Georgia Law Review

Volume 53 | Number 2 Article 8

2019

What the Hack?! Reexamining the Duty of Oversight in an Age of Data Breaches

Amanda M. Payne
University of Georgia School of Law

WHAT THE HACK?! REEXAMINING THE DUTY OF OVERSIGHT IN AN AGE OF DATA BREACHES

Amanda Marie Payne[*]

Due to the proliferation of electronic data and advancements in technology, data breaches have become commonplace. Data breaches are a threat to corporations of all sizes and can have devastating impacts. Focusing solely on Delaware law, this Note explores how doctrines such as the business judgment rule, exculpation provisions, and heightened pleading standards have left shareholders with limited recourse in holding directors liable for the catastrophic consequences of data breaches. Recognizing that shareholders have been unsuccessful alleging Caremark-type claims arising out of a data breach, this Note argues that the expansion of bad faith in Walt Disney provides alternative ground for shareholders to hold directors liable for data breaches. Nevertheless, this Note concedes that courts will be unlikely to accept that argument. Courts are too wary of opening the floodgates of director liability. Therefore, this Note argues that there are certain risks—such as cybersecurity risks—to which Caremark can be extended without eviscerating the business judgment rule. This Note finally argues that where Caremark applies, the standard should be relaxed in the context of cybersecurity. In an age of data breaches, the time has come for the Caremark standard to have some teeth.

---

[*] J.D. Candidate, University of Georgia School of Law, 2019; B.S., International Affairs and Spanish, Florida State University, 2015. I wish to thank Professor Christopher M. Bruner, Stembler Family Distinguished Professor in Business Law, for his guidance in framing and articulating this Note. I would also like to thank my family for their endless support and the editors of the *Georgia Law Review* for their revisions.

TABLE OF CONTENTS

I. INTRODUCTION

Hardly a day goes by without a news report or headline highlighting another cybersecurity incident or corporate hacking. In fact, since 2005, over 8,000 data breaches have been made public in the United States alone.[1] There were about 12 million records exposed in 791 different data breaches within just the first six months of 2017.[2] While the sheer volume of data breaches is alarming, they have recently become a common occurrence due to the proliferation of electronic data and advancements in technology.[3]

Data breaches and cyberattacks are threats to corporations of "all shapes, sizes, locations, and industries."[4] Cyberattacks are a threat to essentially any business using the Internet as a means of holding "intellectual property, competitive trade secrets, customer information, and other corporate data."[5] For example, Target experienced a data breach in 2013 in which hackers stole the debit and credit card data of approximately 70 million customers.[6] In May 2014, hackers stole the personal information of up to 145 million active eBay users.[7] Just a few months later in August 2014, JPMorgan Chase announced that hackers gained access to the data of 76 million households and 7 million small businesses, including credit card numbers, bank accounts, and social security numbers.[8] Not even a week after the JPMorgan Chase breach, Home Depot announced that it had also experienced a data breach resulting in

---

[1] Privacy Rights Clearinghouse, Data Breaches, https://www.privacyrights.org/data-breaches (last visited Oct. 10, 2017).

[2] Herb Weisbaum, *Data Breaches Happening at Record Pace, Report Finds,* NBC NEWS (July 24, 2017, 10:18 AM), https://www.nbcnews.com/business/consumer/data-breaches-happening-record-pace-report-finds-n785881.

[3] *See* Nate Lord, *The History of Data Breaches*, DIGITAL GUARDIAN (Apr. 6, 2018), https://digitalguardian.com/blog/history-data-breaches (providing a history of data breaches).

[4] Thad A. Davis et al., *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2015 COLUM. BUS. L. REV. 613, 628 (2015).

[5] Norah C. Avellan, *The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America*, 54 WASHBURN L.J. 193, 194 (2014).

[6] Shayna Posses, *Target Execs Escape Derivative Claims Over Data Breach*, LAW360 (July 7, 2016), https://www.law360.com/articles/815012/target-execs-escape-derivative-claims-over-data-breach.

[7] Keith Collins, *A Quick Guide to the Worst Corporate Hack Attacks*, BLOOMBERG (updated Mar. 18, 2015), https://www.bloomberg.com/graphics/2014-data-breaches.

[8] *Id*.

56 million stolen payment cards and 53 million pilfered e-mail addresses.[9] Other notable data breaches include: Sony in 2011; LinkedIn, Living Social, and Tumblr in 2012; Yahoo, Adobe, and Apple in 2013; UPS and Twitter in 2014; Deep Root Analytics, MySpace, and health insurance company Anthem in 2015; the U.S. Securities and Exchange Commission in 2016; and InterContinental Hotels Group, Verizon, River City Media, Snapchat, and most notably, Equifax Inc. in 2017.[10]

Well-publicized data breaches can have devastating impacts on businesses. In its *2017 Cost of Data Breach Study: Global Overview,* the Ponemon Institute estimated that the average total cost of a data breach for a company is $3.62 million dollars, with an average cost of $141 for each lost or stolen record that contains sensitive or confidential information.[11] Aside from costs incurred in investigating, notifying, and responding to data breaches, companies also indirectly incur significant reputational costs due to negative publicity, impending litigation, and a lack of shareholder and consumer loyalty and trust.[12] As a result, companies' profits and relationships with investors and other third parties are often negatively affected by data breaches.

The last decade has witnessed an uptick in government responses to data breaches. For example, the Securities and Exchange Commission, the Department of Justice, the Department of Homeland Security, the Federal Trade Commission, the Federal Communications Commission, the Financial Industry Regulatory Authority, and the Consumer Financial Protection Bureau, among

---

[9] *Id.*

[10] *Id.*; Selena Larson, *Every Single Yahoo Account Was Hacked - 3 Billion in All*, CNN (Oct. 4, 2017, 6:36 AM), http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html.

[11] PONEMON INSTITUTE, 2017 COST OF DATA BREACH STUDY: GLOBAL OVERVIEW (2017), https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN.

[12] *See* Victoria C. Wong, *Cybersecurity, Risk Management, and How Boards Can Effectively Fulfill Their Monitoring Role*, 15 U.C. DAVIS BUS. L.J. 201, 213–14 (2015) (describing consumer reactions to data breaches); Avellan, *supra* note 5, at 194 ("To date, American companies have lost trillions of dollars to cyber-attacks. Beyond the losses immediately associated with a data breach, corporations also lose tremendous value through the negative publicity and impending litigation that follows an attack."); VANTIV, *The Scary Side Effects of a Cyber Breach,* https://www.vantiv.com/vantage-point/safer-payments/data-breach-side-effects (last visited Dec. 22, 2018) (explaining that the side effects of a cyber breach include diminished reputation, decreased competitive ability, lost customer trust, and reduced revenue).

others, have begun to make cybersecurity a priority.[13] Nevertheless, Congress remains "hesitant to pass legislation requiring the whole private sector to adopt certain cybersecurity standards and best practices."[14] Indeed, the United States does not have a general data-security statute.[15]

Some states have stepped in to fill this regulatory void. In 2017, for example, the New York Department of Financial Services (DFS) enacted a cybersecurity regulation that requires "banks, insurance companies, and other financial services institutions regulated by DFS" to have a cybersecurity program, written cybersecurity policies, a Chief Information Security Officer, and various controls and plans in place to ensure data safety.[16] Additionally, "nearly all states have enacted so-called 'data breach notification laws.'"[17] For example, Delaware recently amended its data breach notification law in August 2017.[18] Delaware's law, like the notification laws of other states, "requires companies to notify affected Delaware residents of a breach involving their personal information within 60 days . . . after determination of a breach" and "to provide a year of free credit monitoring."[19]

With respect to public corporations, cybersecurity regulations are lacking. In October 2011, the Securities and Exchange Commission

---

[13] Davis et al., *supra* note 4, at 618.

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

[15] *See* Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 COMPETITION: J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL. 229, 230 (2015) ("[T]here is no general data-security statute in the United States. Although some federal statutes . . . address data security in specific industries (health care and financial services, respectively) and most states have data-breach notification laws (which are expanding in scope), most data-breach lawsuits begin in state court, alleging causes of action under state common law.").

[16] Press Release, N.Y. Dep't of Fin. Servs., DFS Cybersecurity Regulation Compliance Requirements Are Effective Today (Aug. 28, 2017) (on file with author).

[17] Matthew George, *How Viable Is the Prospect of Enforcement of Privacy Rights in the Age of Big Data? An Overview of Trends and Developments in Consumer Privacy Class Actions*, 24 J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL. 195, 201 (2015).

[18] *See* Marcus A. Christian et al., *Delaware Amends Its Data Breach Notification Law*, MAYER BROWN (Aug. 29, 2017), https://www.mayerbrown.com/delaware-amends-its-data-breach-notification-law-08-29-2017 (providing an overview of the change in Delaware's data breach notification law).

[19] *Id*.

issued cybersecurity guidance for companies.[20] This guidance is unfortunately non-binding.[21] However, the Commission believes that the "disclosure requirements may impose an obligation on registrants to disclose such risks and incidents."[22] The guidance recommends that corporations consider the following six disclosure obligations when deciding whether to disclose a data breach: (1) risk factors; (2) management's discussion and analysis of financial condition and results of operations (MD&A); (3) description of business; (4) legal proceedings; (5) financial statement disclosures; and (6) disclosure controls and procedures.[23]

In February 2018, the Commission reinforced and expanded upon the October 2011 guidance by providing an interpretive release outlining its "views with respect to cybersecurity disclosure requirements under the federal securities laws as they apply to public operating companies." [24] The release addresses the following: "(1) the materiality of a cybersecurity risk or incident, (2) the timing of disclosures relating to a cybersecurity incident, (3) disclosures about board oversight, (4) insider trading, (5) cybersecurity policies and procedures, (6) cybersecurity assessments, (7) acquisitions, and (8) regulatory and litigation risk."[25] The release makes clear that the Commission "*expect[s]* companies to disclose cybersecurity risks and incidents that are *material* to investors, including the concomitant financial, legal, or reputational consequences."[26] Furthermore, where a company has become aware of a material cybersecurity incident, the Commission "*expect[s]* it to make appropriate disclosure timely and sufficiently prior to the offer and sale of securities."[27]

---

[20] SEC. & EXCH. COMM'N, CF DISCLOSURE GUIDANCE: TOPIC NO. 2 (2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] SEC. & EXCH. COMM'N, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Exchange Act Release No. 34-82746, 2018 WL 993646 (Feb. 21, 2018) [hereinafter SEC Feb. 2018 Release].

[25] Seth Traxler et al., *Key Takeaways from the SEC's 2018 Cybersecurity Guidance*, KIRKLAND & ELLIS (Feb. 28, 2018), https://www.kirkland.com/siteFiles/Publications/Key_Takeaways_from_the_SEC%27s_2018_Cybersecurity_Guidance.pdf.

[26] SEC Feb. 2018 Release, *supra* note 24 (emphasis added).

[27] *Id.* (emphasis added).

Following the February 2018 release, the Commission settled for the first time a case involving charges for failure to disclose a cybersecurity incident. On April 24, 2018, the Commission "announced that the entity formerly known as Yahoo! Inc. has agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose one of the world's largest data breaches in which hackers stole personal data relating to hundreds of millions of user accounts."[28] Consistent with the February 2018 release, this settlement makes clear that cybersecurity related disclosure is a Commission priority. Nevertheless, neither the Commission's October 2011 guidance nor the Commission's February 2018 release imposes a blanket duty to disclose a data breach.[29] Additionally, there is currently no federal law penalizing a board for failing to implement cybersecurity measures.[30]

To hold a corporation's board of directors accountable for data breaches, shareholders must thus turn to corporate law. In corporate law, there are two bedrock fiduciary duties: the duty of care and the duty of loyalty.[31] The duty of care requires that directors "inform themselves, prior to making a business decision, of all material information reasonably available to them."[32] The essence of a plaintiff's duty of care claim is that the defendants failed to keep themselves reasonably informed when making decisions on behalf of the corporation, and such "dereliction caused a monetary loss to the corporation."[33] On the other hand, the duty

---

[28] Press Release, Sec. & Exch. Comm'n, 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; *see also In re* Altaba Inc., Exchange Act Release No. 83096, 2018 WL 1919547 (Apr. 24, 2018) (order instituting cease-and-desist proceedings).

