Directors' *Caremark* Liability for Fraudulent Disclosures to Customers about the Company's Cybersecurity: *SolarWinds* Reconsidered

Jennifer Arlen*

To date, Caremark *cases against directors for corporate trauma arising from woefully deficient cybersecurity have failed, even when cybersecurity was a mission critical risk for the company because, as explained in* SolarWinds*,* Caremark *requires a legal violation, and inadequate cybersecurity generally does not violate positive law. This Article shows that* Caremark *claims to recover for corporate trauma from cyber-events can succeed in an important class of cases: when (1) the company made unlawful materially misleading statements to private and public sector customers about its cybersecurity quality; (2) lying to customers about cybersecurity constituted a mission critical legal risk because, given the nature of the company's product, customers' willingness to deal with the firm depends on their confidence that the company has good cybersecurity, confidence which would be shattered by the confluence of a breach and disclosure that the company mislead its customers; (3) directors knowingly did not satisfy their* Marchand/Caremark *duties relating to cybersecurity disclosure; and (4) the company suffered corporate losses (including from government enforcement actions for customer lies that reached shareholders) proximately caused by the company's misleading statements to consumers. This Article elucidates the potential scope of* Caremark *liability for materially misleading cybersecurity disclosure and shows that had the derivative plaintiffs in* SolarWinds *sought recovery for the corporate trauma caused by SolarWinds' misleading disclosure they likely would have prevailed. The framing identified in this Article also should be applicable for corporate traumas arising from safety violations by companies that lied about product safety.*

* Norma Z. Paige Professor of Law, Faculty Director of the Program on Corporate Compliance and Enforcement, NYU School of Law. I would like to thank Samuel Buell; Joseph Facciponti; Jill Fisch; Gurbir Grewal; Robert Lee Hotz; Vikramaditya Khanna; Jonathan Macey; Randy Milch; Elizabeth Pollman; Hilary Sale; Roy Shapira; Leo Strine, Jr.; Justice Karen Valihura; Jonathan Zytick; and participants at the 50th Anniversary Symposium of the *Journal of Corporate Law*; the Harvard Business School Compliance Roundtable; and the 2024 NYU Corporate Governance & Finance Roundtable: *Caremark*/*Marchand*: Where Are We? Where are We Going, for their helpful discussions and comments. I also would like to thank my research assistants, Cole Fanning-Haag, Liam Kim, and Spencer Nelson.

I. INTRODUCTION

Malicious cyber-events pose a substantial threat to companies, their shareholders and customers, and society at large.[1] These attacks can be deterred by effective cybersecurity. Companies and directors need strong incentives to implement the measures needed. Market forces can help provide such incentives when a company's cybersecurity is material to its customers' welfare but only if companies with deficient cybersecurity do not lie to their customers about the quality of their cybersecurity systems.[2] State and federal law prohibits companies from making materially misleading statements to customers and also false statements and false claims to government authorities with whom they deal.[3] But corporate liability for such statements does not suffice to adequately deter companies from violating

1. *See infra* notes 66–79 and accompanying text.

2. *See generally* Steve Shavell, *Strict Liability Versus Negligence*, 9 J. LEGAL STUD., Jan. 1980, at 1, 5 (describing how companies operating in perfectly informed markets will invest optimally in due care to protect consumer safety); Jennifer Arlen, *Economics of Tort Law*, *in* THE OXFORD HANDBOOK OF LAW AND ECONOMICS: VOLUME 2: PRIVATE AND COMMERCIAL LAW 41, 72–76 (2017) (describing the same result of optimal investment except when contracting problems, such as free-rider and adverse selection, impact private markets).

3. *See infra* Part III.B.

the law, as a result of both managerial agency costs and inadequate detection and sanctioning of corporate misconduct.[4] Directors, who hold the keys to compliance, need to be induced to take affirmative actions to counter-act managerial agency costs by asserting active oversight over both their company's compliance with its legal obligation not to mislead customers about cybersecurity quality and its market imperative to provide the cybersecurity quality customers require.[5]

This Article shows that Delaware's *Caremark* doctrine[6] has the potential to provide directors with such incentives, by imposing duties on them to exert effective oversight over the veracity of the company's statements concerning cybersecurity quality to consumers and government authorities, enforced through the threat of liability should their knowing breach of their duties cause corporate trauma from the confluence of corporate frauds, false statements or false claims about cybersecurity quality and a malicious cyber-event resulting from the firm's cybersecurity deficiencies. By providing directors with personal incentives to oversee the veracity of the company's statements about cyber security quality, *Caremark* helps to counter-act both managerial agency costs and corporate liability's under-deterrence problem,[7] thereby potentially benefiting the company, its shareholders, and society at large through improved corporate veracity and stronger incentives to adopt effective cybersecurity.[8] Corporate trauma potentially recoverable through such actions includes government enforcement and private actions resulting from the firm's misstatements to customers and government authorities, including claims for securities fraud predicated on such statements; and the corporate harm from both decreased sales triggered by customer flight and any regulatory intervention (such as exclusion) proximately caused by the confluence of the company's unlawful materially misstatements to customers and the cyber-event.

