CAREMARK LIABILITY IN THE DIGITAL AGE: CORPORATE DIRECTORS' OVERSIGHT DUTIES IN THE DATA PRIVACY DOMAIN

Sam Gross

INTRODUCTION

When in 1964 Bob Dylan recorded his third album "The Times They Are a-Changin," it seemed unlikely that he was thinking about twenty-first century data privacy laws. Nonetheless, just as the 1960s saw widespread social and legal transformations, so too today's rapid changes in the digital realm have prompted sweeping new privacy laws in the United States and around the world. These extraordinary new measures, which include the California Consumer Privacy Act (CCPA) [1] and the EU's General Data Protection Regulation (GDPR),[2] have left companies scrambling to understand properly their elevated legal duties and obligations.

For board members of the 1.4 million business entities incorporated in the State of Delaware, these new legal regimes likewise create uncharted obligations and risks.[3] This paper will focus on the interplay between these recently enacted privacy measures and one area of Delaware corporate law: the fiduciary duties that corporate directors owe to a company's shareholders. Specifically, this paper will focus on directors' so-called *Caremark* duty. This duty, famously established in the case of *In re Caremark International Inc. Derivative Litigation*,[4] mandates that directors monitor their company for misconduct. This monitoring duty includes ensuring that the company observes all of its legal obligations.

This paper proceeds in five parts. It begins in Part I by briefly surveying Delaware fiduciary duty law, the seminal *Caremark* decision, and its progeny. Next, Part II examines the history and broad statutory requirements of GDPR and the CCPA. Building on this discussion, Part III reviews the related field of corporate data breach litigation. Putting these instructive contextual strings together, Part IV outlines precisely how and why data privacy

[1] California Consumer Privacy Act of 2018 (CCPA), 2018 Cal. Stat. ch. 55.

[2] Regulation (EU) 2016/679 of the European Parliament and Council of the European Union on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Apr. 27, 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294&from=en [hereinafter GDPR].

[3] DEL. DIV. CORPS., 2018 ANNUAL STATISTICS, https://corp.delaware.gov/stats/.

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

requirements could lead to *Caremark* liability for corporate boards, ultimately finding that boards can indeed be held liable under *Caremark* for failing to take appropriate monitoring steps in the data privacy domain. The paper will conclude in Part V by offering practical actions that boards can take to alleviate the risk of liability. These include board level privacy committees, repeated reviews of company monitoring procedures, and regular education on data privacy issues.

I. DIRECTORS' FIDUCIARY DUTIES

In Delaware, a company's board of directors is responsible for "the business and affairs of every corporation."[5] In fulfilling these responsibilities, "the directors owe fiduciary duties of care and loyalty to the corporation and its shareholders."[6] Importantly, these duties apply at all times that a director serves on a corporation's board.[7]

A. Duties of Care & Loyalty

Historically, the board's duty of care required corporate directors to use the "amount of care which ordinarily careful and prudent men would use in similar circumstances."[8] However, Delaware courts have lowered this standard in recent years. Today, the courts examine board decisions under what is effectively a gross negligence standard.[9] Directors meet their duty so long as do not act with "reckless indifference to or a deliberate disregard of the whole body of stockholders or actions which are without the bounds of reason."[10] Accordingly, the decisions of corporate directors are remarkably difficult to challenge through duty of care claims in court.

Directors also owe a duty of loyalty to the corporation. Put simply, the duty of loyalty requires that directors "determine the best interests of the corporation and its stockholders" and to "abjure any action that is motivated by considerations other than a good faith

---

[5] DEL. CODE ANN. tit. 8 § 141(a). *See also* Mills Acquisition Co. v. Macmillan, Inc., 559 A.2d 1261, 1280 (Del. 1989) ("It is basic to our law that the board of directors has the ultimate responsibility for managing the business and affairs of a corporation.").

[6] *Mills Acquisition*, 559 A.2d at 1280. *See generally* 1 R. FRANKLIN BALOTTI & JESSE A. FINKELSTEIN, BALOTTI AND FINKELSTEIN'S DELAWARE LAW OF CORPORATIONS AND BUSINESS ORGANIZATIONS § 4.14 FIDUCIARY DUTIES (3rd ed. 2020).

[7] *See* Emerald Partners v. Berlin, 787 A.2d 85, 90 (Del. 2001).