[29] *See* Sam Young, *Contemplating Corporate Disclosure Obligations Arising from Cybersecurity Breaches*, 38 J. CORP. L. 659, 668–69 (2013) (noting that the SEC guidance does not require disclosure).

[30] *See* Harris Yegelwel, *Cybersecurity Oversight: A Cautionary Tale for Directors*, 20 J. TECH. L. & POL'Y 229, 254–55 (2015) (explaining that a board should not be relieved from potential liability when it suffers a data breach despite the lack of a federal law penalizing a board for its failure to implement cybersecurity measures).

[31] *See* Jack B. Jacobs, *Fifty Years of Corporate Law Evolution: A Delaware Judge's Retrospective*, 5 HARV. BUS. L. REV. 141, 145 (2015) (describing the fiduciary duties of corporate directors).

[32] Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984).

[33] Mark J. Loewenstein, *Shareholder Derivative Litigation and Corporate Governance*, 24 DEL. J. CORP. L. 1, 4 (1999).

of loyalty requires directors to act in good faith and in a manner they reasonably believe to be in the best interest of the corporation and its shareholders.[34]

Data breaches implicate the board's duty of oversight, which is also referred to as the duty to monitor.[35] Although this Note will use those terms interchangeably, it will primarily refer to it as the duty of oversight because "Delaware case law most often describes the duty as oversight."[36] The Delaware Chancery Court originally recognized the duty of oversight as a subset of the duty of care in *In re Caremark International*, *Inc. Derivative Litigation*.[37] However, the Delaware Supreme Court later recategorized *Caremark* as a case about the directors' duty to act in good faith, which is a subset of the duty of loyalty, not the duty of care.[38] As a result, the duty of oversight is now recognized as a subset of the duty of loyalty under Delaware corporate law.[39] This recategorization is significant in light of Delaware's director exculpation statute, which allows a corporation to limit or eliminate director liability for duty of care violations but not for duty of loyalty violations.[40] Therefore, directors can be held monetarily liable for violations of the duty of oversight.

Nevertheless, as Chancellor Allen stated in *Caremark*, a suit alleging a breach of the duty of loyalty arising from a director's failure to exercise oversight over the company, often referred to as a *Caremark* claim, is "possibly the most difficult theory in

---

[34] *See* Jacobs, *supra* note 31, at 145; Guttman v. Huang, 823 A.2d 492, 506 n.34 (Del. Ch. 2003) ("A director cannot act loyally towards the corporation unless she acts in the good faith belief that her actions are in the corporation's best interest.").

[35] Lisa M. Fairfax, *Managing Expectations: Does the Directors' Duty to Monitor Promise More than It Can Deliver?*, 10 U. ST. THOMAS L.J. 416, 416 n. 1 (2012).

[36] *Id*.

[37] *In re* Caremark Int'l, Inc. Derivative Litig., 698 A.2d 959, 961 (Del. Ch. 1996).

[38] *See* Claire A. Hill & Brett H. McDonnell, *Reconsidering Board Oversight Duties After the Financial Crisis*, 2013 U. ILL. L. REV. 859, 861 (2013) (citing Stone v. Ritter, 911 A.2d 362, 373 (Del. 2006)).

[39] *Id.*

[40] DEL. CODE ANN. tit. 8, § 102(b)(7) (2015) ("A provision eliminating or limiting the personal liability of a director to the corporation or its stockholders for monetary damages for breach of fiduciary duty as a director, provided that such provision shall not eliminate or limit the liability of a director: (i) For any breach of the director's duty of loyalty to the corporation or its stockholders; (ii) for acts or omissions not in good faith or which involve intentional misconduct or a knowing violation of law; (iii) under § 174 of this title; or (iv) for any transaction from which the director derived an improper personal benefit.").

corporation law upon which a plaintiff might hope to win a judgment."[41] The *Caremark* standard created a remarkably high hurdle for plaintiff–shareholders; they essentially must prove that the board acted with the intent to inflict harm upon the corporation or that the board did absolutely nothing, despite knowing they needed to do something.[42] Therefore, in reality, the duty of oversight is largely theoretical and fails to provide shareholders with an effective means of holding directors and officers accountable for data breaches.

Making such claims even more difficult, Delaware courts have yet to clearly hold that the duty of oversight extends beyond legal compliance.[43] This is largely due to the fact that a typical *Caremark* claim argues that "defendants are liable for damages that arise from a failure to properly monitor or oversee employee misconduct or violations of law."[44] A case from the Delaware Chancery Court, *In re Citigroup, Inc. Shareholder Derivative Litigation*, comes closest to addressing the issue of extending the duty of oversight to business risks.[45] In *Citigroup*, Chancellor Chandler illustrated the substantive limits of the duty of oversight by stating that the duty to monitor business risks is fundamentally different from the duty to monitor corporate activities for fraud or illegal conduct.[46] By drawing a line between business and legal risks, Chancellor Chandler essentially limited the ability of shareholders to hold

---

[41] *Caremark*, 698 A.2d at 967.

[42] *Caremark* articulated the following 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. In either case, imposition of liability requires a showing that the directors knew that they were not discharging their fiduciary obligations. Where directors fail to act in the face of a known duty to act, thereby demonstrating a conscious disregard for their responsibilities, they breach their duty of loyalty by failing to discharge that fiduciary obligation in good faith.

Stone, 911 A.2d at 370 (citations omitted).

[43] *See* Hill & McDonnell, *supra* note 38, at 862.

[44] *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 123 (Del. Ch. 2009).

[45] *See id.* at 123 (noting that plaintiff's theory was a twist on the traditional Caremark claim).

[46] *Id.* at 131 ("While it may be tempting to say that directors have the same duties to monitor and oversee business risk, imposing *Caremark*-type duties on directors to monitor business risk is fundamentally different.").

directors and officers liable for violating the duty of oversight to only legal risks.

In light of the growing number of data breaches, this Note seeks to reexamine the duty of oversight and its substantive limitations. Focusing solely on Delaware law, this Note explores how doctrines such as the business judgment rule, exculpation provisions, and heightened pleading standards have left shareholders with limited recourse in holding directors liable for the catastrophic consequences of data breaches. Recognizing that shareholders have been unsuccessful alleging *Caremark*-type claims arising out of a data breach, this Note argues that the expansion of bad faith in *Walt Disney* provides alternative ground for shareholders to hold directors liable for data breaches. Nevertheless, this Note concedes that courts will be unlikely to accept that argument. Therefore, this Note rejects Chancellor Allen's categorical refusal to extend *Caremark* beyond legal risks and argues that there are certain risks—such as cybersecurity risks—to which *Caremark* can be extended without eviscerating the business judgment rule. This Note finally argues that where *Caremark* applies, the standard should be relaxed so that plaintiff–shareholders have a means by which they can hold directors accountable for data breaches.

II. RECENT DATA BREACHES AND THEIR RELATED SHAREHOLDER DERIVATIVE SUITS

A. INTRODUCTION TO DERIVATIVE SUITS

In general, data breach litigation can be divided into four categories: (1) shareholder derivative suits; (2) securities fraud class actions; (3) class action lawsuits by the breached company's outside customers or business partners; and (4) enforcement actions by governmental agencies.[47] This Note will focus on the first of these categories.

A derivative suit is brought by a shareholder or group of shareholders "on behalf of the corporation in a representative

---

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

capacity."[48] Derivative suits claim an injury to the corporation, and any recovery goes to the corporation itself.[49]

Because "it is a fundamental principle of corporate governance that the directors of a corporation and not its shareholders manage the business and affairs of the corporation," the decision to sue or to refrain from litigating a claim on behalf of the corporation rests with the board of directors.[50] "[M]ost states, by statute or rules of civil procedure, require demand upon the corporation as a precondition to the commencement of a derivative proceeding."[51] Additionally, Rule 23.1 of the Federal Rules of Civil Procedure requires demand be made.[52] Thus, before a shareholder can bring a derivative suit, the shareholder "must first exhaust intracorporate remedies by making a demand on the directors to obtain the action desired."[53]

Data breach derivative suits often claim that directors breached their fiduciary duties, wasted corporate assets, grossly mismanaged the corporation, and/or abused their control.[54] Nevertheless, not a single derivative action brought by shareholders against a board for breach of fiduciary duties related to a data breach has succeeded.[55] "In fact, no derivative actions . . . in the context of cybersecurity have survived a motion to dismiss."[56] While the potential for litigation against directors and officers following a data breach is high, the last quarter century has witnessed a shift away from director accountability,[57] suggesting that directors and officers may continue to escape liability related to such breaches.

---

[48] JAMES D. COX & THOMAS L. HAZEN, 3 TREATISE ON THE LAW OF CORPORATIONS § 15:3 (3d ed. 2010).

[49] *See id.* (noting the basic distinction between derivative and direct-action suits).

[50] 13 WILLIAM MEADE FLETCHER, FLETCHER CYCLOPEDIA OF THE LAW OF CORPORATIONS § 5963 (Westlaw database updated Sept. 2018).

[51] *Id.* (footnote omitted).

[52] *Id.*

[53] *Id.*

[54] *See* Wong, *supra* note 12, at 203.

[55] *See* Yegelwel, *supra* note 30, at 246.

[56] *Id.*

[57] *See* Anne Tucker Nees, *Who's the Boss? Unmasking Oversight Liability Within the Corporate Power Puzzle,* 35 DEL. J. CORP. L. 199, 205 (2010) ("A quarter-century shift away from director accountability has created a narrow and virtually unenforceable standard for director oversight liability in shareholder derivative suits absent clear violations of the law.").

B. WYNDHAM WORLDWIDE CORPORATION

From April 2008 to January 2010, Wyndham Worldwide Corporation (WWC), a Delaware corporation, "sustained three data breaches that resulted in the theft of credit card and other personal information of over 600,000 customers."[58] After the board unanimously denied his demand, plaintiff–shareholder Dennis Palkon filed a derivative action alleging that WWC's board of directors breached their fiduciary duties of care and loyalty.[59] The complaint alleged that the board wasted corporate assets by (1) failing to implement adequate data security mechanisms and internal controls to protect customers' personal and financial information; and (2) failing to timely disclose the breaches.[60] As to WWC's data security mechanisms and internal controls, the complaint specifically alleged the following: (1) WWC lacked adequate information security policies and procedures (such as firewalls); (2) the operating system behind WWC's server was so out of date that the vendor stopped providing security updates for the operating system for more than three years prior to the intrusions; and (3) the "software was configured inappropriately, resulting in storage of payment card information in clear readable text."[61]

Arguing that the board's demand refusal was not wrongful and that the plaintiff failed to allege any viable state law claims, WWC moved to dismiss pursuant to Rules 23.1(b) and 12(b)(6) of the Federal Rules of Civil Procedure.[62] The court explained that under Delaware law, demand refusal falls within the purview of the business judgment rule.[63] To rebut the business judgment rule, the plaintiff must "plead[] with particularity that the [board's] decision

---

[58] John C. Cleary & Bruce A. Radke, *Lessons From Dismissal of Wyndham Shareholders Derivative Actions,* VEDDER PRICE PC (Nov. 2014), https://www.vedderprice.com/lessons-from-dismissal-of-wyndham-shareholders-derivative-action.