This Article offers a new path forward to using *Caremark* liability to induce directors to assert better oversight over cybersecurity that addresses a central limitation with the standard approach to *Caremark* cybersecurity cases. To date, derivative plaintiffs have predicated their cybersecurity-related *Caremark* cases on corporate trauma resulting from directors' inadequate oversight of the cybersecurity system itself,[9] even when the company

4. Jennifer Arlen, *Evolution of Director Oversight Duties and Liability Under Caremark: Using Enhanced Information-Acquisition Duties in the Public Interest*, *in* RESEARCH HANDBOOK ON CORPORATE LIABILITY 194, 203–04 (Martin Petrin & Christian Witting eds., 2023).

5. For a discussion of why *Caremark* liability is needed to induce companies to comply with their legal duties, see *id.* (*Caremark* is needed to address externalities and agency costs that can lead to both deliberate misconduct and inadequate compliance); *see also* Roy Shapira, *Conceptualizing* Caremark, 100 IND. L.J. 467, 467 (2025) (same).

6. *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 970 (Del. Ch. 1996).

7. Arlen, *supra* note 4, at 197.

8. *See infra* Part II.A (discussing why *Caremark* is needed); Arlen, *supra* note 4.

9. *See generally* Constr. Indus. Laborers Pension Fund v. Bingle, No. 2021-0940, 2022 WL 4102492 (Del. Ch. Sept. 6. 2022); *see also* Firemen's Ret. Sys. of St. Louis *ex rel.* Marriott Int'l, Inc. v. Sorenson, No. 2019-0965, 2021 WL 4593777, at *14 (Del. Ch. Oct. 5, 2021).

also appears to have made materially misleading statements to customers about its cybersecurity.[10] Delaware courts consistently dismiss these claims.[11] *Caremark* liability generally only applies to claims for corporate traumas resulting from legal violations and most companies are not legally required to adopt effective cybersecurity measures.[12] As a result, in *SolarWinds*, the Delaware court dismissed the *Caremark* case against the board, notwithstanding evidence that the company was harmed by its allegedly woefully inadequate cybersecurity, because plaintiffs did not establish that the company's inadequate cybersecurity violated positive law.[13] Yet while the company's cybersecurity itself arguably did not violate the law, the company did allegedly violate the law by making materially misleading statements to business and government customers about the quality of its cybersecurity, misleading them about cybersecurity deficiencies that allegedly enabled the malicious cyber-event.[14]

This Article elucidates the contours of directors' *Caremark* liability to show when directors of companies that made materially misleading statements to private or public customers[15] risk *Caremark* liability for corporate trauma arising from the confluence of these unlawful statements and a cyber-event attributable to significant deficiencies in the companies' cybersecurity, when directors failed to exert the requisite oversight over the veracity of the company's cybersecurity disclosure. Companies that suffer the greatest harm from cyber-events tend to be those whose cyber-deficiencies could lead business or government customers to suffer substantial harm, potentially resulting in customer flight following a cyber-event. They also tend to be those with deficient cyber-security.[16] Business and government customers dealing with firms whose cybersecurity could harm them regularly require companies to attest to the quality of their cybersecurity practices; companies

10. *See, e.g.*, SEC v. SolarWinds Corp., 741 F.Supp. 3d 37 (S.D.N.Y. 2024) (predicating an enforcement action on SolarWinds' alleged materially misleading statements to its customers (including government agencies) about its cybersecurity; statements that also were allegedly material to customers).

11. *Bingle,* 2022 WL 41024929, at *14; *Marriott*, 2021 WL 4593777, at *19.

12. Most cybersecurity deficiencies do not violate the law because the U.S. generally does not require companies to implement specific protections. Nevertheless, a growing number of states do impose specific cybersecurity requirements on firms. For example, financial institutions and insurance companies regulated by the New York Department of Financial Services are required to adopt certain specific cybersecurity practices, including multi-factor identification and encryption. Cybersecurity Requirements for Financial Services Companies, 23 NYCRR §§ 500.12, 500.15. The NY Shield Act requires firms to develop and maintain "reasonable safeguards to protect the security, confidentiality, and integrity of private information" and provides a list of specific cybersecurity features which a firm can take to guarantee it is in compliance. N.Y. GEN. BUS. LAW § 899-bb (2024).

13. *Bingle*, 2022 WL 4102492, at *1.