[8] Graham v. Allis-Chambers Mfg. Co., 188 A.2d 125, 130 (Del. Ch. 1963).

[9] BALOTTI & FINKELSTEIN, *supra* note 6, § 4.15.

[10] Tomczak v. Morton Thiokol, Inc., 1990 Del. Ch. LEXIS 47 (Del. Ch. Apr. 5, 1990).

concern for such interests."[11] Directors cannot engage in self-dealing at the expense of the corporation. The corporation's interests must come first.

B. A New Duty for Corporate Boards: Allis Chalmers Red Flags

In addition to making decisions about the company, corporate directors' other principal function is that of oversight.[12] This duty of oversight originates from the seminal Delaware Supreme Court case of *Graham v. Allis Chalmers Mfg. Co.*[13] The defendant in that case, Allis Chalmers, was a large manufacturer of electrical equipment with over 30,000 employees.[14] After the corporation and several employees pleaded guilty to price fixing, a class of stockholders filed a derivative action to recover damages on behalf of the corporation.[15] The directors claimed not to have known about the activities of the offending company employees.[16]

The Delaware Supreme Court found for the directors and famously held:

> 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.[17]

Nonetheless, the Court also noted that if a director "has refused or neglected cavalierly to perform his duty as a director, or has ignored either willfully or through inattention obvious danger signs of employee wrongdoing, the law will cast the burden of liability upon him."[18] The Court found that there were no grounds for suspicion in this case and the directors were therefore blameless for the conduct that ultimately led to the corporate liability.[19] *Allis Chalmers* thus created a new imposition of board liability situated under the duty of care. However, these monitoring duties only applied where

---

[11] Revlon, Inc. v. MacAndrews & Forbes Holdings, Inc., 506 A.2d 173, 181 (Del. 1986).
[12] BALOTTI & FINKELSTEIN, *supra* note 6, § 4.14.
[13] *Allis-Chalmers*, 188 A.2d 125, 130 (1963).
[14] *Id.*
[15] *Id.* at 127.
[16] *Id.* at 127–29.
[17] *Id.* at 130.
[18] *Id.*
[19] *Id.*

boards had "red flags" of wrongdoing, and were accordingly on notice of the need to further investigate the misconduct.

C. The Modern Formulation: In re Caremark

Allis Chalmers stood as the definitive case on monitoring for over thirty years. However, in 1996, Chancellor Allen famously expanded upon the duties of directors to monitor corporate operations. That case, *In re Caremark Int'l Inc. Derivative Litigation*, has since become the seminal authority on the topic of monitoring duties.[20] *Caremark* involved a health care provider's alleged violations of federal and state laws banning compensation to physicians in exchange for Medicare or Medicaid referrals towards certain products.[21] As a result of the alleged violations, Caremark was subject to an extensive four-year federal investigation and was eventually indicted on multiple felonies.[22] The company subsequently entered into several settlement agreements with the Department of Justice and others.[23] These agreements totaled approximately $250 million.[24] A group of Caremark shareholders later brought suit to recover these losses from the company's individual directors.[25] The plaintiffs alleged that the company's "directors allowed a situation to develop and continue which exposed the corporation to enormous legal liability and that in so doing they violated a duty to be active monitors of corporate performance."[26]

In finding for the defendants, Chancellor Allen concluded that a plaintiff must "show either (1) that the directors knew or (2) should have known that violations of law were occurring and, in either event, (3) that the directors took no steps in a good faith effort to prevent or remedy that situation, and (4) that such failure proximately resulted in the losses complained of."[27] He concluded that here there was no evidence that the directors knew of the legal violations.[28]

Crucially however, in reaching this conclusion the Chancellor moved beyond *Allis Chalmers* red flags and instead held that directors have an affirmative duty to create systems for discovering wrongdoing within the company.[29] He stated:

---

[20] In re Caremark Int'l Inc. Derivative Litig., 698 A.2d 959 (Del. Ch. 1996).
[21] *Id.* at 962–64.
[22] *Id.*
[23] *Id.* at 966.
[24] *Id.* at 961.
[25] *Id.*
[26] *Id.* at 967.
[27] *Id.* at 971.
[28] *Id.*
[29] *Id.* at 970.