[59] Palkon v. Holmes, No. 2:14-CV-01234(SRC), 2014 WL 5341880, at *2 (D.N.J. Oct. 20, 2014).

[60] *Id.* ("At the heart of Plaintiff's Complaint is an assertion that Defendants failed to implement adequate data-security mechanisms . . . [and] that Defendants failed to timely disclose the data breaches after they occurred.").

[61] Complaint at 3, *Palkon*, 2014 WL 5341880. The Complaint alleged that the operating system was so out of date that the vendor had last provided security updates more than three years before the intrusions occurred. *Id.*

[62] *See Palkon*, 2014 WL 5341880, at *3.

[63] *Id.*

[to refuse demand] was either: (1) 'made in bad faith,' or (2) 'based on an unreasonable investigation.'"[64]

Underlying the plaintiff's bad faith claim, the plaintiff argued that "the board's refusal was influenced by conflicted legal counsel."[65] The plaintiff argued that the law firm was conflicted because it already represented WWC in related FTC litigation, and that WWC's general counsel was conflicted because he faced personal liability stemming from the data breaches.[66] The court explained that "[the firm's] obligations in the FTC and shareholder matters were identical: it had to act in WWC's best interest," and that the plaintiff's argument regarding WWC's general counsel lacked factual support.[67]

Additionally, the plaintiff argued that "the Board's investigation was predetermined and thus unreasonable."[68] In response, the court stated that "[i]n light of the ample information the Board had at its disposal when it rejected Plaintiff's demand, and considering the numerous steps the Board took to familiarize itself with the subject matter of the demand, Plaintiff has also failed to make this showing."[69] Noting the strong presumption of the business judgment rule, the court explained that "courts uphold even cursory investigations by boards refusing shareholder demands."[70] The court thus granted the defendants' motion to dismiss.[71]

C. TARGET CORPORATION

Over the 2013 holiday season, Target Corporation, a Minnesota corporation, suffered a data breach that resulted in the theft of more than 70 million customers' credit card and debit card information.[72]

---

[64] *Id.* (citing *In re* Merrill Lynch & Co., 773 F.Supp.2d 330, 351 (S.D.N.Y. 2011).

[65] *Id.* at *4.

[66] *Id.* at *4–5.

[67] *Id.* at *5 ("Plaintiff pleads no facts whatsoever as to what exactly McLester's supposed role was in the creation of the security programs. What was his intimate involvement? Without an answer to that question, Plaintiff's assertion falls short of the particularized pleading requirement of Rule 23.1(b), and it constitutes a conclusory allegation that the Court must disregard.").

[68] *Id.*

[69] *Id.*

[70] *Id.* at *6 (citing Levine v. Smith, 591 A.2d 194, 199, 214 (Del. 1991), *overruled by* Brehm v. Eisner, 746 A.2d 244 (Del. 2000)).

[71] *Id.* at *7.

[72] *See* Posses, *supra* note 6.

As a result, numerous shareholders filed derivative suits against Target.[73] In a consolidated complaint, the plaintiffs alleged, among other things, that the directors breached their duty of loyalty "by knowingly and/or in conscious disregard of their fiduciary duties: (i) failing to implement a system of internal controls to protect customers' personal and financial information; (ii) failing to oversee the (inadequate) internal controls that failed to protect customers' personal and financial information; and (iii) causing and/or permitting the Company to conceal the full scope of the data breach, which led to the loss of 110 million records."[74]

The complaint specifically alleged that Target's board: (1) knew Target's point-of-sale machines were vulnerable, yet decided not to update the systems; (2) bought a state-of-the-art program to protect its servers, yet failed to take the time and effort to develop data security controls or implement industry best practices; and (3) "failed to implement and oversee the people, policies, and procedures necessary to successfully run the program."[75] The complaint also alleged that once the hackers were in the system, there were no firewalls or other common protective measures in place to prevent the hackers from migrating across the system.[76]

Shortly after the complaint was filed, Target formed a special litigation committee (SLC) "to investigate all of the shareholders' claims, determine whether it made sense for Target to pursue the allegations and respond to the litigation on behalf of the board."[77] The SLC concluded that Target should not pursue the derivative claims against the board; therefore, Target and the director–defendants moved to dismiss.[78] Unfortunately for the plaintiffs,

---

[73] *See, e.g.*, Complaint & Demand for Jury Trial, Davis v. Steinhafel, No. 0:14-CV-00261, 2014 WL 497105 (D. Minn. Jan. 28, 2014); Complaint & Demand for Jury Trial, Kulla v. Steinhafel, No. 0:14-CV-00203, 2014 WL 459982 (D. Minn. Jan. 21, 2014); Complaint & Demand for Jury Trial, Collier v. Steinhafel, No. 0:14-CV-00266, 2014 WL 321798 (D. Minn. Jan. 29, 2014).

[74] Consolidated Complaint at 72, *Davis*, 2014 WL 3853976.

[75] *Id.* at 1.

[76] *Id.* at 3.

[77] *See* Posses, *supra* note 6.

[78] *Id.* ("After 21 months, the committee issued a 91-page report in March, concluding that Target shouldn't pursue derivative claims against the officers and directors, the motion said. The committee moved to dismiss the actions in May, contending that the court should defer to its decision."); Memorandum of Law of the Special Litigation Committee of the Board of Directors of Target Corporation in Support of its Motion for Approval and Dismissal, *Davis v. Steinhafel,* No. 14-CV-00203, 2016 WL 2905335 (D. Minn. May 6, 2016); Defendants

"[u]nder Minnesota law, courts do not second-guess an SLC's conclusions or re-examine the merits of its decisions; rather, the Court's inquiry is limited to determining whether the SLC's members are disinterested and independent and whether the SLC's methodology indicates that its decision was the product of a good faith investigation."[79] The plaintiff–shareholders subsequently stipulated to the dismissal of all shareholder claims.[80] Therefore, in a short two-page order without analysis, the court granted the motions to dismiss.[81]

D. THE HOME DEPOT, INC.

Over the course of several months in 2014, hackers accessed the security system of The Home Depot, Inc., a Delaware corporation, and managed to steal the financial data of 56 million customers.[82] The consolidated complaint alleged, among other things, that the board breached its duty of loyalty by failing to institute internal controls sufficient to oversee the risks that Home Depot faced in the event of a breach.[83] To support the allegations, the complaint alleged a number of deficiencies in Home Depot's network security as it stood at the time of the breach.[84] For example, the board was informed that Home Depot was out of compliance with the Payment Card Industry Data Security Standards on multiple levels.[85]

Memorandum in Support of their Motion to Dismiss, *Davis v. Steinhafel*, No. 14-CV-00203, 2016 WL 2905337 (D. Minn. May 11, 2016).

[79] *See Davis,* 2016 WL 2905335.

[80] *Davis v. Steinhafel*, No. 14-CV-00203, 2016 BL 515842 (D. Minn. July 7, 2016) (order granting motions to dismiss).

[81] *Id.*

[82] *See* Joseph B. Crace, Jr. & Virginia M. Yetter, *When Does Data Breach Liability Extend to the Boardroom?*, LAW360 (Apr. 3, 2017), https://www.law360.com/articles/907786 (describing the Home Depot breach and its related litigation).

[83] Redacted Consolidated Complaint at 37, Bennek v. Ackerman, No. 1:15-CV-2999, 2015 WL 10008489 (N.D. Ga. Sept. 2, 2015).

[84] *Id*. at 17.

[85] *See In re* The Home Depot, Inc. Shareholder Derivative Litig., 223 F. Supp. 3d 1317, 1322 (N.D. Ga. 2016) ("According to the Complaint, Home Depot's contracts with financial institutions required them to comply with the Payment Card Industry Data Security Standards ("PCI DSS"), which established a minimum level of protection for data security. PCI DSS 2.0, the version of the standards in place at the time of the Breach, required Home Depot to: (1) install and maintain a firewall, (2) protect against malware and regularly update its anti-virus software, (3) encrypt transmission of cardholder data, (4) not store cardholder data beyond the time necessary to authorize a transaction, (5) limit access to payment card data, and (6) to regularly test its data security systems.").

Additionally, encryption technology had only been installed in twenty-five percent of Home Depot's stores by the time the breach was discovered.[86] Once the breach was discovered, Home Depot was able to install encryption technology in the remaining seventy-five percent of its stores in just six days.[87]

The plaintiffs made no demand on the board, and as a result, the defendants filed a motion to dismiss pursuant to Rule 23.1(b).[88] Applying Delaware law, the Northern District of Georgia found that the plaintiffs failed to overcome the "incredibly high hurdle" of showing that the directors either "*knew* they were not discharging their fiduciary obligations or that the directors demonstrated a *conscious* disregard for their responsibilities such as by failing to act in the face of a known duty to act."[89] Although the plaintiffs acknowledged that a plan was in place, they argued that Home Depot implemented the plan too slowly.[90] The court stated that the directors violated their duty of loyalty only "if they knowingly and *completely* failed to undertake their responsibilities."[91] The court then noted that "as long as the . . . [d]irectors pursued *any* course of action that was reasonable, they would not have violated their duty of loyalty."[92] The court admitted that "one can safely say that the implementation of the plan was probably too slow," but reasoned that the decision need not be perfect—just reasonable—and granted Home Depot's motion to dismiss.[93]

E. EQUIFAX INC.

On September 7, 2017, Equifax Inc., a Georgia corporation, issued a press release announcing a data breach which resulted in hackers accessing information such as names, Social Security numbers, birth dates, addresses, and driver's license numbers, from

---

[86] *Id.* at 1323.
[87] *Id.*
[88] *Id.* at 1323–24.
[89] *Id.* at 1325 (quoting *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 123 (Del. Ch. 2009)).
[90] *Id.* at 1326.
[91] *Id.* (quoting Lyondell Chem. Co. v. Ryan, 970 A.2d 235, 243–44 (Del. 2009)).
[92] *Id.*
[93] *Id.* at 1332.

approximately 143 million U.S. consumers.[94] Additionally, the hackers accessed "credit card numbers for approximately 209,000 U.S. consumers, . . . certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers," and personal information for an undisclosed number of United Kingdom and Canadian residents.[95] The investigation revealed that the unauthorized access occurred from mid-May until it was discovered on July 29, 2017.[96]

The day after the data breach was announced, Equifax's stock price opened nearly fifteen percent lower than the day before.[97] The Federal Trade Commission publicly confirmed that it launched an investigation into Equifax.[98] Several state attorneys general opened investigations into the hacking, and others filed lawsuits seeking civil penalties.[99] The Securities and Exchange Commission also began investigating Equifax after it discovered that three of Equifax's officers sold their shares just days after the company discovered the data breach.[100] Equifax's Form 10-Q, which was filed on November 9, 2017, stated that "more than 240 class actions have been filed by consumers . . . in federal, state, and Canadian courts relating to the cybersecurity incident."[101] The various plaintiffs

---

[94] Press Release, Equifax Inc., Equifax Announces Cybersecurity Incident Involving Consumer Information (Sept. 7, 2017) (on file with the Securities and Exchange Commission).

[95] *Id*.

[96] *Id*.

[97] Carmen Germaine, *Investors Could Find Litigation Success with Equifax Breach*, LAW360 (Sept. 11, 2017, 8:53 PM), https://www.law360.com/articles/962711/investors-could-find-litigation-success-with-equifax-breach.

[98] *See* Brian Fung & Hamza Shaban, *The FTC Is Investigating the Equifax Breach*, WASH. POST (Sept. 14, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/09/14/the-ftc-confirms-its-investigating-the-equifax-breach-adding-to-a-chorus-of-official-criticism/?utm_term=.80d8ebf6448f (describing the FTC's investigation and the congressional response to the data breach).