14. *SolarWinds*, 741 F.Supp. 3d at 79–80 (identifying unlawful materially misleading statements to customers that reached shareholders).

15. This Article focuses on materially misleading statements to consumers, and not fraud on shareholders, because *Caremark* only provides directors with significant incentives to exert effective oversight over disclosure with respect to those legal risks that are mission critical risks. *See, e.g.*, Arlen, *supra* note 4; *see also* Jennifer Arlen, *The Story of* Allis-Chalmers*,* Caremark*, and* Stone*: Directors' Evolving Duty to Monitor*, *in* CORPORATE STORIES 323 (J. Mark Ramseyer ed., 2009) (concluding that *Caremark*'s original formulation—pre-*Marchand*—set forth a standard of care that is too vague to induce directors' to exert effective oversight under a bad faith standard of liability). As explained later, fraud on consumers can constitute a mission critical risk. By contrast, fraud on shareholders, unconnected to fraud on consumers or other counter-parties (such as lenders), rarely should lead to the type of long-run harm to the firm apparently required for a mission critical risk determination. *See infra* note 111.

16. *See infra* Part III.

anticipate this and publish such attestations on their websites. Such companies often can only retain customers by either implementing effective cybersecurity that complies with their public pronouncements or lying to their business and government customers by making material misstatements about the company's compliance with cybersecurity best practices.[17] While the deficient cybersecurity itself regularly is not unlawful, knowing materially misleading statements to consumers and knowing false statements or false claims to government authorities are illegal.[18] In such cases, derivative plaintiffs may have a valid *Caremark* claim against the board for corporate trauma resulting from these unlawful materially misleading statements, should evidence reveal that directors failed to exert the requisite oversight over the company's compliance with legal prohibitions on materially misleading statements to consumers and such statements were a proximate cause of corporate trauma resulting from the cyber-event.

Caremark does not create a genuine threat of director liability for all corporate materially misleading statements to consumers relating to cybersecurity, however. *Caremark* only creates a genuine threat of liability in the narrow set of circumstances where *Caremark* imposes specific, discretion-constraining duties on directors to oversee the specific legal risk in question. *Caremark* only imposes such specific oversight duties in a narrow set of circumstances: when violating the law in question could cause harms that create a "mission critical risks" to the firm.[19] Thus, *Caremark* cybersecurity cases for inadequate oversight over the veracity of the company's cybersecurity disclosures generally will be limited to situations where defrauding customers about the company's cybersecurity constituted a mission critical risk.

Examining the cases, this Article concludes that mission critical legal risks are those that could cause harms that threaten the firm's long-run value, generally by reducing future earnings. Delaware courts regularly categorize legal risks as mission critical when the legal violation could lead to sufficiently serious consumer harm to trigger ruinous customer flight[20] or damaging intervention by a regulator that curtail future sales, (e.g., through plant closings, delicensing, debarment or exclusion).[21]

Corporate materially misleading about cybersecurity to business and government customers who could be egregiously harmed by deficient cybersecurity often will constitute a mission critical risk as such lies could trigger customer flight following a cyber-event if customers conclude they cannot trust the firm; in some cases, regulators may intervene as well.[22] In these circumstances, *Caremark* imposes actionable duties on directors, requiring them to (1) ensure that the company has systems to verify the accuracy of its cybersecurity disclosures, (2) expressly allocate oversight over cybersecurity disclosures to a specific

17. *E.g.*, *Bingle*, 2022 WL 4102492, at *4.

18. *See infra* Part III (discussing the relevant laws).

19. *See infra* Part II; Arlen, *supra* note 4, at 198 (explaining why directors generally cannot be held liable for breach of their oversight duties under *Caremark*'s original formulation). For a discussion of the limitation of *Caremark* when violations are not a mission critical risk, see Arlen, *supra* note 15, at 323.

20. *See e.g.*, Marchand v. Barnhill, 212 A.3d 805 (Del. 2019). For a discussion of when corporate misconduct is likely to trigger customer flight, see generally Cindy R. Alexander & Jennifer Arlen, *Does Conviction Matter? The Reputational and Collateral Effects of Corporate Crime*, *in* RESEARCH HANDBOOK ON CORPORATE CRIME AND FINANCIAL MISDEALING 87–147 (Jennifer Arlen ed., 2018).

21. *See e.g.*, *Marchand*, 212 A.3d at 807–09; *In re* Boeing Co. Derivative Litig., No. 2019-0907, 2021 WL 4059934, at *26 (Del. Ch. Sept. 7, 2021); *see infra* Part II.C.