> Thus, I am of the view that 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 . . . [may] render a director liable for losses caused by non-compliance with applicable legal standards.[30]

It is now established Delaware law that boards must create and oversee these internal reporting and monitoring systems.[31]

D. Embracing a Bad Faith Element: Stone v. Ritter

The final case to hone modern duty to monitor jurisprudence came in 2006 with *Stone v. Ritter*.[32] The Delaware Supreme Court was presented once again with a derivative action, this time after AmSouth Bank was required to pay $50 million in fines and civil penalties relating to the failure of bank employees to comply with the federal Bank Secrecy Act and various other anti-money laundering regulations.[33] The Court first reaffirmed that *Caremark* correctly identified the conditions predicate for director oversight liability.[34] However, the Court also emphasized that "imposition of liability requires a showing that the directors knew that they were not discharging their fiduciary obligations."[35] In other words, the Court held that plaintiffs could not prevail on a *Caremark* claim without showing that a fiduciary acted in bad faith; a director's actions must rise to the level of actual disloyalty to the corporation. To satisfy their duty of loyalty in regards to monitoring, directors must only make a good faith effort to implement an oversight system and then a good faith effort to monitor it.

E. Reviving Duty to Monitor Claims: Marchand v. Barnhill

Given the *Stone* scienter requirement, observers have long viewed failure to monitor claims as largely a lost cause.[36] This changed in June 2019 with the Delaware Supreme Court decision in

---

[30] *Id.*
[31] *See* Hillary A. Sale, *Monitoring Caremark's Good Faith*, 32 DEL. J. CORP. L. 719, 755 (2007).
[32] Stone ex rel. AmSouth Bancorporation v. Ritter, 911 A.2d 362 (Del. 2006).
[33] *Id.* at 365.
[34] *Id.* at 370.
[35] *Id*.
[36] *See, e.g.*, Francis Pileggi, *Court Describes Board Duty of Oversight*, DEL. CORP. & COM. LITIG. BLOG (Oct. 24, 2016), https://www.delawarelitigation.com/2016/10/articles./chancery-court-updates/court-describes-board-duty-of-oversight/ (noting that such claims are "often described as one of the most difficult to prevail upon in corporate litigation.").

Marchand v. Barnhill.[37] The facts in *Marchand* surrounded an ice cream manufacturer's deadly listeria outbreak that resulted in three deaths.[38] The complaint alleged that the board of Blue Bell Creameries took effectively no monitoring actions.[39] The board scheduled no reports on food safety and did not discuss red flags in the period leading up to the outbreak.[40]

The Delaware Supreme Court reversed the Chancery Court's dismissal of the case and allowed the claims to proceed against the board.[41] In so doing, the Court reiterated that "Caremark does have a bottom-line requirement that is important: the board must make a good faith effort—i.e., try—to put in place a reasonable board-level system of monitoring and reporting."[42] Although *Caremark* claims undoubtedly remain difficult for plaintiffs to establish, *Marchand* nonetheless confirms that boards must meet their oversight duties and can be held liable if they leave this compliance and oversight entirely to the corporation's management.

II. CURRENT DATA PRIVACY LEGAL REGIMES

A. EU General Data Protection Regulation

The European Union's General Data Protection Regulation (GDPR), which first went into effect on May 25, 2018, established a unified code of data privacy laws across all EU member states.[43] The regulation applies to any business entities that offers goods or service to, or monitors the behavior of, EU citizens or residents.[44] This is true regardless of the location of the business.[45] Notably, however, GDPR applies only to those EU citizens or residents within the physical bounds of the EU at the time of the activity.[46] Thus, the GDPR does not apply to EU citizens or residents who are traveling or living abroad.[47]

The GDPR provides extensive data protections to EU residents. Some key provisions include: requiring that terms and condition statements be in plain language and easy to understand,[48] requiring that businesses ask for consent each time they access

[37] Marchand v. Barnhill, 212 A.3d 805 (Del. 2019).
[38] *Id.* at 807.
[39] *Id.* at 809.
[40] *Id.* at 822.
[41] *Id.* at 808.
[42] *Id.* at 821.
[43] *See* GDPR, *supra* note 2.
[44] *Id.* Art. 3 § 2.
[45] *Id.* Art. 3 § 3.
[46] *Id.* Art. 3 § 2.
[47] *Id.*
[48] *Id.* Art. 12 § 1.

private data,[49] and empowering EU residents with the right to demand that a company erase all personal data connected to that resident.[50]

In addition to the broad rights and protections granted to EU residents, the GDPR is perhaps equally groundbreaking for the penalties that it imposes for noncompliance. Businesses and organizations found in violation of the GDPR provisions can be fined up to 4 percent of their annual global turnover, or up to 20 million euros, whichever is higher.[51] For large multinational corporations, this turnover percentage could potentially be a figure in the billions of dollars.