[99] *See* Peter J. Henning, *Hack Will Lead to Little, if Any, Punishment for Equifax*, N.Y. TIMES (Sept. 20, 2017), https://www.nytimes.com/2017/09/20/business/equifax-hack-penalties.html ("Massachusetts filed a lawsuit seeking civil penalties from Equifax for not protecting sensitive information.").

[100] *See* Kevin LaCroix, *Equifax Data Breach Litigation Now Includes Securities Suit*, D&O DIARY (Sept. 13, 2017), http://www.dandodiary.com/2017/09/articles/cyber-liability/equifax-data-breach-litigation-now-includes-securities-suit ("[O]n August 1, 2017 – that is, just days after the company discovered the data breach — Chief Financial Officer John Gamble sold shares worth $946,374 and Joseph Loughran, president of U.S. information solutions, exercised options to dispose of stock worth $584,099. Rodolfo Ploder, president of workforce solutions, sold $250,458 of stock on Aug. 2.").

[101] Equifax Inc., Quarterly Report (Form 10-Q) (Nov. 9, 2017).

"generally claim to have been harmed by alleged actions and/or omissions by Equifax in connection with the cybersecurity incident and assert a variety of common law and statutory claims seeking monetary damages, injunctive relief and other related relief."[102]

Numerous shareholders filed derivative complaints against Equifax and of its directors and officers in the Northern District of Georgia.[103] After competing motions, the court issued an order on April 4, 2018 appointing Nancy A.K. Weyl and John Weyl as lead plaintiffs and Joseph H. Weiss of WeissLaw LLP as lead counsel.[104] On July 12, 2018, the lead plaintiffs filed a verified consolidated shareholder derivative complaint seeking "to redress injuries suffered, and to be suffered, by Equifax as a direct result of breaches of fiduciary duties, violations of the federal securities laws, violations of consumer laws, waste of corporate assets, and unjust enrichment, as well as the aiding and abetting thereof, by the [named directors and officers.]"[105] Specifically, Count I alleges, among other things, that Equifax and the named directors and officers (1) failed to have reasonable and necessary risk oversight, information security, internal control, monitoring, crisis management governance, and disclosure controls; (2) utterly disregarded safeguarding critically sensitive and confidential information; (3) failed to take adequate measures to protect Equifax's data systems; (4) ignored numerous red flags and warnings; and (5) failed to maintain adequate monitoring systems to detect security breaches.[106]

In support of those allegations, the complaint highlights that Equifax has long acknowledged both the importance of data security and the fact that it is regularly the target of attempted cyber threats.[107] Despite such acknowledgement, the complaint states that Equifax "has systematically experienced problems protecting

---

[102] *Id*.

[103] *See, e.g.*, Complaint & Demand for Jury Trial, Bax v. Smith, No. 0:18-CV-00317 (N.D. Ga. Jan. 22, 2018); Complaint & Demand for Jury Trial, Boston Ret. Sys. v. Smith, No. 0:18-CV-00317 (N.D. Ga. Mar. 22, 2018).

[104] *In re* Equifax, Inc. Derivative Litig., No. 1:18-CV-00317 (N.D. Ga. Apr. 4, 2018) (order appointing lead plaintiffs and lead counsel).

[105] Complaint & Demand for Jury Trial at 116, *In re* Equifax, Inc. Derivative Litig., No. 1:18-CV-00317 (N.D. Ga. July 12, 2018).

[106] *Id*. at 120–21.

[107] *Id*. at 40–44.

consumers' information dating back years" which, along with specific warnings from consultants and third parties, "put the Board on notice that they had failed to implement effective security systems, practices, defenses, and monitoring and that Equifax was highly susceptible to a data breach."[108] After providing numerous examples of Equifax's recent problems protecting consumers' information, the complaint then narrowed in on Equifax's problematic software—"Apache Struts."[109]

"On March 7, 2017, the Apache Software Foundation issued two security bulletins advising of critical security vulnerabilities in the Apache Struts software . . . ."[110] The vulnerability was ranked as "critical" and users, like Equifax, were advised "to upgrade to the new versions, which contained a security patch."[111] On March 9, 2017, the Department of Homeland Security emailed Equifax directly warning of the vulnerability and specifically instructing Equifax to install the patch.[112] Despite additional urgent warnings and alerts as to the severity of the vulnerability, "Equifax failed to install the patch or take other necessary measures to protect against the flaw."[113] Just two months later, "hackers began exploiting the known and unpatched vulnerability" until the data breach was detected on July 29, 2017.[114]

As of this writing, Equifax has not yet answered or responded to the complaint. Nevertheless, the Equifax data breach has prompted conversations about cybersecurity protocols, protections, and what corporations should be doing to better protect data.

III. THE EVOLUTION OF FIDUCIARY DUTIES UNDER DELAWARE LAW

Directors of Delaware corporations stand in a fiduciary relationship to both shareholders and the corporations upon whose boards they serve.[115] This idea was expressed as early as 1926 in

---

108 *Id*. at 45-46.
109 *Id*. at 56.
110 *Id*.
111 *Id*.
112 *Id*. at 57.
113 *Id*. at 59.
114 *Id*.
115 *See* Randy J. Holland, *Delaware Directors' Fiduciary Duties: The Focus on Loyalty*, 11 U. PA. J. BUS. L. 675, 681 (2009) ("The directors of Delaware corporations stand in a fiduciary

Bodell v. General Gas & Electric Corp.[116] In 1939, the Supreme Court of Delaware explicitly stated that "[c]orporate officers and directors . . . stand in a fiduciary relation to the corporation and its stockholders."[117] Under Delaware law, directors' fiduciary duties—the duty of care and the duty of loyalty—have evolved over the years in foundational corporate law cases.[118]

A. THE DUTY OF CARE

The duty of care is a largely process-based duty that requires directors, in making decisions, to inform themselves of all material information reasonably available.[119] Although the Supreme Court of Delaware stated in 1963 that directors are required to "use that amount of care which ordinarily careful and prudent men would use in similar circumstances,"[120] the applicable standard for establishing a violation of the duty of care is gross negligence.[121]

1. The Business Judgment Rule

The business judgment rule is "an acknowledgment of the managerial prerogatives of Delaware directors under Section 141(a)."[122] The traditional formulation of the rule was that "[a] complete absence of selfish motive and of personal profit on [the directors'] part forcefully argues that their judgment was formed in absolute honesty and entire good faith."[123] However, in *Aronson v. Lewis*, the Supreme Court of Delaware described the rule as "a presumption that in making a business decision the directors of a

relationship not only to the stockholders, but also to the corporations upon whose boards they serve.").

116 *Id*. at 680; *see* Bodell v. Gen. Gas & Elec. Corp., 132 A. 442, 446 (Del. Ch. 1926) ("There is no rule better settled in the law of corporations than that directors in their conduct of the corporation stand in the situation of fiduciaries.").

117 Guth v. Loft, Inc., 5 A.2d. 503, 510 (Del. 1939).

118 *See* Jacobs, *supra* note 31 and accompanying text.

119 *See* Holland, *supra* note 115, at 691.

120 Graham v. Allis-Chalmers Mfg. Co., 188 A.2d 125, 130 (Del. 1963).

121 *See* Jacobs, *supra* note 31, at 146 ("[O]nly one year before, the Delaware Supreme Court held that the standard for due care liability was 'gross negligence'—a far more onerous standard to satisfy than the simple negligence standard under common tort law.").

122 *See* Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984); DEL. CODE ANN. tit. 8, § 141(a) (2016) ("The business and affairs of every corporation . . . shall be managed by or under the direction of a board of directors . . . .").

123 Bodell v. Gen. Gas & Elec. Corp., 132 A. 442, 449 (Del. Ch. 1926).

corporation acted on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company."[124] The rule has developed from a "rule of deference to expert opinion" into a "structural procedural defense precluding judicial inquiry into the directors' challenged actions."[125] The rule "protect[s] and promote[s] the full and free exercise of the managerial power granted to Delaware directors."[126]

There are two overarching rationales underlying the business judgment rule. First, shareholder interests are best served if corporate directors are risk-seeking instead of risk-averse.[127] "[B]ecause potential profit often corresponds to the potential risk, it is very much in the interest of shareholders that the law not create incentives for overly cautious corporate decisions."[128] Shareholders can diversify their portfolios, thereby reducing their volatility and making sure that "courts need not bend over backwards to give special protection to shareholders" who chose not to do so.[129] Second, "courts are ill equipped and infrequently called on to evaluate what are and must be essentially business judgments."[130] In other words, "judges . . . are poorly positioned to assess the propriety of complex business decisions."[131] As the Supreme Court of Delaware explained, "the essence of the business judgment rule [is] that a court will not apply 20/20 hindsight to second guess a board's decision."[132] If the board's decision can be attributed to a rational

---

[124] *Aronson*, 473 A.2d at 812.

[125] Dalia Tsuk Mitchell, *The Import of History to Corporate Law*, 59 ST. LOUIS U. L.J. 683, 692 (2015).

[126] Smith v. Van Gorkom, 488 A.2d 858, 872 (Del. 1985) (citing Zapata Corp. v. Maldonado, 430 A.2d 779, 782 (Del. 1981)).

[127] *See* Gagliardi v. Trifoods Int'l Inc., 683 A.2d 1049, 1052 (Del. Ch. 1996) ("Shareholders don't want (or shouldn't rationally want) directors to be risk averse."); Christine Hurt, *The Duty to Manage Risk*, 39 J. CORP. L. 253, 272 (2014) ("The traditional argument for limiting the enforcement of this duty with the business judgment rule, and against claims that corporate boards were negligent, is that shareholders would prefer boards to be risk-seeking instead of risk-averse.").

[128] Joy v. North, 692 F.2d 880, 886 (2d Cir. 1982).

[129] *Id.*

[130] Auerbach v. Bennett, 393 N.E.2d 994, 1000 (N.Y. 1979).

[131] Ryan Scarborough & Richard Olderman, *Why Does the FDIC Sue Bank Officers? Exploring the Boundaries of the Business Judgment Rule in the Wake of the Great Recession*, 20 FORDHAM J. CORP. & FIN. L. 367, 374 (2015).

[132] *See* Brehm v. Eisner, 746 A.2d 244, 260 (Del. 2000); *see also Joy*, 692 F.2d at 886 ("[A] reasoned decision at the time made may seem a wild hunch viewed years later against a background of perfect knowledge.").

business purpose, then the court will not substitute its judgment for that of the board.[133] Courts do not want to act as "super-directors," nor will courts "measure, weigh or quantify directors' judgments."[134] Essentially, the rule is process-based, meaning the court will look at how the decision was made instead of the result of the decision.[135]

2. Exculpatory Provisions

Prior to 1985, "no public company board of directors had been liable for money damages solely for breaching their duty of care."[136] In 1985, business and legal communities were rocked when the Supreme Court of Delaware decided *Smith v. Van Gorkom*.[137] In *Smith*, "an unconflicted and independent board was found grossly negligent for approving an arm's length merger without having informed themselves of the fair value of their company."[138] Specifically, the directors breached their duty of care by failing "to inform themselves of all information reasonably available to them and relevant to . . . [the] merger" and by failing "to disclose all material information such as a reasonable stockholder would consider important in deciding whether to approve the [merger]."[139]

The *Smith* decision was "highly criticized,"[140] "decried as a threat to free-market, corporate capitalism,"[141] and its dissenting opinion

---

[133] *See* Holland, *supra* note 115, at 681 ("A hallmark of the business judgment rule is that a court will not substitute its judgment for that of the board if the latter's decision 'can be attributed to any rational business purpose.'"); *see also* Sinclair Oil Corp. v. Levien, 280 A.2d 717, 720 (Del. 1971) ("A board of directors enjoys a presumption of sound business judgment, and its decisions will not be disturbed if they can be attributed to any rational business purpose.").

