* note 13.
134. Ferrillo et al., *supra* note 77.
135. *Id.*
136. Ackerman, *supra* note 13, at 27.
137. Ferrillo et al., *supra* note 77.
138. *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 971 (Del. Ch. 1996).
139. Ackerman, *supra* note 13, at 12.
140. *Id.*

> consider appointing board members with some IT governance or cybersecurity risk experience.[141]

By implementing these six factors from Firrello et al.'s Mission Critical Framework,[142] a board of directors will have a much higher likelihood of being able to dismiss a *Caremark* claim following a cyberattack, even if cybersecurity is considered mission critical to the success of the corporation.

3. Case Studies of Courts Evaluating Cybersecurity and Caremark Liability

In order to see these claims in practice, Brennan Ackerman outlines five case studies of public companies that suffered cyberattacks, including Wyndham Hotels, Target, Wendy's, Yahoo!, and Home Depot.[143] This analysis will focus on the two derivative lawsuits that applied Delaware law to cybersecurity claims: Wyndham and Home Depot.

Wyndham's data was breached three times between April 2008 and January 2010.[144] The plaintiff's claims were dismissed "based on the board's discretion to not pursue Palkon's lawsuit, the lack of bad faith present in the board's decision, and the adequacy of the internal investigation following the shareholder demand."[145] The business judgment rule was applied to the board's decision not to bring suit, and the court found that a "fear of personal liability does not render a corporate director conflicted."[146] This case was not decided on the merits of the cybersecurity claim, but the court addressed *Caremark* claims for cybersecurity breaches in a footnote, clarifying that the plaintiff failed to show a breach of the board's duty of loyalty "because the company had installed cybersecurity measures before the first data breach, and the board had discussed the cyber breach and the risk of future breaches."[147] Directors are generally able to dismiss a shareholder demand under the business judgment rule unless "the board members either predetermined the results of the investigation in the interest of protecting themselves, or that they failed to undertake a reasonable investigation . . . ."[148] Going forward, this case study provides directors with helpful guidance. To increase the likelihood of dismissal, the board should document both the discussions leading to and the

141. *Id.* at 30.

142. Ferrillo et al., *supra* note 77.

143. Ackerman, *supra* note 13, at 13.

144. *Id.* at 18.

145. *Id.*; Palkon v. Holmes, No. 2:14-CV-01234 SRC, 2014 U.S. Dist. LEXIS 148799 (D.N.J. Oct. 20, 2014).

146. Ackerman, *supra* note 13, at 19; Palkon v. Holmes, No. 2:14-CV-01234 SRC, 2014 U.S. Dist. LEXIS 148799 (D.N.J. Oct. 20, 2014).

147. Ackerman, *supra* note 13, at 20 ("These discussion[s] and actions included the following: conducting fourteen quarterly meetings in which it discussed the cyberattacks, company security policies and proposed security enhancements; appointing the board's audit committee to investigate the breaches, with the committee meeting at least sixteen times to review cybersecurity; and hiring a technology firm to recommend security enhancements, which the company had begun to implement."); Palkon v. Holmes, No. 2:14-CV-01234 SRC, 2014 U.S. Dist. LEXIS 148799 (D.N.J. Oct. 20, 2014).

148. Ackerman, *supra* note 13, at 20.

reasoning behind the board's planned response to cyberattacks and the plans to prevent breaches. The board should establish a robust reporting system that notifies them of each breach and each investigation. Other safeguards include outside consultations, disposal of unnecessary records, and budget reviews.[149]

Home Depot was the victim of cyberattacks multiple times between April 2014 and September 2014.[150] In order to successfully show demand futility, "Delaware law . . . requires a plaintiff to show that a director's conduct is 'so egregious on its face that board approval cannot meet the test of business judgment, and a substantial likelihood of director liability therefore exists.'"[151] As previously discussed, the court did not examine Home Depot's board committee in a formalistic manner. Because the audit committee received regular data security reports and then briefed the board on these reports, the court found this was a sufficient committee even if it did not formally have those responsibilities under the company's charter.[152] Home Depot's board did not have a perfect plan, but the court found that it was sufficient, writing that "[t]he limited plan was enough to satisfy the board's duty of loyalty."[153] A company's response plan does not need to be perfect in order to protect the board of directors from claims of bad faith following a cyberattack.[154] With this limited plan, the directors were able to get the case dismissed.[155]