B. The California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) is widely considered the most stringent data privacy law ever passed in the United States. Effective as of January 1, 2020, the CCPA mirrors many of the key components found in the GDPR.[52] While the CCPA is only in force at a state level, California's wide-ranging economic impact means that the law is still expected to impact more than 500,000 businesses.[53] At its core, the new law protects California residents' rights to know what personal information a company is collecting or selling, and grants the power to veto such use.[54]

Contrary to the GDPR, the CCPA provides for certain *de minimis* requirements to define its scope of application. A company is subject to the CCPA if it satisfies one or more of three criteria. The company must: (1) have annual gross revenues of $25 million or more; (2) buy, sell, or share the personal information on more than 50,000 consumers, households, or devices or; (3) derive more than half of its annual revenues from selling consumers' personal information.[55]

Similar to the GDPR, California residents can now ask companies subject to the CCPA about the type of information they collect and, when asked, companies must provide explicit details on how and to whom personal information is sold and shared, and for what reasons.[56] The new law also empowers California residents with greater control over how their personal information is collected

---

[49] *Id.* Art. 6 § 1.
[50] *Id.* Art. 17 § 1.
[51] *Id.* Art. 83 § 6.
[52] *See generally* CCPA, *supra* note 1.
[53] *Risk & Compliance*, FOCAL POINT, https://focal-point.com/services/risk-compliance/compliance/.
[54] COMPUTER LAW: A GUIDE TO CYBERLAW AND DATA PRIVACY LAW § 43.30 (2019).
[55] CAL. ANN. CODE 1798.140(c).
[56] *Id.* 1798.130(a).

and used. For example, a company, upon request, must provide a consumer with the data that has been collected about that person over the preceding 12 months.[57] This disclosure generally must occur within 45 days of receiving the request.[58] Furthermore, the CCPA requires that companies honor individuals' requests to opt out of data collection and to honor any individual's request to have their personal information deleted.[59]

The CCPA and the GDPR are intended to empower citizens to better understand and control their personal information and data. Though there are notable differences, both measures grant new rights and impose heightened data protection duties. To accomplish these goals, the laws grant broad prosecutorial powers to their respective enforcement agencies and, perhaps most importantly, stiff penalties and fines for companies found to be out of compliance.

III. DATA BREACH CASES

Given the relative novelty of these new privacy frameworks, there are no cases to date in which plaintiffs have directly asserted *Caremark* claims against corporate directors in relation to a company's CCPA or GDPR violations. With that said, continuing GDPR enforcement actions and the recent rollout of the CCPA will almost certainly lead to litigation in the not-so-distant future. Given the dearth of pertinent data privacy cases, it is instructive to examine a factually similar, yet more robust, line of case law for guidance: shareholder suits alleging *Caremark* claims that arise out of large-scale company data breaches.

A. Wyndham Data Breach

One of the earliest data breach cases came about after Wyndham's hotel property management system was hacked on three different occasions between April 2008 and January 2010.[60] The hackers breached Wyndham's main network and those of its hotels through a "brute force attack," in which they guessed user IDs

---

[57] *Id.*

[58] *Id.* 1798.130(a)(2) ("[A] business shall, in a form that is reasonably accessible to consumers ... Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer.").

[59] *Id.* 1798.135(a)(1) ("(a) A business ... shall, in a form that is reasonably accessible to consumers: (1) Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information").