[134] *Brehm*, 746 A.2d at 264, 266.

[135] *See* Robert T. Miller, *The Board's Duty to Monitor Risk After Citigroup*, 12 U. PA. J. BUS. L. 1153, 1164–65 (2010) ("Delaware courts consider not the content of the decision (that is, whether the decision was on the merits right or wrong, reasonable or unreasonable, prudent or foolish, etc.) but only the process of decision-making leading up to the decision (that is, whether the directors considered all the material information reasonably available and made an honest judgment as to what was in the best interest of the company)." (footnotes omitted)).

[136] Jacobs, *supra* note 31, at 146.

[137] 488 A.2d 858 (Del. 1985).

[138] Jacobs, *supra* note 31, at 146; *see also Smith*, 488 A.2d at 864 (finding that the board's decision "was not the product of an informed business judgment").

[139] *Smith*, 488 A.2d at 893.

[140] Bernard S. Sharfman, *The Enduring Legacy of* Smith v. Van Gorkom, 33 DEL. J. CORP. L. 287, 289 (2008).

[141] Stephen J. Lubben & Alana J. Darnell, *Delaware's Duty of Care*, 31 DEL. J. CORP. L. 589, 599 (2006).

referred to the decision as a "comedy of errors."[142] In response to *Smith*, Delaware quickly adopted Delaware General Corporation Law (D.G.C.L.) Section 102(b)(7).[143] The statute allows corporations to adopt a charter provision "eliminating or limiting the personal liability of a director to the corporation or its stockholders for monetary damages for breach of fiduciary duty as a director."[144] The statute carves out several exceptions, specifying circumstances in which exculpation is not available to a director.[145] The statute expressly prohibits exculpation for breaches of the fiduciary duty of loyalty, acts or omissions not in good faith, and transactions from which a director receives an improper personal benefit.[146] The statute has been read "as authorizing charter provisions limiting or eliminating director liability for duty of care violations."[147] In effect, this provision has "limit[ed] the usefulness of most due care claims."[148] When invoked, an exculpatory provision essentially provides a basis for dismissal at the outset of a case that alleges a violation of the duty of care.[149]

B. THE DUTY OF LOYALTY

The duty of loyalty is sometimes referred to as the authentic fiduciary duty.[150] In *Guth v. Loft, Inc.*, the Supreme Court of Delaware stated that "[t]he rule that requires an undivided and unselfish loyalty to the corporation demands that there shall be no conflict between duty and self-interest."[151] The court explained that directors "are not permitted to use their position of trust and

---

142 *Smith*, 488 A.2d at 894 (McNeilly J., dissenting).

143 *See* John L. Reed & Matt Neiderman, *"Good Faith" and the Ability of Directors to Assert § 102(b)(7) of the Delaware General Corporation Law as a Defense to Claims Alleging Abdication, Lack of Oversight, and Similar Breaches of Fiduciary Duty*, 29 DEL. J. CORP. L. 111, 113 (2004) (providing a brief history and background of § 102(b)(7)).

144 DEL. CODE ANN. tit. 8, § 102(b)(7) (2015).

145 Jacobs, *supra* note 31, at 147.

146 DEL. CODE ANN. tit. 6, § 102(b)(7) (2003).

147 Reed & Neiderman, *supra* note 143, at 114 (internal quotations omitted).

148 Lubben & Darnell, *supra* note 141, at 600.

149 Richard B. Kapnick & Courtney A. Rosen, *The Exculpatory Clause Defense to Shareholder Derivative Claims,* SIDLEY AUSTIN LLP (2010), https://www.sidley.com/~/media/files/publications/2010/01/the-exculpatory-clause-defense-to-shareholder-de__/files/view-article/fileattachment/kapnickrosen_reprint.pdf.

150 *See, e.g.*, Mitchell, *supra* note 125, at 683.

151 Guth v. Loft, Inc., 5 A.2d. 503, 510 (Del. 1939).

confidence to further their private interests."[152] Should any such conflict arise, the director must place the interests of the corporation and its shareholders ahead of his or her personal interests.[153] The duty of loyalty demands of an officer or director "the utmost good faith in his relation to the corporation which he represents."[154]

1. The Duty of Good Faith

In 1993, in *Cede & Co. v. Technicolor, Inc.*, the Supreme Court of Delaware identified the "*triads* of [directors'] fiduciary duty—good faith, loyalty [and] due care."[155] The court thus interpreted the duty of good faith "as a third, standalone, liability-creating fiduciary duty of equal dignity."[156]

After *Technicolor*, Delaware courts saw plaintiffs bringing bad faith cases as a way to get around the exculpation provision.[157] However, in 2005, the Supreme Court of Delaware more fully addressed the duty of good faith in *In re Walt Disney Co. Derivative Litigation*.[158] In *Walt Disney*, the court gave the duty of good faith "content and meaning . . . by holding that bad faith required conduct more egregious than gross negligence."[159] Specifically, the court said that "[a] failure to act in good faith may be shown . . . where the fiduciary intentionally acts with a purpose other than that of advancing the best interests of the corporation, where the fiduciary acts with the intent to violate applicable positive law, or where the fiduciary intentionally fails to act in the face of a known duty to act, demonstrating a conscious disregard for his duties."[160] This meant that plaintiffs could no longer attempt to run around exculpation provisions by conflating the duties of care and good faith.[161] One year later, in *Stone v. Ritter*, the Supreme Court of Delaware "put good faith back in the original doctrinal box where it had always

---

[152] *Id.*

[153] *Id.*

[154] *Id.*

[155] Cede & Co. v. Technicolor, Inc., 634 A.2d 345, 361 (Del. 1993).

[156] Jacobs, *supra* note 31, at 147.

[157] *Id.* at 148.

[158] *In re* Walt Disney Co. Derivative Litig., 906 A.2d 27 (Del. 2006).

[159] Jacobs, *supra* note 31, at 148 (citing *Walt Disney*, 906 A.2d at 67).

[160] *Walt Disney*, 906 A.2d at 67.

[161] Jacobs, *supra* note 31, at 148 ("*Disney* also put an end to plaintiffs' attorney efforts to do an end run around § 102(b)(7) through arguments that conflated the duties of care and good faith.").

properly belonged—as a subsidiary element or 'condition' of the duty of loyalty."[162]

2. The Duty of Oversight

The duty of oversight has existed since 1963, when *Graham v. Allis-Chalmers Manufacturing Co.* was decided, but the duty was largely irrelevant and nameless until 1996.[163] Prior to *Graham*, "there had been no cases challenging a board for a failure to act."[164] Delaware cases reviewing board conduct almost always involved an affirmative decision by the board.[165] In *Graham*, the plaintiff–shareholders claimed that the board failed to monitor whether senior management was complying with applicable law.[166] The Delaware Supreme Court stated that "directors of a corporation in managing the corporate affairs are bound to use that amount of care which ordinarily careful and prudent men would use in similar circumstances."[167] However, the court held that "absent cause for suspicion there is no duty upon the directors to install and operate a corporate system of espionage to ferret out wrongdoing which they have no reason to suspect exists."[168] In terms of oversight, *Graham* only imposed an obligation on boards not to ignore red flags.[169]

Thirty-three years after *Graham,* the duty of oversight finally received some name recognition. In the 1996 Delaware Supreme

---

[162] *Id*. at 149; *see* Stone v. Ritter, 911 A.2d 362, 370 (Del. 2006) ("[A]lthough good faith may be described colloquially as part of a 'triad' of fiduciary duties that includes the duties of care and loyalty, the obligation to act in good faith does not establish an independent fiduciary duty that stands on the same footing as the duties of care and loyalty." (footnote omitted)).

[163] *See* Graham v. Allis-Chalmers Mfg. Co., 188 A.2d 125, 130 (Del. 1963) ("The precise charge made against these director defendants is that, even though they had no knowledge of any suspicion of wrongdoing on the part of the company's employees, they still should have put into effect a system of watchfulness which would have brought such misconduct to their attention in ample time to have brought it to an end . . . . On the contrary, it appears that 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. If such occurs and goes unheeded, then liability of the directors might well follow, but absent cause for suspicion there is no duty upon the directors to install and operate a corporate system of espionage to ferret out wrongdoing which they have no reason to suspect exists.").

[164] Jacobs, *supra* note 31, at 149.

[165] *See id*. ("[M]ost Delaware cases reviewing board conduct involved an affirmative decision by the board, typically to approve a corporate transaction of some kind.").

[166] *Graham*, 188 A.2d at 127.

[167] *Id*. at 130.

[168] *Id*.

[169] *Id*.

Court case, *In re Caremark International*, *Inc. Derivative Litigation*, plaintiff–shareholders sued the board for failing to monitor the conduct of senior management, who had violated "federal and state laws and regulations applicable to health care providers" and caused the company to incur significant civil and criminal penalties.[170] In other words, the board failed to know about the illegal conduct of the corporation's senior managers. Chancellor William T. Allen explained that corporate boards must be reasonably informed concerning the corporation and assure themselves "that information and reporting systems exist in the organization that are reasonably designed to provide . . . timely, accurate information sufficient to allow management and the board . . . to reach informed judgments concerning both the corporation's compliance with law and its business performance."[171] The court held that in cases where the board is unaware of employee misconduct that results in the corporation being held liable, "only 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 exists—will establish the lack of good faith that is a necessary condition to liability."[172]

The *Caremark* decision "raised the *Allis-Chalmers* obligation not to ignore red flags to an affirmative duty to conclude that an adequate corporate compliance system was in place."[173] However, *Caremark* failed to clearly articulate "what conduct would constitute an actionable violation of the duty of oversight" or how that duty fit within the other fiduciary duties.[174] The duty of oversight appeared to "flow[] from the duty of care," but this meant little in light of the fact that "due care liability would be precluded in any company having a § 102(b)(7) exculpatory charter provision."[175]

In *Stone v. Ritter*, the Supreme Court of Delaware addressed *Caremark* head on, and established the current doctrine: in order to prevail on a *Caremark* claim, a plaintiff must prove that either (a)

---

170 *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 960 (Del. Ch. 1996).
171 *Id.* at 970.
172 *Id.* at 971.
173 Mercer Bullard, *Caremark's Irrelevance*, 10 BERKELEY BUS. L.J. 15, 24 (2013).
174 Jacobs, *supra* note 31, at 150.
175 *Id.* at 150–51.