4. Policy Considerations

As the Delaware courts continue to grapple with new cybersecurity claims of *Caremark* liability, the policy implications of these important decisions must be considered. One area of concern is the risk-taking that a board of directors will tolerate. There are several negative implications if a board of directors becomes too risk-averse, and the business judgment rule exists to mitigate the personal liability of directors in order to allow these directors to pursue projects that maximize value for shareholders.[156] However, Ferrillo et al. question if this business judgment rule remains the best policy where "what is at stake is compliance with laws imposed on corporations to secure wider benefits for society[.]"[157]

Compliance mechanisms are not certain to prevent liability.[158] This causes firms to overspend on compliance measures that do not effectively mitigate the risks of cybersecurity breaches.[159] This practice harms shareholders and society "through poorly specified compliance programs and the opportunity cost of lack

149. *Id.* at 21.
150. *Id.*
151. *Id.* at 22; In re Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317 (N.D. Ga. 2016).
152. Ackerman, *supra* note 13, at 22.
153. *Id.*
154. *Id.*
155. *Id.*
156. Ferrillo et al., *supra* note 24, at 44.
157. *Id.*
158. *Id.*
159. *Id.*

of experimentation with new compliance technology."[160] This uncertainty stems from the standard for monitoring.[161] The plaintiffs must "demonstrate that the board had failed to ensure that their firm had *any* sort of compliance program."[162] This has restricted judicial discussions on compliance to egregious cases of the worst forms of compliance and fails to provide "any guidance on *good* practice" regarding the duty to monitor.[163]

In practice, since the *Caremark* decision, corporations have increased compliance which has resulted in more shareholder litigation being defeated earlier on at the motion to dismiss stage.[164] Even when *Caremark* was decided, the court "announced that this claim was 'possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment.'"[165] Because these claims are so difficult to get past the motion to dismiss stage, there is less caselaw to provide corporations with guidance when structuring their compliance programs.[166] For corporations looking to minimize litigation and cybersecurity risks, there are still plenty of murky areas yet to be defined by the courts. This can result in the risk-averse corporations taking too many precautions and investing too many resources into compliance programs, and other corporations investing too little and exposing themselves to liability.

IV. PUBLIC COMPANIES

A. Background

For public companies that are subject to securities laws, the regulations and requirements from the Securities and Exchange Commission ("SEC") are often more stringent than any *Caremark* duties. In contrast to the complete failure to monitor that is required for a *Caremark* claim, the SEC imposes an affirmative duty on public companies to establish monitoring systems and maintain records for disclosures.[167] Because so many companies that are building cybersecurity compliance programs are Exchange Act reporting companies, this Note analyzes several of the SEC disclosure requirements that can apply to cybersecurity issues. For companies that fall outside the scope of federal securities laws, *Caremark* fills that gap as it applies to all companies incorporated in Delaware.

In 2011, the Division of Corporation Finance at the SEC issued guidance for public companies developing compliance programs to meet the SEC's

160. *Id.*
161. *Id.* at 47.
162. *Id.*
163. *Id.*
164. Pollman, *supra* note 103, at 2032.
165. *Id.* at 2036.
166. *Id.*
167. Press Release Nos. 33-10459; 34-82746, SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, at 5 (Feb. 26, 2018) https://www.sec.gov/rules/interp/2018/33-10459.pdf [hereinafter SEC Guidance].

disclosure obligations for cybersecurity risks and breaches.[168] This guidance clarifies that although the SEC has not established any requirements toward cybersecurity specifically, the SEC may still require companies to disclose cybersecurity risks and breaches.[169] After this guidance in 2011, many companies established disclosure protocols for cybersecurity breaches that were based on a system of risk factors.[170] In annual reports filed in 2012, about 88% of public Fortune 500 companies and about 78% of Fortune 501–1000 companies included cybersecurity risk factor disclosure.[171]

The SEC's approach to cybersecurity regulation has focused on a mandatory disclosure regime.[172] The SEC published guidance in 2018 to assist public companies by further clarifying the disclosure requirements for cybersecurity risks and breaches.[173] Because of the costs associated with a cybersecurity breach as well as the frequency of these breaches, the SEC requires public companies to disclose all material risks as well as all breaches of cybersecurity in a timely fashion.[174] The guidance from 2018 is clear that public companies "must disclose in a timely fashion those cybersecurity risks and incidents that are material to investors."[175] This guidance is directed toward companies that have already experienced a breach, as well as companies that have material risks but have not yet experienced a breach.[176]