22. *See infra* Part III.B.

unit of the board; (3) establish procedures that require management to report cyber disclosure compliance system deficiencies and detected materially misleading statements to the board and ensure management in fact does report, and (4) assert active oversight over investigating suspected violations and terminate confirmed violations.[23] Thus, directors can by liable under *Caremark* even when they regularly receive brief reports on the company's cybersecurity if directors fail to comply with these duties, for example, by failing to require management to inform the board about any material deviations between the company's statements to customers about its cybersecurity and its actual systems. In such situations, directors would face potential liability for all corporate harm proximately caused by the unlawful statements, including government enforcement and private class actions arising from such statements (including securities fraud actions if predicated on misleading statements aimed at consumers that also reached shareholders), as well as harm from lost revenues resulting from customer flight, and, potentially, regulatory interventions such as delicensing or exclusion.

This Article is organized as follows. Section 2 examines the structure of Delaware's *Caremark* doctrine to identify which legal risks Delaware is likely to deem to be mission critical risk and what duties are imposed on directors in these circumstances. It then explains why directors in the *SolarWinds* case were not held liable under *Caremark* even though the court concludes that inadequate cybersecurity was a mission critical risk. Section 3 shows that *Caremark* liability can be predicated on a corporation's materially misleading statements to consumers about their cybersecurity quality when such misleading disclosures constitute a mission critical risk. Section 4 then reexamines *SolarWinds* and finds that the derivative plaintiffs likely could have prevailed had they based their case on directors' breach of their oversight duties to deter unlawful materially misleading statements to consumers and the government about the company's cybersecurity.

II. DIRECTORS' OVERSIGHT LIABILITY UNDER CAREMARK

This Section sets forth Delaware law on directors' liability for inadequate oversight of legal compliance. It shows that *Caremark* generally only potentially provides directors with significant incentives to oversee legal compliance with those laws whose violation could cause harms that constitute a mission critical legal risk for the company (hereinafter *Caremark 2.0*). This Section then identifies the prerequisites to mission critical risk status. It shows that for many firms, deficient cybersecurity does create a mission critical risk but nevertheless does not trigger *Caremark* liability because inadequate cybersecurity rarely violates positive law, as was the case with *SolarWinds*.

A. Directors' Liability Under Caremark *for their Company's Legal Violations*

Governments cannot rely entirely on corporate and individual-wrongdoer criminal liability to deter corporate crime. Directors also must be held liable if they knowingly allow their companies to violate the law. They also must be subject to duties designed to promote compliance and held personally liable if they utterly neglect these duties in bad faith.[24]

23. *See Marchand*, 212 A.3d at 809, 821–22; *Boeing*, 2021 WL 4059934, at *33; *see also* Arlen, *supra* note 4.

24. Arlen, *supra* note 4, at 209.

Directors' liability is required to address two problems plaguing deterrence through corporate criminal liability: under-deterrence and agency costs. Corporate liability does not adequately deter companies because corporate crime is detected and sanctioned so infrequently that many companies can profit from violating the law.[25] Moreover, companies may violate the law, even when they do not profit from misconduct, as a result of managerial agency costs. These can arise if managers can benefit from either misconduct or reduced compliance expenditures.[26] Properly designed, *Caremark* oversight liability can ameliorate both problems by causing directors to internalize costs of misconduct and inadequate compliance, thereby motivating them to cause the firm to deter, and terminate, corporate crime.[27]

Delaware adopted its *Caremark* doctrine to enhance directors' incentives to deter corporate misconduct. Yet *Caremark*'s original formulation did little to achieve these goals.[28] Traditional *Caremark* imposes four duties on directors relating to their company's compliance with the law. First,[29] directors may not knowingly allow their firm to violate the law and, upon discovering a legal violation, directors must intervene to terminate it (*Massey* Claim).[30] Second, directors[31] must adopt policies and procedures to deter legal violations,

25. *Id.*; Shapira, *supra* note 5, at 509–12; *cf.* Eugene F. Soltes, *The Frequency of Corporate Misconduct: Public Enforcement Versus Private Reality*, 26 J. FIN. CRIME 923, 924–26 (2019) (presenting evidence of firms committing hundreds of undetected violations a year); Jennifer Arlen & Lewis A. Kornhauser, *Battle for Our Souls: A Psychological Justification for Corporate and Individual Liability for Organizational Misconduct*, 2023 U. ILL. L. REV. 673, 728–29 (arguing legal norms alone do not suffice to deter corporate misconduct that benefits companies and their employees, managers, and directors).

26. Arlen, *supra* note 4; *cf.* Jennifer H. Arlen & William Carney, *Vicarious Liability for Fraud on Securities Markets: Theory and Evidence*, 1992 UNIV. ILL. L. REV. 691, 691 (finding securities fraud generally arises from agency costs); Cindy R. Alexander & Mark A. Cohen, *Why Do Corporations Become Criminals? Ownership, Hidden Actions, and Crime as an Agency Cost*, 5 J. CORP. FIN., Mar. 1999, at 1, 1 (providing evidence that corporate crime is positively correlated with agency costs).