"the directors utterly failed to implement any reporting or information systems or controls" to monitor the business, or (b) "having implemented such a system or controls, [the directors] consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."[176] The court noted that the "imposition of liability requires a showing that the directors *knew* that they were not discharging their fiduciary obligations."[177] This means that oversight liability has a scienter requirement.[178]

Oversight liability was the bedrock of the plaintiff's principal claim in *In re Citigroup Inc. Shareholders Derivative Litigation* which was brought before the Delaware Chancery Court in 2009.[179] In the wake of the financial crisis, Citigroup's shareholders asserted that some of Citigroup's former directors "breached their fiduciary duties by failing to properly monitor and manage risks the [c]ompany faced from problems in the subprime lending market."[180]

Unlike historical *Caremark* claims, the oversight claim in *Citigroup* was premised on an alleged failure by the board to detect and prevent excessively risky business decisions—*not* fraud or illegality—by corporate employees.[181] The *Citigroup* decision offers an example of how one might adapt *Caremark* claims to cases of risk management failure.[182] However, Chancellor Chandler stated that although "it may be tempting to say that directors have the same duties to monitor and oversee business risk, imposing *Caremark*-type duties on directors to monitor business risk is fundamentally different . . . [because doing so] would involve courts in conducting hindsight evaluations of decisions at the heart of the business judgment of directors."[183] The Chancellor concluded that "[o]versight duties under Delaware law are not designed to subject directors, even expert directors, to *personal liability* for failure to

---

176 *Id*. at 370.
177 *Id*. (emphasis added).
178 Miller, *supra* note 135, at 1157.
179 *In re* Citigroup Inc. S'holders Derivative Litig., 964 A.2d 106 (Del. Ch. 2009).
180 *Id*. at 111.
181 *Id*.
182 *See* Stephen M. Bainbridge, *Caremark and Enterprise Risk Management*, 34 J. CORP. L. 967, 978 (2009) (describing the *Citigroup* decision's adaptation to the context of risk management failure).
183 *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 131 (Del. Ch. 2009).

predict the future and to properly evaluate business risk."[184] However, Chancellor Chandler did not completely shut the door. He explained that although the plaintiff–shareholders in *Citigroup* failed to state a *Caremark* claim, "it may be possible for a plaintiff to meet the burden under some set of facts."[185] Therefore, it is possible for shareholders to hold a board liable under *Caremark* for failing to oversee and monitor the corporation's cybersecurity risks—under the right set of facts.[186]

IV. THE PLEADING STANDARD

Under Delaware law, before a shareholder can bring a derivative suit, the shareholder must comply with Court of Chancery Rule 23.1[187] by either: (1) making a pre-suit demand by presenting the allegations to the board and requesting that they bring suit, or (2) pleading with particularity facts showing that a demand on the board would have been futile.[188] If demand is made, the board considers the demand and typically declines to sue.[189] The decision not to sue is protected by the business judgment rule.[190]

If a plaintiff–shareholder challenges a specific board decision without making demand on the board, the shareholder must provide particularized factual allegations that raise a reasonable doubt that: (1) the directors are disinterested and independent, or (2) the challenged transaction was otherwise the product of a valid exercise of business judgment (the "*Aronson* Test").[191] However, when a

---

[184] *Id.*

[185] *Id.* at 126.

[186] *Id.*

[187] DEL. CT. CH. R. 23.1.

[188] *Citigroup*, 964 A.2d at 120.

[189] *See* Joseph W. Cooch, *In re* Citigroup Inc. Shareholder Derivative Litigation*: In the Heat of Crisis, Chancery Court Scrutinizes Executive Compensation*, 6 J. BUS. & TECH. L. 169, 177 (2011) (providing an overview of the pre-suit demand requirement and demand futility).

[190] *Id.*

[191] *See* Levine v. Smith, 591 A.2d 194, 205–06 (Del. 1991) ("Assuming a plaintiff cannot prove that directors are interested or otherwise not capable of exercising independent business judgment, a plaintiff in a demand futility case must plead particularized facts creating a reasonable doubt as to the 'soundness' of the challenged transaction sufficient to rebut the presumption that the business judgment rule attaches to the transaction."), *overruled on other grounds by* Brehm v. Eisner, 746 A.2d 244 (Del. 2000); *see also Brehm*, 746 A.2d at 253 ("Our view is that in determining demand futility the Court of Chancery . . . must decide whether, under the particularized facts alleged, a reasonable doubt is created that: (1) the directors are disinterested and independent [or] (2) the challenged transaction was

plaintiff–shareholder complains of board *in*action, as is common in data breach litigation, the shareholder "must allege particularized facts that 'create a reasonable doubt that, as of the time the complaint is filed, the board of directors could have properly exercised its independent and disinterested business judgment in responding to a demand.'"[192] In other words, even in cases where the business judgment rule is inapplicable, plaintiffs still bear the burden of having to plead non-exculpated claims, such as the duty of oversight, based on particularized facts alleging bad faith.[193]

Plaintiff–shareholders thus face a catch-22. If they make demand and the board declines to sue, plaintiff–shareholders must overcome the presumption of the business judgment rule—a very difficult task to accomplish. If the plaintiff–shareholders choose not to make a demand, they must establish that demand would have been futile—also a difficult task. Plaintiff–shareholders almost always choose the latter option, also known as demand futility.[194] As a result, after shareholders file their complaint, defendants usually "move[] to dismiss the complaint under Rule 23.1 on the ground that a demand was required but not made."[195] Courts often find that the shareholders failed to plead with particularity and grant the defendant's motion to dismiss.[196]

Pleading with particularly is remarkably difficult in the context of *Caremark* claims. Shareholders are subject to information asymmetry, which is made more difficult by the fact that modern corporations have various levels of board and executive

---

otherwise the product of a valid exercise of business judgment." (citing Aronson v. Lewis, 473 A.2d 805, 814 (Del. 1984))); *Citigroup*, 964 A.2d at 120.

192 *Citigroup*, 964 A.2d at 120 (quoting Rales v. Blasband, 634 A.2d 927, 934 (Del. 1993)).

193 *See* Martin Petrin, *Assessing Delaware's Oversight Jurisprudence: A Policy and Theory Perspective*, 5 VA. L. & BUS. REV. 433, 479 (2011) ("To successfully plead bad faith, the plaintiff must allege with particularity that a director knowingly violated a fiduciary duty or failed to act in violation of a known duty to act, demonstrating a conscious disregard for her duties.").

194 *See* Jack B. Jacobs, *The Vanishing Substance-Procedure Distinction in Contemporary Corporate Litigation: An Essay*, 41 SUFFOLK U. L. REV. 1, 3 (2007) ("Although both the Federal and Delaware Rule 23.1 contemplate the making of a demand, in most Delaware stockholder derivative actions, no demand is ever made.").

195 *Id*.

196 *See, e.g.*, *In re* The Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp.3d 1317, 1327 (N.D. Ga. 2016) (holding that the demand requirement was not excused).

committees.[197] Shareholders struggle not only to allege red flags that are substantial in the court's eyes, but also to show that the boards were aware of the red flags in the first place.[198] Shareholders must also plead facts that demonstrate scienter, which gets "at the heart of the meaning of bad faith—a conscious disregard for one's responsibilities."[199] Although shareholders may utilize D.G.C.L. Section 220, which allows them limited access to corporations' "books and records,"[200] plaintiffs often lack access to documents and other sources of evidence "that reveal with particularity the defendant's state of mind."[201]

Worsening the pleading situation for plaintiff–shareholders, the Delaware Supreme Court characterized the demand requirement as "a rule of substantive right" in its 1984 *Aronson* case.[202] In *Aronson*, the court stated that "the demand requirement of Rule 23.1 is . . . designed to give a corporation the opportunity to rectify an alleged wrong without litigation, and to control any litigation which does arise."[203] As a result, substantive business judgment concepts such as disinterest, independence, due care, and good faith "acquired operative significance in determining whether

---

[197] *See* Hurt, *supra* note 127, at 281 ("First, the board of directors must not have any type of risk-management system in place, but must be on notice of the problem because of the existence of 'red flags.' These facts are not easily alleged, particularly against a modern corporation with various levels of board and executive committees.").

[198] *See, e.g.*, *In re* Citigroup, Inc. S'holder Derivative Litig., 964 A.2d 106, 128 (Del. Ch. 2009) ("The 'red flags' [alleged] in the Complaint amount to little more than portions of public documents that reflected the worsening conditions in the subprime mortgage market and in the economy generally.").

[199] *See* Eric J. Pan, *Rethinking the Board's Duty to Monitor: A Critical Assessment of the Delaware Doctrine*, 38 FLA. ST. U. L. REV. 209, 215, 232 (2011) ("The Delaware Supreme Court's decision made it more difficult for plaintiffs to bring duty to monitor claims. The court placed the burden on the plaintiff to demonstrate a director's scienter in failing to act in the face of red flags.").

[200] *See* DEL. CODE ANN. tit. 8, § 220 (2010) ("Any stockholder, in person or by attorney or other agent, shall, upon written demand under oath stating the purpose thereof, have the right during the usual hours for business to inspect for any proper purpose, and to make copies and extracts from: (1) The corporation's stock ledger, a list of its stockholders, and its other books and records.").

[201] Pan, *supra* note 199, at 232.

[202] Aronson v. Lewis, 473 A.2d 805, 809 (Del. 1984); *see also* Jacobs, *supra* note 194, at 4 ("In adopting this test, the Aronson court blended together a procedural requirement with a substantive rule . . . by characterizing the demand requirement as a substantive right and by infusing the term "demand futility" with substantive business judgmentconcepts . . . .").

[203] *Aronson*, 473 A.2d at 809 (citing Lewis v. Aronson, 466 A.2d 375, 380 (Del. Ch. 1983)).

a derivative action would be allowed to survive."[204] In effect, viewing the demand requirement as a rule of substantive right has created "mini-litigation" regarding substantive business judgment concepts within the pleading stage—despite the fact that shareholders have only limited access to materials that would enable them to plead with particularity.

V. EXISTING LAW PROVIDES ALTERNATIVE GROUND FOR SHAREHOLDERS

Thus far, shareholders have been unsuccessful alleging *Caremark*-type claims—that the board breached its duty to oversee and monitor cybersecurity risks—arising out of a data breach. Fortunately, there is alternative, narrow ground under existing law for plaintiff–shareholders to hold directors liable for the catastrophic consequences of a data breach. When a shareholder brings a derivative suit, the shareholder must overcome the business judgment rule.[205] As discussed in Part III, this rule presumes that in making a business decision, management "acted on an informed basis, in good faith, and in honest belief that the action taken was in the best interest of the company."[206] To overcome this presumption, the plaintiff–shareholder must show at least one of the following: (1) that the director(s) engaged in self-dealing or waste; (2) that the decision-making process was grossly negligent (i.e., the directors failed to inform themselves prior to making the decision); or (3) that the directors acted in bad faith.[207] Since most Delaware corporations have enacted exculpation provisions pursuant to D.G.C.L. Section 102(b)(7), plaintiff–shareholders will struggle to succeed on claims that the directors' decision-making was grossly negligent.[208] Nevertheless, corporations may not exculpate directors for acts or omissions not in good faith or for breach of the duty of loyalty, which is "breached

---

[204] Jacobs, *supra* note 172, at 5.

[205] *See* Hurt, *supra* note 127, at 270–71.

[206] *Aronson*, 473 A.2d at 812.

[207] *See* Joseph K. Leahy, *A Decade After Disney: A Primer on Good and Bad Faith*, 83 U. CIN. L. REV. 859, 861 (2015) (describing the business judgment rule and how to overcome it).

[208] *Id*. ("Yet, proving gross negligence on its own probably will be insufficient for a plaintiff to survive a motion to dismiss, because the vast majority of Delaware corporations have waived damages for breaches of the duty of care, including gross negligence.").

when a director acts in bad faith."[209] In *Walt Disney*,[210] the Supreme Court of Delaware "squarely addressed, for the first time, the meaning of bad faith under Delaware corporate law."[211] In doing so, the court provided alternative ground for plaintiff–shareholders to succeed in bringing derivative suits related to a data breach by alleging that the board acted in bad faith.

In *Walt Disney*, plaintiff–shareholders brought a derivative action alleging, among other things, that the directors and officers breached their fiduciary duties relating to the hiring and firing of Michael Ovitz, who was a close friend of Disney's then-CEO Michael Eisner.[212] Ovitz was fired just after fourteen months in office with a generous termination payment amount of approximately $130 million.[213] The plaintiffs alleged that "the directors' rubber-stamping of Ovitz's hiring was not just negligent or grossly negligent, but bad faith."[214] In deciding the case, the Supreme Court of Delaware expanded the traditional understanding of "bad faith."