Rebecca Rabinowitz critiques the 2018 guidance as merely repetitive of the 2011 guidance from the SEC's Division of Corporation Finance.[177] After receiving this guidance from the Division of Corporation Finance and from the SEC, companies may still require more specific guidance in order to build effective cybersecurity compliance programs. In particular, Rabinowitz calls for more explanation regarding when a breach of cybersecurity is material and needs to be disclosed, as well as when those disclosures are considered timely.[178]

The SEC requires timely disclosures of risks and breaches.[179] In order to comply with this timeframe, companies need to have disclosure controls and procedures in place before these risks and breaches arise.[180] The procedures should "provide an appropriate method of discerning the impact that such matters may have on the company and its business, financial condition, and results of operations, as well as a protocol to determine the potential materiality

168. *Id.*
169. *Id.* at 5–6.
170. *Id.* at 6.
171. *Id.* at 6, n.12.
172. Rebecca Rabinowitz, Note, *From Securities to Cybersecurity: The SEC Zeroes in on Cybersecurity*, 61 B.C. L. REV. 1535, 1574 (2020).
173. SEC Guidance, *supra* note 167, at 1.
174. *Id.* at 4.
175. Rabinowitz, *supra* note 172, at 1574.
176. SEC Guidance, *supra* note 167, at 4.
177. Rabinowitz, *supra* note 172, at 1574.
178. *Id.* at 1575.
179. SEC Guidance, *supra* note 167, at 4.
180. *Id.*

of such risks and incidents."[181] In order to meet the disclosure obligations under federal securities laws, it is important for companies to maintain comprehensive procedures and disclosure controls.[182] These procedures must enable the company to make timely disclosures of all material events, including events related to risks and breaches of cybersecurity.[183] The SEC describes a variety of ways that a company can make these disclosures in its 2018 Guidance pertaining to cybersecurity disclosure requirements.

B. 2018 Guidance from the SEC

Regulation S-K and Regulation S-X have several disclosure requirements. These requirements do not refer to cybersecurity risks and breaches in particular, but in order to meet the disclosure requirements, companies should disclose any known risks and breaches of cybersecurity.[184] Public companies are required to file periodic reports which make disclosures on a regular and ongoing basis.[185] The Form 10-K is one type of periodic report that requires annual disclosures regarding material cybersecurity risks and breaches.[186] If a public company is aware of a material cybersecurity risk or breach, these periodic disclosure obligations can be triggered.[187]

Public companies must also disclose cybersecurity risks and breaches in the Securities Act and Exchange Act registration statements.[188] These statements require the disclosure of all material facts that are "necessary to make the statements therein not misleading."[189] If failing to mention a material cybersecurity risk or breach would make these statements misleading, then the public company must disclose that risk or breach.[190] An omission is material "if there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that disclosure of the omitted information would have been viewed by the reasonable investor as having significantly altered the total mix of information available."[191] To apply this materiality standard to cybersecurity risks and breaches,

> companies generally weigh, among other things, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company's operations. The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any

181. *Id.*
182. *Id.*
183. *Id.* at 6–7.
184. *Id.* at 8.
185. *Id.*
186. *Id.*
187. SEC Guidance, *supra* note 167, at 9.
188. *Id.*
189. *Id.*
190. *Id.*
191. *Id.* at 10; *see also* TSC Indus. v. Northway, 426 U.S. 438, 449 (1976).

> compromised information or the business and scope of company operations. The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause. This includes harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities.[192]

In weighing these factors, companies look to the sensitivity of the information that is exposed and the ramifications of the potential breach.[193] The ramifications may depend on the scope of the breach or on the potential harm that could be caused based on the type of information that is accessed by the hackers.[194]

Companies must "maintain the accuracy and completeness of effective shelf registration statements with respect to the costs and other consequences of material cybersecurity incidents."[195] In order to maintain this accuracy, public companies can update information using a Form 8-K or Form 6-K to disclose the occurrence and ongoing consequences of a breach of cybersecurity.[196] Even if a company made a prior disclosure, the company still has a duty to correct any information that the company later determines was untrue at the time it was previously disclosed.[197] If the company later learns contradictory information that existed at the time of the initial disclosure, the company must disclose.[198] The company also has a duty to update if the previous disclosure becomes materially inaccurate after the initial disclosure.[199] For these reasons, public companies should assess the need to correct or update previous disclosures while they are investigating a breach of cybersecurity.[200]