[60] Palkon v. Holmes, No. 2:14-CV-01234, 2014 WL 5341880, at *1 (D.N.J. Oct. 20, 2014).

and passwords to enter an administrator's account.[61] The three breaches resulted in hackers obtaining the data of 619,000 Wyndham consumers.[62]

Following the breach, a group of plaintiffs filed a derivative suit in the District of New Jersey but applying Delaware law.[63] At heart, the plaintiffs argued that the director-defendants violated their fiduciary duties to Wyndham when they failed to implement adequate data-security mechanisms that allegedly led to the eventual breach.[64] The Court rejected this novel argument and explained in a footnote: "Plaintiff concedes that security measures existed when the first breach occurred, and admits the Board addressed such concerns numerous times."[65] Thus, according the court, the plaintiffs had no claim because under *Stone v. Ritter* a plaintiff must show a corporation's "directors utterly failed to implement any reporting or information system ... [or] consciously failed to monitor or oversee its operations thus disabling themselves from being informed."[66] This is a high standard for plaintiffs to meet. The Court found neither of these present in this case and granted defendants' respective motions to dismiss.[67]

B. Target Data Breach

In 2013, in the height of the holiday shopping season, Target suffered a data breach and theft of more than 40 million customers' credit card and debit card information. This breach generated massive litigation that extended for several years.[68] As of 2016, Target has estimated the total cost of the breach at over $290 million.[69]

Because of these massive losses, shareholders filed a derivative action against Target's executives and directors in the District of Minnesota, where Target is incorporated and headquartered. Among other claims, the shareholders' complaint

---

[61] *Id.* (A brute force attack involves the attacker using computer software to rapidly submit massive numbers of passwords or phrases in the hope of randomly identifying the correct access combinations.).
[62] *Id.*
[63] *Id.* at 3. Because the parties were citizens of different states and the amount in controversy exceeded $75,000, the federal court exercised diversity jurisdiction pursuant to 28 U.S.C. § 1332(a)(2). Venue and personal jurisdiction were presumably met given that Wyndham is headquartered in Parsippany, New Jersey. *Id*. at 1.
[64] *Id.* at 2.
[65] *Id.* at 6.
[66] *Id.*
[67] *Id.* at 7.
[68] *See Cost of 2013 Target Data Breach Nears $300 Million*, HASHEDOUT (May 26, 2017), https://www.thesslstore.com/blog/2013-target-data-breach-settled/.
[69] *Id.*

mirrored the language of the complaint in Wyndham and alleged that the "Defendants breached their duty of loyalty by knowingly or recklessly: (i) failing to implement a system of internal controls to protect customers' personal and financial information ... ."[70] Target subsequently convened a special litigation committee to investigate the incident.[71] This committee ultimately issued a 91-page report finding no actionable claims against the Target directors.[72] Unlike *Wyndham*, the District Court in Target applied Minnesota law, which gives significant weight to such board committee's recommendations.[73] The District of Minnesota eventually rejected the derivative claims and dismissed the suit in a short two-page order.[74]

C. Home Depot Data Breach

In September 2014, Home Depot learned that it had been the victim of a criminal breach of its payment card data systems.[75] After an investigation, Home Depot confirmed that hackers had managed to steal the financial data of 56 million customers over the course of several months.[76] This breach followed soon after other well-publicized retailer data breaches, including Target and Neiman Marcus.[77] The hackers gained access to Home Depot's network by obtaining a third-party vendor's user name and password.[78] Ultimately, the breach may have cost Home Depot as much as $10 billion in direct and indirect damages including reputation, goodwill, and standing in the business community.[79]

Soon after, shareholders filed suit against the company's directors alleging they breached their duty of loyalty by failing to institute internal controls sufficient to oversee Home Depot's risks, and by disbanding a committee that had been tasked with oversight

---

[70] Davis v. Steinhafel, Verified Shareholder Derivative Complaint for Breach of Fiduciary Duty and Waste of Corporate Assets, 2014 WL 497105 (D. Minn. Jan. 28, 2014).
[71] TARGET CORPORATION, REPORT OF THE SPECIAL LITIGATION COMMITTEE 1 (Mar. 30, 2016).
[72] *Id.* at 2.
[73] *Target Internal Report Results in Dismissal of Suit Over Cyberbreach*, 32 NO. 2 WESTLAW JOURNAL CORPORATE OFFICERS & DIRECTORS LIABILITY 3 (Jul. 25, 2016).
[74] Davis v. Steinhafel, Order Granting Defendants' Motions to Dismiss (July, 7, 2016).
[75] In re The Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317, 1321 (N.D. Ga. 2016).
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id. See also* In re The Home Depot, Inc. S'holder Derivative Litig., Verified Consolidated Shareholder Derivative Complaint at ¶ 235 (March 14, 2016).