The traditional understanding of "bad faith" refers to "director actions that are motivated by a dishonest purpose or ill will towards the corporation and/or its shareholders."[215] The Supreme Court of Delaware explained, however, that "at least three different categories of fiduciary behavior are candidates for the 'bad faith' pejorative label."[216] These three categories exist on a spectrum.[217] On one end of the spectrum is the traditional, quintessential

---

[209] *Id*. at 862.

[210] *In re* Walt Disney Co. Derivative Litig., 906 A.2d 27 (Del. 2006).

[211] Leahy, *supra* note 207, at 863.

[212] 906 A.2d at 36; *see also* Leahy, *supra* note 207, at 867–68 (The plaintiffs in *Disney* alleged, *inter alia*, that the board rubberstamped Ovitz's hiring and gigantic compensation as a favor to Disney's then-CEO Michael Eisner, because Ovitz and Eisner were long-time, close friends.").

[213] 906 A.2d at 35.

[214] Leahy, *supra* note 207, at 868; *In re* Walt Disney Co. Derivative Litig., 825 A.2d 275, 278 (Del. Ch. 2003) ("[T]he facts alleged in the new complaint do not implicate merely negligent or grossly negligent decision making by corporate directors. Quite the contrary; plaintiffs' new complaint suggests that the Disney directors failed to exercise *any* business judgment and failed to make *any* good faith attempt to fulfill their fiduciary duties to Disney and its stockholders.").

[215] Leahy, *supra* note 207, at 863; *see also Walt Disney*, 906 A.2d at 64 n.102 (affirming the accuracy of this traditional understanding).

[216] 906 A.2d at 64.

[217] *Id*. (using the concept of a spectrum to describe the different categories of fiduciary behavior).

understanding of "bad faith."[218] On the opposite end is fiduciary conduct taken solely by reason of gross negligence, without any malevolent intent.[219] This end of the spectrum represents "less culpable, *good* faith conduct that is nonetheless wrongful because it violates the duty of care."[220] This end of the spectrum may not result in director liability since "grossly negligent conduct, without more, does not and cannot constitute [bad faith]."[221]

The Court of Chancery identified a third category, which falls somewhere in the middle of the spectrum. As defined by Chancellor Chandler, the third category of bad faith is intended to capture conduct that constitutes an "intentional dereliction of duty, a conscious disregard for one's responsibilities."[222] Chancellor Chandler explained that "this concept . . . is an appropriate (although not the only) standard for determining whether fiduciaries have acted in good faith."[223] In affirming this definition, the Supreme Court of Delaware explained that the "universe of fiduciary misconduct is not limited to either disloyalty in the classic sense . . . or gross negligence."[224] The court explained that conduct falling within the middle of the spectrum, which is "qualitatively more culpable than gross negligence, should [also] be proscribed" in order "to protect the interests of the corporation and its shareholders."[225] The court stated that the doctrinal vehicle to address such violations is the duty to act in good faith.[226] The court identified three of the "most salient" examples of bad faith, but stated that "[t]here may be other examples of bad faith yet to be proven or alleged."[227] In refusing "a definitive and categorical definition of the universe of acts that would constitute bad faith,"[228]

---

218 *Id*.

219 *Id*.

220 Leahy, *supra* note 207, at 866–67.

221 906 A.2d at 65.

222 *Id*. at 66 (citing *In re* Walt Disney Co. Derivative Litig., 907 A.2d 693 (Del. Ch. 2005)).

223 *Id*. at 62.

224 *Id*. at 66. The court also explained that this third category of bad faith receives support from the statutory language of D.G.C.L. § 102(b)(7)(ii), which "distinguishes between 'intentional misconduct' and a 'knowing violation of law' (both examples of subjective bad faith) on the one hand, and 'acts . . . not in good faith,' on the other." *Id*. at 67.

225 *Id*. at 66.

226 *Id*.

227 *Id*. at 67.

228 *Id*.

the Supreme Court of Delaware left open the precise contours of bad faith. Most importantly, the court noted that conduct falling in the middle of the spectrum is not exculpable.[229]

Therefore, existing law provides alternative ground for shareholder derivative suits related to a data breach that is separate from a *Caremark*-type claim, which has traditionally involved the failure to monitor compliance and fraud, and based upon *Walt Disney*'s expansion of bad faith. Plaintiff–shareholders could succeed without having to undertake the difficult task of proving subjective bad faith. However, plaintiff–shareholders would need to prove more than gross negligence on behalf of the directors. In other words, plaintiff–shareholders would need to show that their claim alleges conduct that falls in the middle of the spectrum and is therefore not exculpable.

For example, hypothetical corporation ABC owns one of the largest chain clothing stores in the United States. ABC's database contains sensitive information about its customers, including credit card numbers and social security numbers. The directors are aware of the need for appropriate oversight and have therefore ensured that a risk management assessment system is in place. The system is designed to protect data, monitor for data breaches, and alert senior management when a breach is discovered. After having put the system in place, the directors feel at ease knowing they have fulfilled their *Caremark* oversight duties—they have ensured that a reasonable information and reporting system exists. Two years have passed without any cyberattacks on corporation ABC. However, many other corporations in ABC's industry have sustained enormous data breaches in the last two years. Additionally, ABC's system has become outdated and ABC's directors learn that their system is the same system used by Target prior to its data breach. Further, the directors learn that the system is unable to protect against some of the latest hacking techniques. Nevertheless, the board fails to address any cybersecurity concerns at their meetings or redress the cybersecurity issues. Six months later, hackers infiltrate ABC's network and steal sensitive data.

---

[229] *Id.* ("Because the statute exculpates directors only for conduct amounting to gross negligence, the statutory denial of exculpation for 'acts . . . not in good faith' must encompass the intermediate category of misconduct captured by the Chancellor's definition of bad faith.").

Soon after the data breach, a shareholder files a derivative suit against ABC. Rather than filing a *Caremark*-type claim—alleging that the board breached its oversight duties—the suit alleges that the board acted in bad faith. Under these facts, the plaintiff–shareholder may be able to succeed in accusing the directors not only of gross negligence, but also of intentionally failing to redress the known cybersecurity issues, evidencing a conscious disregard of a known risk. The plaintiff–shareholder would likely not be able to show that the directors subjectively intended to harm the corporation. However, the plaintiff–shareholder may be able to show that the board intentionally chose not to redress the cybersecurity issues despite knowing the probable harmful consequences of a massive data breach.

VI. RELAXING THE *CAREMARK* STANDARD FOR DATA BREACH LIABILITY

A. OVERVIEW

In *Citigroup*, Chancellor Chandler made clear his concern that allowing directors to be held personally liable for failing to monitor for business risks would open the floodgates for board liability, ultimately eviscerating the business judgment rule.[230] Chancellor Chandler pointed out that "Delaware Courts have faced these types of claims many times and have developed doctrines to deal with them—the fiduciary duty of care and the business judgment rule."[231] Assuming Chancellor Chandler's concerns are ubiquitous among his colleagues, Delaware Courts are unlikely to allow claims alleging bad faith with respect to cybersecurity risks. Therefore, this Note agrees with the outcome of *Citigroup*, but rejects Chancellor Allen's categorical refusal to extend *Caremark* beyond legal risks. Instead,

---

[230] *See In re* Citigroup, Inc. S'holder Derivative Litig., 964 A.2d 106, 125 (Del. Ch. 2009) ("[C]orporations have certain responsibilities to implement and monitor a system of oversight; however, this obligation does not eviscerate the core protections of the business judgment rule—protections designed to allow corporate managers and directors to pursue risky transactions without the specter of being held personally liable if those decisions turn out poorly. . . . To the extent the Court allows shareholder plaintiffs to succeed on a theory that a director is liable for a failure to monitor business risk, the Court risks undermining the well settled policy of Delaware law by inviting Courts to perform a hindsight evaluation of the reasonableness or prudence of directors' business decisions.").

[231] *Id.* at 124.

this Note argues that there are certain risks to which *Caremark* can be extended without eviscerating the business judgment rule. This Note then argues that where *Caremark* applies, courts should relax the standard so that plaintiff–shareholders have a means by which they can hold the board accountable. In an age of data breaches, the time has come for the *Caremark* standard to have some teeth.

B. EXTENDING *CAREMARK* BEYOND LEGAL COMPLIANCE

In *Caremark*, Chancellor Chandler held that the duty of oversight only requires that a board implement programs to monitor for fraud and illegal conduct.[232] Years later in *Citigroup*, Chancellor Chandler explained that extending the duty of oversight to business risks would impinge on a board's business judgment.[233] However, the line should not be drawn at whether a risk is categorized as legal or business. The line between such risks can be blurry and it is unclear how the categories should be differentiated. There are certain risks that boards should be required to monitor and guard against regardless of their categorization. This is not to say that a board must have a system in place to prevent every possible problem—there must be some parameters. This Note proposes three parameters for risks to which *Caremark* should be extended.

First, the risk should be preventable. The *Caremark* standard itself is concerned with implementing systems to prevent problems that may affect the business enterprise.[234] Preventable risks "are internal risks, arising from within the organization, that are

---

[232] *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 970 (Del. Ch. 1996) ("[A] director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by noncompliance with applicable legal standards."); *see also Citigroup*, 964 A.2d at 131 ("There are significant differences between failing to oversee employee fraudulent or criminal conduct and failing to recognize the extent of a Company's business risk. Directors should, indeed must under Delaware law, ensure that reasonable information and reporting systems exist that would put them on notice of fraudulent or criminal conduct within the company.").

[233] *Citigroup*, 964 A.2d at 131 ("To impose oversight liability on directors for failure to monitor 'excessive' risk would involve courts in conducting hindsight evaluations of decisions at the heart of the business judgment of directors.").

[234] *See* Bainbridge, *supra* note 182, at 968 ("*Caremark* held that the board of directors has a duty to ensure that appropriate 'information and reporting systems' are in place to provide the board and top management with 'timely, accurate information.'" (quoting *Caremark*, 698 A.2d at 970)).

controllable and ought to be eliminated or avoided."[235] Preventable risks, such as employees' unauthorized, illegal actions, are best managed through monitoring.[236] This is consistent with *Caremark*, where Caremark's employees violated "federal and state laws and regulations applicable to health care providers" by receiving payments for referring Medicare and Medicaid patients.[237] As with illegal conduct, data breaches can have a significant impact on businesses and can be prevented through the implementation of monitoring programs. Such programs can notify companies if their software is vulnerable to attack or in need of an update, or if a hacker has entered their system.

Second, the risk should not go to the heart of the business judgment rule. The business judgment rule protects directors from being held liable for business decisions, including the failure to see the extent of a company's business *risk*.[238] In *Citigroup*, Chancellor Allen defined risk as "the chance that a return on an investment will be different than expected."[239] One rationale underlying the business judgment rule is that protecting decision makers encourages more profitable risk-taking in order to maximize returns for investors.[240] Essentially, the heart of the business judgment rule lies in protecting those business decisions and risks associated with financial transactions and financial exposure that may result in excessive risk or loss in return on investment. Unlike *Citigroup*, where the risk involved financial exposure to the subprime

---

[235] Robert S. Kaplan & Anette Mikes, *Managing Risks: A New Framework*, HARV. BUS. REV. (2012), https://hbr.org/2012/06/managing-risks-a-new-framework.

[236] *Id.* (stating that preventable risks are "best managed through active prevention: monitoring operational processes and guiding people's behaviors and decisions toward desired norms").

[237] *Caremark*, 698 A.2d at 960–61.

[238] *In re* Citigroup, Inc. S'holder Derivative Litig., 964 A.2d 106, 126 (Del. Ch. 2009) ("To impose liability on directors for making a "wrong" business decision would cripple their ability to earn returns for investors by taking business risks. Indeed, this kind of judicial second guessing is what the business judgment rule was designed to prevent.").