27. For a more detailed discussion, see Arlen, *supra* note 4, at 215 (explaining how *Caremark 2.0* deters by inducing directors to have the firm produce, and obtain, information about compliance failures and misconduct, information they must act on if it reveals the firm violated the law).

28. *Id.*; Arlen, *supra* note 15 (discussing *Caremark*'s original formulation).

29. *Massey* claims technically are not *Caremark* claims because the prohibition on knowing legal violations pre-dates *Caremark*. Nevertheless, Delaware courts regularly place *Massey* claims under the *Caremark* umbrella.

30. Directors cannot rely on the Business Judgement Rule to justify knowing corporate misconduct—even when the firm expects to profit from it—because Delaware law requires corporations to seek profit within the bounds of the law. *See, e.g.*, Arlen, *supra* note 4, at 203–04; Kent Greenfield, *Ultra Vires Lives! A Stakeholder Analysis of Corporate Illegality (with Notes on How Corporate Law Could Reinforce International Law Norms)*, 87 VA. L. REV. 1279, 1281–82, 1316 (2001); Elizabeth Pollman, *Corporate Disobedien*ce, 68 DUKE L.J. 709, 726–27 (2019) (prohibiting companies from violating the law enhances corporate law's legitimacy); Leo E. Strine, Jr. et al., *Loyalty's Core Demand: The Defining Role of Good Faith in Corporation Law*, 98 GEO L. REV. 629, 648–53 (2010); La. Mun. Police Emples. Ret. Sys. v. Pyott, 46 A.3d 313, 352 (Del. Ch. 2012) (noting directors who cause the company to violate the law are disloyal and liable for the harm they cause); *In re* Massey Energy Co. Derivative & Class Action Litig., No. 5430, 2011 WL 2176479, at *21 (Del. Ch. May 31, 2011); Metro Commc'n Corp. BVI v. Advanced Mobilecomm Techs. Inc., 854 A.2d 121, 131 (Del. Ch. 2004) ("Under Delaware law, a fiduciary may not choose to manage an entity in an illegal fashion, even if the fiduciary believes that the illegal activity will result in profits for the entity."); Guttman v. Jen-Hsun Huang, 823 A.2d 492, 506 n.34 (Del. Ch. 2003) ("[O]ne cannot act loyally as a corporate director by causing the corporation to violate the positive laws it is obliged to obey.").

31. *In re* Caremark Int'l Inc., 698 A.2d 959, 967 (Del. Ch. 1996); *see generally* Arlen, *supra* note 4. *Caremark* duties also extend to officers, see *In re* McDonald's Corp. S'holder Derivative Litig., 289 A.3d 343, 362–

including an information and reporting system designed to detect violations and transmit the information to senior management and the board (hereinafter a compliance function) (*Caremark* Prong 1).[32] Third, directors must exert on-going oversight of the company's compliance with the law by periodically obtaining information about compliance (*Caremark* Prong 2a). Finally, upon the discovery of red flags, directors must ensure the company investigates suspected misconduct (which triggers their duty to terminate misconduct should it be detected) (*Caremark* Prong 2b).[33] Directors who intentionally or utterly neglected these duties face liability for harm their lack of oversight proximately caused their company—including for investigation costs, sanctions, private liability, and reputational harm.[34]

Yet these *Caremark* duties do not provide directors with meaningful incentives to improve or effectively oversee their companies' compliance functions.[35] The duties themselves only require the bare minimum of directors—specifically to (1) adopt *some form* of compliance function; (2) provide *some relatively minimal* oversight over it (even if only over the policies or training); and (3) ensure the company responds in some way to detected misconduct. Directors retain full discretion to determine how to satisfy these minimal duties. Directors who do the bare minimum (ostensibly in good faith) are insulated from liability by the Business Judgement Rule, even if the board adopted a compliance function which did not require management to promptly report compliance deficiencies and serious detected misconduct to the board, did not ask management about whether the firm might be violating the law, and passively oversaw investigations of misconduct, relying on senior management.[36]

B. Caremark *2.0 Oversight Duties for Mission Critical Risks*

Recognizing the deficiencies with *Caremark*'s original formulation, Delaware subsequently revised *Caremark* to impose explicit substantive oversight duties on directors—duties that curtail the discretion they otherwise would enjoy under the Business Judgement Rule to decide for themselves what information to obtain and how active to be. Yet cognizant of the need not to overly circumscribe the Business Judgement Rule, Delaware limited these heightened requirements to the situations where a legal violation could directly or

64 (Del. Ch. 2023), but is less likely to be effective because officers often will enjoy the protection of the demand requirement. *See id.* at 359.