of those risks.[80] The Court conceded that "one can safely say that the implementation of the plan was probably too slow." [81] Nevertheless, quoting Delaware case law the Court concluded that the "[d]irectors' decisions must be reasonable, not perfect" and found for the defendant directors once again.[82]

IV. ASSESSING BOARD LIABILITY

A. The High Bar of Caremark Claims

Together, these cases reaffirm the procedural and substantive difficulties facing plaintiffs who attempt to make *Caremark* claims in the data privacy and security realm. Courts in Delaware, as well as those outside the state applying Delaware law, have repeatedly repudiated plaintiffs' attempts to hold boards accountable for data breaches after the fact.

These case precedents should be reassuring for boards. In many ways data privacy liability closely tracks that of data breaches. As pointed out by the *Wyndham* court, once a board adopts any security measures, no matter how basic, it likely meets its burdens under *Ritter*.[83] After all, *Ritter* employs fairly absolutist language requiring that directors "utterly fail" to implement a reporting and monitoring system or "consciously fail" to monitor it. Thus, presumably as with the data breaches, once a board has established basic systems to report and address violations of GDPR or the CCPA, the board cannot subsequently be held accountable.

B. Reasons for Caution

Nonetheless, there are still reasons for boards to give additional attention to the data privacy domain. The data privacy sphere differs from prior data breach litigation in significant and potentially powerful ways. First and foremost, current data privacy laws—including both GDPR and the CCPA—have concrete, formalized requirements that put boards on notice concerning what is expected of the corporation. This regime contrasts markedly from cybersecurity law governing data breaches, which remains largely unsettled and amorphous at both the state and federal levels. In fact, U.S. companies frequently express frustration with the lack of explicit guidance concerning their cybersecurity and data protection legal obligations. Although frameworks such as guidelines from the National Institute of Standards and Technology (NIST) provide helpful objectives for companies, these tools are intended merely as

---

[80] *Id.*
[81] *In re The Home Depot*, 223 F. Supp. 3d at 1327.
[82] *Id.*
[83] Palkon v. Holmes, 2014 WL 5341880, at *6 (D.N.J. Oct. 20, 2014).

industry best practices; they are not substantive law.[84] The Target, Home Depot, and Wyndham cases illustrate this point. In all three cases, the plaintiffs made only broad claims of unreasonable board behavior; none pointed to specific violations of positive data security law.[85]

These distinctions are important. As Vice Chancellor Slights recently noted, "Delaware courts are more inclined to find *Caremark* oversight liability at the board level when the company operates in the midst of obligations imposed upon it by positive law yet fails to implement compliance systems, or fails to monitor existing compliance systems, such that a violation of law and resulting liability occurs."[86] He went on to explain, "[i]n other words, it is more difficult to plead and prove Caremark liability based on a failure to monitor and prevent harm flowing from risks that confront the business in the ordinary course of its operations."[87]

This distinction is important because preparing for data breaches looks much more like an ordinary business risk. Although companies can take preparatory measures, they do not know if or when a data extrication attempt might occur. Moreover, there is little in the way of positive law compelling particular actions by a corporation. Instead, companies must act reasonably given their circumstances. On the other hand, there is no question that data privacy laws explicitly obligate certain delineated actions and internal corporate processes. As a result, Delaware courts are presumably more likely to find *Caremark* oversight liability in the data privacy domain.

Additionally, it is worth remembering that these landmark data breach cases were decided prior the Delaware Supreme Court's recent revival of oversight claims in *Marchand*. Delaware corporate law commentators have given considerable weight to the *Marchand* decision and its potential effects on future *Caremark* causes of action. Plaintiffs in both data breach and data privacy cases now have a helpful precedent to rely on in coming years. Only time will tell the full scope and import of the *Marchand* decision, yet there is no doubt that plaintiffs will seek to utilize this favorable precedent to the full extent possible. Accordingly, boards would be well advised to show extra vigilance in fulfilling their oversight duties until they understand *Marchand's* long-term effects on the Delaware corporate litigation landscape. Directors should not be lulled into a

---

[84] U.S. DEP'T OF COMMERCE, NAT'L INSTIT. STANDARDS & TECH. (NIST), *Cybersecurity Framework*, https://www.nist.gov/cyberframework.
[85] *See supra* Part III.
[86] In re Facebook, Inc. Section 220 Litig., No. 2018-0661-JRS, 2019 WL 2320842 at *13 (Del. Ch. 2019).
[87] *Id.*

sense of security by past successes in getting data breach claims dismissed, as the risk of successful derivative actions may be closer than originally thought.