[239] *Id.*

[240] *See* Aaron Brumbaugh, *The Business Judgment Rule and the Diversified Investor: Encouraging Risk in Financial Institutions*, 17 U.C. DAVIS BUS. L.J. 171, 174 (2017) ("The Business Judgment Rule offers decision makers a safeguard from liability associated with the possible poor outcomes of those risky decisions, which in turn encourages the decision makers to be less averse to risk and thus more willing to take the risks and aim for the returns that diversified shareholders want.").

mortgage market for short-term profits,[241] neither legal risks (like those in *Caremark*) nor cybersecurity risks go to the heart of the business judgment rule. The risk associated with cybersecurity is that the corporation's sensitive data will be exposed and used in a harmful way.

Lastly, the risk should pose a significant threat to a corporation and its business performance. As Chancellor Allen explained in *Caremark*, the board should ensure that "information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation's *compliance with law* and *its business performance*."[242] Cybersecurity risks pose an enormous threat to businesses—just ask Wyndham, Target, Home Depot, and Equifax.[243] Data breaches not only expose a business's sensitive data, but they can also cause a corporation to incur relentless litigation from both shareholders and consumers, a loss in investor and consumer trust and loyalty, and a drop in stock prices.

C. RELAXING *CAREMARK*

Where the *Caremark* standard applies, it is impossibly high.[244] When analyzing *Caremark* claims that allege a board has breached its duty to oversee and monitor cybersecurity risks, courts should no longer merely ask whether *any* reporting systems exist. In the cybersecurity context, the mere existence of a system does little to satisfy a board's duty of oversight and ensure that the corporation is protected from data breaches. Therefore, courts should relax the *Caremark* standard and infer bad faith when the board only nominally implements a system. The core question that courts should ask is whether the board acted in good faith in implementing a corporate information and reporting system. In the context of cybersecurity, there are certain factors that courts should consider

---

241 *See Citigroup*, 964 A.2d at 113–15 (explaining the losses and risks associated with the company's actions).

242 698 A.2d at 970 (emphasis added).

243 *See supra* Part II.B–E.

244 *See Caremark*, 698 A.2d at 967 ("The theory here advanced is possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment.").

to determine whether the board acted in good faith: (1) the manner in which the cybersecurity monitoring system was implemented; (2) whether the monitoring system ensured that data security mechanisms were maintained, updated, or enhanced; and (3) the mechanism's capabilities in light of the volume and type of data stored.

1. The Manner of Implementation

Examining the manner in which cybersecurity monitoring systems were implemented is a process-oriented approach, which is consistent with a business judgment analysis. *In re The Home Depot, Inc. Shareholder Derivative Litigation* is a prime example for the necessity of examining the implementation of such systems.[245] In this case, there was no dispute that a plan existed for the protection of Home Depot's data.[246] However, the court found issue in the plan's slow implementation.[247] Judge Thrash stated in the opinion that "one can safely say that the implementation of the plan was probably too slow . . . . [T]he Board probably should have done more."[248]

The implementation of cybersecurity monitoring systems should be especially scrutinized when the board is aware of deficiencies in its data security. For example, Home Depot was well aware of deficiencies in its data security prior to the breach; the board and audit committee knew that Home Depot was out of compliance with Payment Card Industry Data Security Standards on multiple levels.[249] While compliance with a contract does not rise to the compliance with law as seen in the typical *Caremark* claim, the board's failure to comply with the PCI DSS is evidence that the board did not act in good faith to protect the interests of the shareholders by protecting the company's data.

The court should also consider whether the board was only nominally implementing a monitoring system. For example, despite Home Depot's board knowing that it lacked sufficient data security

---

[245] *See generally In re* The Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317 (N.D. Ga. 2016).

[246] *Id.* at 1326 ("Importantly, the Plaintiffs repeatedly acknowledge that there *was* a plan . . . .").

[247] *Id.*

[248] *Id.* at 1327.

[249] *Id.* at 1322.

mechanisms, it installed encryption technology at only twenty-five percent of its stores before the breach was discovered.[250] Rather than ensuring that the deficiencies were cured by quickly implementing security measures, such as data encryption technology, the board ignored the risk posed by such insufficiencies.[251] The board essentially checked the "have a reporting system or controls" box. After it discovered the breach, Home Depot was able to install encryption technology in the remaining seventy-five percent of its stores in just six days.[252]

2. Maintaining, Updating, & Enhancing

Courts should also examine whether the company's monitoring systems ensured that its data security mechanisms were maintained, updated, or enhanced as needed. Corporations often implement mechanisms, like software or encryption technology, to protect their data.[253] However, the technology that hackers use is changing and becoming more complex every day.[254] Therefore, a mechanism that was implemented five years ago, or just one year ago, may fail to protect against the latest advancements in hacking technology. A company's monitoring system must be able to notify the board when a data security mechanism needs maintenance or an update.

A common theme in shareholder derivative suits for data breaches is that the corporation's mechanisms or operating systems were out of date or not maintained. For example, in the *Wyndham*

---

[250] *Id.* at 1322–23 ("On September 8, 2014, Home Depot acknowledged that there had been a breach of its network . . . . At the time of the Breach, Home Depot's security systems were still 'desperately out of date.' . . . For example, encryption technology had only been installed at twenty-five percent of its stores by the time the Breach was discovered in September 2015.").

[251] *Id.* at 1322 ("On multiple occasions before the Breach, . . . Home Depot was out of compliance with PCI DSS on multiple levels . . . . Home Depot would likely continue to be out of compliance until February 2015.").

[252] *Id.*

[253] *See* Dan Hirsh, *Understanding Firewalls and Their Role in Network Security*, SCHNEIDER ELECTRIC (Aug. 19, 2011), https://blog.schneider-electric.com/datacenter/2011/08/19/understanding-firewalls-and-their-role-in-network-security ("In practice, most companies deploy two firewalls to create a DMZ, or demilitarized zone.").

[254] *See, e.g.,* Danny Palmer, *Hackers Are Using This New Attack Method to Target Power Companies*, ZDNET (July 10, 2017), http://www.zdnet.com/article/hackers-are-using-this-new-attack-method-to-target-power-companies (describing a new hacking technique that allows hackers to run phishing campaigns without malicious code).

case, Wyndham used a vendor to provide the company's operating system.[255] An operating system "is software that communicates with the hardware and allows other programs to run. It is comprised of system software, or the fundamental files your computer needs to boot up and function."[256] The burden was on Wyndham to update its operating system, however, Wyndham failed to do so. Wyndham's operating system was so out of date that the vendor stopped providing security updates for more than three years prior to the data breach.[257] Operating systems must be updated in order to address security vulnerabilities because "[o]lder software will continue to have the same bugs and exploitable holes in the code that allow hackers and cyber criminals [access]."[258] Considering that the board in *Wyndham* allowed the company to have a vulnerable operating system and go three years without security updates, it can hardly be said that the board fulfilled its duty of oversight in good faith.

3. The Mechanisms in Place

When conducting a *Caremark* analysis, courts should also examine a company's cybersecurity mechanisms in light of the volume and type of data stored. When a board implements a monitoring plan or system for its cybersecurity, the mere fact that a plan or system exists is no longer acceptable. The monitoring mechanisms must be capable of protecting against intrusive data breaches. This means that courts should consider the number of mechanisms in place, whether the mechanisms appropriately protect the type of data stored, whether the mechanisms are adaptable to new technology, and whether the mechanisms provide for real-time detection as opposed to infrequent system scanning. For example, a company like Equifax, which possesses the data of

---

[255] Verified Shareholder Derivative Complaint for Breach of Fiduciary Duty, Waste of Corporate Assets, and Unjust Enrichment at 3, Palkon v. Holmes, No. 2:14-CV-01234(SRC) (D.N.J. Oct. 20, 2014).

[256] TECHTERMS, OPERATING SYSTEM (2016), https://techterms.com/definition/operating_system.

[257] Verified Shareholder Derivative Complaint for Breach of Fiduciary Duty, Waste of Corporate Assets, and Unjust Enrichment at 3, Palkon v. Holmes, No. 2:14-CV-01234(SRC) (D.N.J. Oct. 20, 2014).

[258] Marshal de Saxe, *5 Reasons Why It's Important to Update Your Software Regularly*, SAXONS BLOG (July 18, 2017), http://www.saxonsgroup.com.au/blog/tech/5-reasons-important-update-software-regularly.

more than 820 million consumers and more than 91 million businesses worldwide,[259] should have heightened cybersecurity protections because of the sheer volume and sensitive nature of the data it stores.

Additionally, courts should consider whether the mechanisms are capable of preventing both the intrusion into the company's system and migration across the system once inside. In other words, directors are in a better position when they have implemented a double layer of protection. For example, when Target's system was hacked, there were no firewalls or other common protective measures in place to prevent the hackers from exploring and migrating across the system.[260] Therefore, once inside, the hackers had free reign and went undetected for months.[261] The monitoring system in place was incapable of detecting the breach.

Another important consideration is whether there were red flags that the company's mechanisms were inadequate or that certain malware or technology posed a threat to the mechanisms in place. For example, when Target was hacked, the hackers used BlackPOS,[262] which "is a specialized piece of malware designed to be installed on point-of-sale (POS) devices and record all data from credit and debit cards swiped through the infected system."[263] BlackPOS has been used in several similar attacks that affected customers of Chase Bank, Capital One, Citibank, and more.[264] After these public breaches, other corporations' boards should have inquired into their data security mechanisms to determine how they would fare in the face of a BlackPOS attack. However, many corporations fail to take affirmative steps to prevent data breaches even when they know which technologies hackers might use. The Home Depot breach was a stark example of this; the hackers used a

---

[259] Press Release, Equifax Inc., Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes (Sept. 15, 2017) (on file with the Securities and Exchange Commission).

[260] Consolidated Complaint at 3, Davis v. Steinhafel, No. 14-CV-203(PAM/JJK), 2014 WL 3853976 (D. Minn. July 18, 2014).

[261] *Id*.

[262] *Id*. at 45.

[263] Chris Smith, *Expert Who First Revealed Massive Target Hack Tells Us How It Happened*, BGR (Jan. 16, 2014, 11:00 AM), http://bgr.com/2014/01/16/how-was-target-hacked.

[264] *Id*.

version of BlackPOS that was very similar to the one used in the Target data breach just a few months earlier.[265]

VII. CONCLUSION

In an age of massive data breaches, boards should be held to a higher standard with respect to their duty to oversee and monitor cybersecurity risks. Thus far, shareholders have been unsuccessful alleging *Caremark*-type claims related to a data breach. Although alternative ground for shareholder derivative suits related to a data breaches does exist based on *Walt Disney's* expansion of bad faith, it is unlikely that courts will allow these claims. Courts are too wary of opening the floodgates of director liability and eviscerating the business judgment rule. Therefore, courts should extend the *Caremark* standard beyond legal risks to certain other risks; those that are preventable, do not go to the heart of the business judgment rule, and do pose a substantial threat to the corporation and its business performance. Where courts apply the *Caremark* standard, they should relax it to hold boards to a higher standard and allow shareholders to hold directors accountable for failing to oversee and monitor cybersecurity risks. Corporations must affirmatively and continuously focus on their cybersecurity protections, rather than treat it as a routine exercise in ticking boxes. Liability in the cybersecurity context is necessary to prevent directors and officers from having a false sense of security once they have established some base level of risk management.

---

[273] *See* Brian Krebs, *Home Depot Hit by Same Malware as Target*, KREBS ON SECURITY (Sept. 7, 2014, 11:14 PM), https://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target (describing in depth background on the variant of BlackPOS used in the Target and Home Depot breaches).