32. *Caremark*, 698 A.2d at 970; Stone v. Ritter, 911 A.2d 362, 368 (Del. 2006). A company's compliance program is a subset of the measures companies must take to deter corporate misconduct. The full set of measures constitute a company's compliance function. *See generally* Jennifer Arlen, *The Compliance Function*, *in* THE OXFORD HANDBOOK OF CORPORATE LAW AND GOVERNANCE (Jeffrey N. Gordon & Wolf-Georg Ringe eds., 2d ed. 2025).

33. *Stone*, 911 A.2d at 370; Arlen, *supra* note 2, at 23.

34. *Caremark*, 698 A.2d at 970.

35. Arlen, *supra* note 4; Arlen, *supra* note 15.

36. Arlen, *supra* note 4; *See, e.g.*, *Stone*, 911 A.2d at 372–73 (dismissing a *Caremark* action against the board of a bank that implemented a deficient anti-money laundering compliance program). Directors could face oversight liability if a federal law imposed more specific duties on directors and they utterly neglected those duties. *E.g.*, *In re* China Agritech, Inc. S'holder Derivative Litig., 2013 WL 2181514 (Del. Ch. May 21, 2013) (*Caremark* claim against audit committee survives motion to dismiss which did not meet for over two years).

indirectly cause corporate harm that constitutes a "mission critical legal risk" (MCLR) (hereinafter *Caremark 2.0*).[37]

Specifically, when a company faces a mission critical legal risk, *Caremark 2.0* imposes enhanced duties on directors at three different points in time: (1) ex ante, when the directors implement structures governing their oversight of the company's compliance function (Prong 1); (2) after the compliance program is established, through on-going director oversight of the compliance function (Prong 2a); and (3) once any potential material misconduct is detected and brought to the board's attention (Prong 2b).[38] These duties are all designed to push information about compliance deficiencies and detected misconduct from management to the board, thereby enhancing the probability that the board promptly learns about mission critical risk violations, triggering its duty to terminate it.[39]

Specifically, *Caremark 2.0* Prong 1 requires directors to adopt a compliance program that both designates which unit of the board is responsible for overseeing a mission critical risk and requires management to report to that unit on compliance deficiencies and suspected violations of the mission critical legal risk.[40] *Caremark 2.0* Prong 2a requires the responsible unit of the board to actually exercise oversight—reserving time to learn about, and ensuring that management reports on, deficiencies in the company's compliance function and suspected violations of the mission critical risk.[41] *Caremark 2.0* Prong 2b governs directors' oversight duties once the company learns it may have violated a covered law (red flag).[42] Directors must assert direct oversight over the company's investigation and ultimate response and cannot simply delegate to management.[43] Each of these duties circumscribes the Business Judgement Rule by requiring directors to obtain information and assert oversight over matters they might otherwise have delegated to management.

Boards subject to these *Caremark 2.0* duties can face a genuine risk of liability under *Caremark*. *Caremark*'s bad faith standard for director liability provides less insulation to directors given the specificity of the oversight duties imposed. Directors who could evade liability under *Caremark 1.0* through cursory attention to compliance policies and procedures[44] cannot evade liability under *Caremark 2.0* if the board failed to devise systems and

---

37. *See generally* Marchand v. Barnhill, 212 A.3d 805 (Del. 2019); Teamsters Local 443 Health Servs. & Ins. Plan v. Chou, No. 2019-0816, 2020 Del. Ch. LEXIS 274 (Del. Ch. Aug. 24, 2020); *In re* Clovis Oncology, Inc. Derivative Litig., No. 2017-0222, 2019 WL 4850188 (Del. Ch. Oct. 1, 2019); *In re* Boeing Co. Derivative Litig., No. 2019-0907, 2021 WL 4059934 (Del. Ch. Sept. 7, 2021); *In re* Wal-Mart Stores, Inc. Del. Derivative Litig., No. 7455, 2016 WL 2908344 (Del. Ch. May 13, 2016). For a justification of these enhanced duties, see Arlen, *supra* note 4.

38. *E.g.*, *Marchand*, 212 A.3d at 813; *Boeing*, 2021 WL 4059934, at *24. Delaware courts generally refer to *Caremark* Prong 1 and Prong 2 duties. This discussion separates Prong 2 into two separate duties because Delaware's Prong 2 both looks at what steps directors took to engage in on-going oversight over the firm's compliance with the mission critical risk, prior to any detected misconduct, and what they did to respond to red flags. *Id.*; *see generally* Arlen, *supra* note 4.