V. PROPOSALS FOR TANGIBLE BOARD ACTION

A. Board Level Committees to Monitor Compliance with Data Laws

In early 2018, news outlets revealed that a British company, Cambridge Analytica, had used a personality quiz app to obtain inappropriately the personal data of millions of Facebook users without consent.[88] In connection with this scandal, Facebook ultimately reached a settlement with the FTC in which the social media giant agreed to a $5 billion civil penalty, the largest ever imposed on a company for violating consumers' privacy.[89]

A major component of this consent order was the requirement that Facebook "create an Independent Privacy Committee of its Board of Directors, with members designated through an independent nominating committee established by Facebook."[90] This committee was to be informed about "all material privacy risks and issues at the company" and has "approval-and-removal authority over a new cadre of designated compliance officers and a third-party assessor that will not answer to Facebook."[91] Put simply, the FTC order obligated Facebook to create a board-level committee to ensure the company's compliance with applicable data privacy rules.

Corporate boards should not, however, wait for the FTC, California Attorney General, Information Commissioner's Office, or other enforcement agency to initiate an action before taking proactive measures. Instead, the Facebook settlement should serve as a signpost to the current boards of Delaware corporations. First and foremost, creating a board-level committee devoted solely to data privacy demonstrates that directors take seriously their legal and regulatory obligations. Such a committee is a conspicuous

---

[88] *See, e.g.*, Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, GUARDIAN (Mar. 17, 2018, 6:03 P.M.), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[89] Leslie Fair, *FTC $5 Billion Facebook Settlement: Record-breaking and History-Making*, FTC BUS. BLOG (Jul. 24, 2019, 8:52 A.M.), *https*://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history.

[90] United States v. Facebook, Plaintiff's Consent Motion for Entry of Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief and Memorandum in Support, (D.D.C. Jul. 24, 2019).

[91] Fair, *supra* note 89.

public indicator that the board is aware of its duties and is not sitting idly by in this domain. In other words, creating this committee represents a board's good faith effort to fulfill its *Caremark* monitoring duties.

Yet the benefits go beyond this public signaling. This is because a privacy committee would naturally conduct the exact types of monitoring required under *Caremark* and its progeny. For instance, under its settlement with the FTC, Facebook agreed that its newly formed Privacy Committee would meet with management to "discuss [Facebook's] assessment of material risks to the privacy, confidentiality, and Integrity of the Covered Information and the steps [Facebook] has taken or plans to take to monitor or mitigate such risks.[92] The committee is likewise responsible for reviewing "procedures and any related policies with respect to risk assessment and risk management." [93] These enumerated activities are prototypical examples of the types of actions and behavior patterns that insulate boards from *Caremark* liability.

These responsibilities can be clearly juxtaposed with the absent board actions that the Delaware Supreme Court found so important in *Marchand*. There, Chief Justice Strine emphasized that the complaint alleged "no regular process or protocols that required management to keep the board apprised of food safety compliance practices, risks, or reports existed."[94] This missing dialogue with management was key. Had the board communicated with top management, they likely would not only have met their duties under *Caremark*, but they also would have been made aware of crucial red flags at the company's factories, and given the opportunity to take mitigating steps to prevent the outbreak. By creating a board-level committee explicitly tasked with interfacing with management about data privacy and other related issues, corporate boards take a significant step towards avoiding Blue Bell Creamery's pitfalls.