Item 503(c) of Regulation S-K and Item 3.D of Form 20-F require a public company to disclose factors that make an investment in the company's securities "speculative or risky."[201] In making that disclosure, companies should consider the following cybersecurity risk factors:

> the occurrence of prior cybersecurity incidents, including their severity and frequency; the probability of the occurrence and potential magnitude of cybersecurity incidents; the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity

192. SEC Guidance, *supra* note 167, at 10–11.
193. *Id.*
194. *Id.*
195. SEC Guidance, *supra* note 167, at 9.
196. *Id.*
197. *Id.*
198. *Id.* at 12.
199. *Id.*
200. *Id.*
201. *Id.* at 13.

> risks; the aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third party supplier and service provider risks; the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers; the potential for reputational harm; existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies; and litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.[202]

In addition to the disclosures required by Item 503(c) of Regulation S-K and Item 3.D of Form 20-F, Item 303 of Regulation S-K and Item 5 of Form 20-F require financial disclosures that can be triggered by the "the cost of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents."[203] Large data security breaches can cost a company around $347 million in legal fees, penalties, and remediation costs.[204]

The 2018 guidance emphasizes that disclosure obligations do not require a company to give hackers a roadmap of the security system protecting the company's data, but still require the company to give more than a generic, boilerplate disclosure of risk.[205] The SEC does not require public companies to "disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident."[206] If companies were required to publicly disclose this information, then future hackers may be able to use the information to more easily breach the security system.[207] In disclosing the risks of a cybersecurity breach, the company should address material risks and breaches specific to that company in particular, including potential financial, legal, and reputational ramifications of a breach.[208] Additionally, the 2018 guidance suggests that while the SEC will provide flexibility as to the timing of the disclosure to allow the company to assess the impact of a breach or assist law enforcement, a

---

202. *Id.* at 13–14.

203. *Id.* at 15. ("Item 303 of Regulation S-K and Item 5 of Form 20-F require a company to discuss its financial condition, changes in financial condition, and results of operations. These items require a discussion of events, trends, or uncertainties that are reasonably likely to have a material effect on its results of operations, liquidity, or financial condition, or that would cause reported financial information not to be necessarily indicative of future operating results or financial condition and such other information that the company believes to be necessary to an understanding of its financial condition, changes in financial condition, and results of operations.")

204. Vigliarolo, *supra* note 7.

205. SEC Guidance, *supra* note 167, at 11.

206. *Id.*

207. *Id.*

208. *Id.*

lengthy, ongoing, internal or external investigation will not enable a company to avoid making a public disclosure of a material cybersecurity breach.[209]

The 2018 guidance indicates that the best disclosure controls and procedures "identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents."[210] It is important that these procedures can assess breaches promptly in order to meet the various disclosure requirements the SEC has established in a timely fashion.[211]

C. Applying the 2018 Guidance from the SEC: Altaba

The case against Altaba, previously known as Yahoo!, as previously mentioned resulted in a $35 million penalty from the SEC for misleading investors by failing to disclose the data breach that occurred in 2014.[212] The cyberattack compromised the personal data of hundreds of millions of users.[213] Yahoo! failed to disclose this cyberattack to the public until 2016 when an acquisition by Verizon Communications, Inc. began.[214] While the 2018 Guidance from the SEC was released a few years after Yahoo!'s cybersecurity breach, this 2018 Guidance can inform other companies on the SEC's disclosure expectations. When looking at the facts of the cyberattack against Yahoo! and the company's response, it is clear from the 2018 Guidance that Yahoo! failed to comply with the SEC disclosure regime.

A few days after the cyberattack occurred, Yahoo!'s information security team learned that Russian hackers had stolen the personal data of hundreds of millions of Yahoo! users.[215] This information was then reported to the senior management and legal department at Yahoo!, but the company failed to investigate the breach and failed to disclose the breach to investors until more than two years later during the acquisition of Yahoo! by Verizon Communications, Inc.[216] The SEC considered this cyberattack to be material, and Yahoo!'s failure to disclose the attack to the public for more than two years was untimely, resulting in the $35 million penalty.[217] Steven Peikin, Co-Director of the SEC Enforcement Division, commented on this cyberattack against and failed disclosure by Yahoo!, stating "[w]e do not second-guess good faith exercises of judgment about cyber-incident disclosure. But we have also cautioned that a company's response to such an event could be so lacking