39. Arlen, *supra* note 4.

40. *E.g.*, *Marchand*, 212 A.3d at 821; *Chou*, 2020 Del. Ch. LEXIS 274, at *48–51; *Clovis Oncology*, 2019 WL 4850188, at *13; *Boeing*, 2021 WL 4059934, at *26; *Wal-Mart Stores*, 2016 WL 2908344, at *6–7. For a justification of these enhanced duties, see Arlen, *supra* note 4.

41. *E.g.*, *Marchand*, 212 A.3d at 809; *Boeing*, 2021 WL 4059934, at *25. *See generally* Arlen, *supra* note 4.

42. *See Boeing*, 2021 WL 4059934, at *1.

43. *Id.* at 29; Arlen, *supra* note 4.

44. *E.g.*, Stone v. Ritter, 911 A.2d 362, 364–65 (Del. 2006); *Marchand*, 212 A.3d at 823–24.

require management to report to them on compliance deficiencies and suspected violations of mission critical risks.[45]

Caremark 2.0 should enhance director oversight over these risks and, most importantly, increase the probability that information about compliance weaknesses and harms from mission critical legal risks reaches the board.[46] This information-producing and channeling impact of *Caremark 2.0* should help deter violations by shifting control from managers—who are more likely to obtain private benefits from misconduct or face termination, demotion, or sanction as a result of its revelation—to directors, who have less to lose from revelation of misconduct and who face personal liability under the *Massey* Prong of *Caremark* if they fail to terminate it.[47]

C. Identifying Mission Critical Legal Risks

Delaware courts have not yet specified what type of legal violations constitute mission critical risks. While many cases involve legal violations by heavily regulated companies that did or could have killed people, Delaware has applied *Caremark 2.0* duties in other circumstances as well.

The cases suggest that Delaware judges have restricted *Caremark 2.0* duties to those legal violations that risked such enormous harm to the company that directors simply could not ignore them, in an effort to avoid excessive interference with directors' Business Judgement Rule discretion. Examining the cases, it appears that the critical question is whether the failure to prevent the category of legal risk in question could cause egregious long-term harm to the firm. The cases generally entail harms from legal violations whose discovery could substantially reduce the firm's future revenues, either because of reputational damage or through regulatory intervention, such as delicensing, product recalls, debarment or exclusion.[48] Legal risks that threaten to substantially reduce corporate revenues for many

45. *E.g.*, *Marchand*, 212 A.3d at 821; *Boeing*, 2021 WL 4059934, at *1.

46. A mission critical risk finding is vital to oversight cases, but not *Massey* claims, because plaintiffs can prevail in a *Massey* claim against a board (or officer) who knowingly allowed the company (or an employee) to violate the law regardless of whether the legal risk is mission critical. *See generally In re* Massey Energy Co. Derivative & Class Action Litig., No. 5430, 2011 WL 2176479 (Del. Ch. May 31, 2011); *see also In re* McDonald's Corp. S'holder Derivative Litig., 289 A.3d 343 (Del. Ch. 2023) (*Caremark* violation from the head of HR's deliberate failure to stop known sexual harassment, including by himself).

47. Arlen, *supra* note 4.

48. *Id.* Delaware appears to have a second implicit: that deterrence of the harm from the legal risk is important to society, as evidenced by extensive regulations (and oversight) or special enforcement initiatives aimed at deterring the risk. *Id.* Absent this requirement, Delaware courts seeking to determine whether a legal risk presented such a threat to the firm that directors could not possibly ignore it in good faith would examine not only the harm should a violation occur, but also the probability that it would occur and be detected and the costs of deterring the harm. When considering potential regulatory responses, they also would consider the likelihood that the regulator would in fact impose serious consequences. *Cf.* Teamsters Local 443 Health Servs. & Ins. Plan v. Chou, No. 2019-0816, 2020 Del. Ch. LEXIS 274 (Del. Ch. Aug. 24, 2020). Yet instead, Delaware judges consistently focus only on the magnitude of the harm, an approach that is consistent with *Caremark 2.0* also seeking to induce directors to deter risks that might profit the firm but that impose serious harms on society that society has expressed a strong interest in deterring. Arlen, *supra* note 4. This is consistent with the view that *Caremark 2.0* is also structured to serve society's interests in corporate compliance with its most important laws. *See, e.g.*, Arlen, *supra* note 4; *but cf.* Ont. Provincial Council of Carpenters' Pension Tr. Fund v. Walton, 2023 WL 3093500, at *49–51 (Del. Ch. Apr. 26, 2023) (expressing doubt about the court's ability to determine which laws protect vital social interests). Moreover, to date almost all *Caremark 2.0* cases involved companies operating in

years not only risk immediate peril but also could render the company unable to fully recover in the future.[49] In making the mission critical risk assessment, Delaware courts assess, but also look beyond, the consequences imposed by law for the category of legal violation.[50] They also consider the long-term consequences to the firm of the harm that can arise from the legal violation (e.g., the reputational harm from products that kill consumers).[51]