Finally, it is worth noting that the FTC consent requires that all members on the Facebook Privacy Committee be independent directors from outside the company.[95] Though this is the gold standard, this level of separation from the board is likely not required in other contexts. Facebook's settlement with the FTC came in the wake of a violated earlier FTC decree and the fallout from the Cambridge Analytica scandal, which saw the unapproved distribution of information from millions of its users. Nevertheless,

---

[92] United States v. Facebook Inc,, Stipulated Order for Civil Penalty, Monetary Judgment and Injunctive Relief, at 23 (D.D.C. Jul. 24, 2019).
[93] *Id.*
[94] Marchand v. Barnhill, 212 A.3d 805, 822 (Del. 2019).
[95] United States v. Facebook Inc,, Stipulated Order for Civil Penalty, Monetary Judgment and Injunctive Relief, at 30 (D.D.C. Jul. 24, 2019).

it is crucial that all board members selected for the committee, whether inside or outside directors, are capable of critically engaging in the privacy compliance discussions. As the Facebook order states, any director on the Privacy Committee must have the ability to "understand corporate compliance and accountability programs and to read and understand data protection and privacy policies and procedures."[96]

B. Data Privacy Education and Issues Training

A board-level privacy committee helps ensure reliable communication with management and serves as an instrument to monitor compliance measures being implemented within the company. Still, this committee does not absolve the *Caremark* responsibilities of the full board. This point is especially salient in an area such as data privacy, which is characterized by a rapidly shifting regulatory landscape. To ensure *Caremark* duties are met, boards should initiate regular education programs to inform themselves on applicable privacy requirements and how companies can address them. Ideally, this education should also include ideas on how to structure and operate effective compliance programs in this domain. These education sessions can be led by internal company experts such as a Chief Privacy Officer, or by external professionals who specialize in data privacy compliance.[97]

Such programs also display a board's intent to stay up to date on new data privacy rules such as the CCPA or GDPR. In doing so, these trainings once again evince the board's good faith efforts to serve as effective supervisors of the company's reporting and compliance systems. In *Marchand*, "the board meetings [were] devoid of any suggestion that there was any regular discussion of food safety issues."[98] By inserting consultations with internal or external specialists into scheduled board meetings, directors can ensure they are adequately staying abreast of key issues. It is worth reiterating that directors are by no means necessarily held accountable if "illegal or harmful activities" evade the compliance systems.[99] It is only important for liability purposes that directors made good faith efforts to implement and monitor reasonable compliance systems at the outset.

C. Conduct Audits of Data Privacy Reporting and Monitoring Systems

Audits of reporting and monitoring systems, whether

---

[96] *Id.* at 12.
[97] Examples of outside experts offering these advisory services include consulting firms such as KohnReznick, Gartner, and IBM, among others.
[98] *Marchand*, 212 A.3d 805, 822 (Del. 2019).
[99] *Id.* at 821.

conducted with internal personnel or contracted through a third-party, are a common method for checking the effectiveness of these *Caremark* mandated systems. Though common, such audits potentially offer an especially powerful tool in the data privacy domain. This is because few areas of law have gone through such extensive transformations in such a short period of time. Additionally, the global aspect of data privacy issues necessarily entails complicated technological and people networks. As a result, auditing GDPR and CCPA compliance systems can fully ensure that these systems meet expectations and provide adequate methods of reporting problems up the chain of command.

CONCLUSION

The application of *Caremark* oversight duties to data privacy issues does not require novel or sweeping changes in the boardroom. Instead, *Caremark* demands only that boards appropriately acknowledge the heightened duties associated with new data privacy regimes and respond accordingly. While boards are not expected to categorically prevent issues from arising, they must ensure that problems can be located and remediated when they do occur.

To date, no court decisions have directly weighed in on *Caremark* liability resulting from a violation of the CCPA or the GDPR. However, data breach case precedents indicate that courts are likely unsympathetic to such *Caremark* claims filed against corporate boards. So long as boards undertake good faith efforts to implement reporting and monitoring systems addressing these new legal regimes, they would almost certainly be absolved of any *Caremark* liability. Nevertheless, the CCPA and the GDPR are affirmative legal regimes that make specific demands on corporations operating in their jurisdictions. As a result, boards should recognize that Delaware courts could be inclined to acquiesce to *Caremark* claims in such positive law settings.

Accordingly, corporate boards should take practical steps towards insuring that their companies have adequate reporting and monitoring systems in place. These measures include board-level data privacy committees, regular education programs, and audits of current systems. In taking these steps, directors can fulfill their fiduciary duties to the company, promote the continued operational integrity of their corporation, and serve as leaders of corporate governance in a crucial but rapidly changing area of the law.