209. *Id.* at 12.
210. *Id.* at 20.
211. *Id.*
212. *See supra* text accompanying notes 1–5; *see also* SEC Press Release, *supra* note 1, at 1.
213. *Id.*
214. *Id.*
215. *Id.*
216. *Id.*
217. *Id.*

that an enforcement action would be warranted. This is clearly such a case."[218] Yahoo!'s response was so lacking that the SEC had to issue a monetary penalty.[219] The incident itself was clearly material considering the scale of the cyberattack and the sensitivity of the data.[220] Additionally, Yahoo!'s response was clearly "lacking" by failing to disclose to the public for over two years.[221]

Leading to this problem, Yahoo! did not have sufficient controls and procedures in place that were capable of assessing its disclosure obligations regarding cyberattacks.[222] It is essential for large companies to have procedures established that ensure disclosure of material cybersecurity information to investors. According to the SEC's order,[223] Yahoo! had filed several periodic reports during the two-year period that followed the breach, and Yahoo! failed to disclose the breach in any of those reports.[224] Yahoo! also did not disclose the potential business and legal implications following the cyberattack.[225] In its periodic reports, Yahoo! only mentioned "the risk of" cybersecurity breaches.[226] Yahoo! failed to consult its auditors or outside counsel about the cyberattack and its disclosure obligations in public filings.[227] This lack of established procedure resulted in nondisclosure and a hefty fine.

CONCLUSION

Plaintiffs can bring a *Caremark* claim against a board of directors for having utterly failed to implement any reporting system or if there is a reporting system and the directors have consciously failed to monitor or oversee its operations. After *Marchand* and *In re Clovis*, plaintiffs have been more successful bringing these claims. After *Marchand*, "plaintiffs may find it easier to plead a board's utter failure to implement reporting systems under the first prong," and after *In re Clovis*, "plaintiffs may find it easier to plead a board's conscious failure of oversight and willful ignorance of red flags under the second prong."[228]

As cyberattacks become more frequent, it is important for companies to establish effective procedures for addressing these breaches. For corporations looking to assess their risk of liability and create compliance processes to shield this potential liability, there are a few important takeaways from prior court decisions regarding *Caremark* liability. If cybersecurity is deemed mission critical for a company, the board of directors would be wise to evaluate its cybersecurity framework by creating a board committee, processes and

218. *Id.*
219. *Id.*
220. *Id.*
221. *Id.*
222. SEC Press Release, *supra* note 1, at 2.
223. *Id.*
224. *Id.*
225. *Id.*
226. *Id.*
227. *Id.*
228. Watts, *supra* note 37, at 15.

protocols, regular evaluations of risk, systems to report red flags, full reports to the board, and a designated portion of time at board meetings to discuss cyber security.

Even without extensive caselaw developed in the area of cybersecurity and fiduciary duties, case studies can inform what is required for a board to meet its duty of loyalty. From these examples, it will help a board to "discuss relevant risks, implement a reporting system whereby it is informed of important cybersecurity developments, and put in place internal controls." [229] The board should focus its planning energy on both mitigating the risks of a cyberattack and implementing safeguards, while also creating plans and procedures to effectively respond to a cyberattack. The plaintiff in these actions still has a difficult standard of proof to meet to demonstrate that the board's duty of loyalty has been violated. In *In re Home Depot*, the plaintiff could not show that the board violated its duty of loyalty, despite the limited actions that the board of directors took to prevent a cyberattack.[230]

While these duties under *Caremark* apply to all companies incorporated under Delaware law, the Exchange Act reporting companies are subject to even more stringent requirements regarding cybersecurity. According to the 2018 Guidance from the SEC, these companies must disclose any material risk or incident relating to cybersecurity in a timely fashion.

As the courts continue to develop caselaw regarding cybersecurity risks and *Caremark* liability, there are important interests to balance. As with many other compliance regimes, the government does not want companies to be spending excessive corporate resources on compliance programs because the directors fear personal liability for the business decisions of the board. However, the Delaware courts aim to balance these concerns with the goal of *Caremark* which is to "encourage boards to engage with their executives about their firms' compliance activities."[231] There must be a balance between incentivizing companies to establish effective compliance regimes and avoiding the unnecessary expenditure of corporate resources on too much compliance.

229. Ackerman, *supra* note 13, at 32.

230. *Id.*

231. Firrello et al., *supra* note 24, at 39.