Harms from legal violations have been found to constitute a mission critical legal risk in three situations, each of which entails a threat to the firm's long-term welfare. First, when the legal violation causes a sufficiently substantial harm to consumers that revelation of the harm arising from the legal violation[52] would likely cause (and often did cause) many customers to eschew future dealings with the firm.[53] Such customer flight is a mission critical risk if the products implicated by the violation constitute a substantial portion of the firm's profits. Importantly, consumer flight could transform a legal violation into a mission critical risk even if the flight would be triggered by news of the harm (e.g., death) regardless of whether the firm violated the law.[54]

---

heavily regulated industries whose activities could cause serious harm, such as death or serious personal injury. And most entail violations that legislatures deem sufficiently serious to have granted a regulator agency authority to enjoin violators from future risk-creating activities. These activities include through delicensing, debarment, exclusion, production stoppages and product recalls, or other injunctions. *E.g.*, *Marchand*, 212 A.3d at 807 (involving a listeria outbreak that killed many people); *Chou*, 2020 Del. Ch. LEXIS 274, at *4–5 (addressing potentially deadly violations of drug safety); *Walton*, 2023 WL 3093500, at *1 (regulation of opioids); *Boeing*, 2021 WL 4059934, at *1 (regarding plane safety issues); *Clovis Oncology*, 2019 WL 4850188, at *1 (violating clinical trial protocols designed to protect patients); Arlen, *supra* note 4.

49. Thus, it is not enough to show that the firm probably could not pay the legal sanctions that would result from its violation of the law. This limitation is important since otherwise directors of closely held and smaller publicly held corporations would face *Caremark* 2.0 duties with respect to the multitude of federal violations that could trigger fines that exceed their ability to pay. *See* Cindy R. Alexander & Mark A. Cohen, *The Evolution of Corporate Criminal Settlements: An Empirical Perspective on Non-Prosecution, Deferred Prosecution, and Plea Agreements*, 52 AM. CRIM. L. REV. 537, 584–85 n.193 (2015) (noting a significant number of smaller firms cannot pay the fine); Jennifer Arlen, *Corporate Criminal Liability: Theory and Evidence*, *in* RESEARCH HANDBOOK ON THE ECONOMICS OF CRIMINAL LAW 148 (Keith Hylton & Alon Harel eds., 2012) (same); *see also* Nathan Atkinson, *Corporate Liability, Collateral Consequences, and Capital Structure*, 2023 COLUM. BUS. L. REV. 1, 2–3.

50. In determining whether a legal risk could pose such a threat, Delaware judges consider the potential implications for the entire company of failing to prevent the *category of legal violation* in question, as opposed to just the impact on the firm of the specific violation that occurred by the unit of the firm that violated the law. Thus, in *Chou*, the court did not focus solely on whether it was mission critical for the parent to prevent misconduct at the subsidiary guilty of the violation, but rather on whether it was mission critical for the parent, a pharmaceutical company, to ensure that all its operations complies with health and safety regulations given the consequences the regulator could impose on it for failing to do so. *Chou*, 2020 Del. Ch. LEXIS 274, at *14–18.

51. *Id.* at *50–51.

52. Notice that in *Marchand* the court focused on consumer reaction to the harm from the safety violation—death—and not only on the sanctions that directly resulted from the firm violating the law. *See Marchand*, 212 A.3d at 814–15.

53. *E.g.*, *Marchand*, 212 A.3d at 815 (harm to the company substantially resulted from customers' reaction to news that the company's one product, ice cream, killed multiple people); *e.g.*, Alexander & Arlen, *supra* note 20 (companies should suffer harm from reputational damage from criminal settlements when the sanctioned misconduct entailed conduct that harms customers, suppliers or other counter-parties who conclude, based on the available facts, that they would face excessive risk of harm should they deal with the firm in the future).

54. Thus, in *Marchand*, the court determined that the legal risk was mission critical because consumers could be expected to avoid ice cream recently found to have listeria, whether that violated the law or not. *Marchand*, 212 A.3d at 809 (food safety is a mission critical risk because the company "can only thrive if its

Second, a legal violation also can constitute a mission critical risk when it could empower a government agency to either delicense, debar, or exclude the company from markets or consumers vital to it or recall or prevent the sales of products important to its welfare.[55] For example, companies that violate the Federal Food, Drug, & Cosmetic Act, or commit federal health care fraud, or certain False Claims Act violations often risk debarment or exclusion from dealing with Health and Human Services (HHS) and the customers whose care HHS pays for. Indeed, many successful[56] *Caremark 2.0* oversight cases involve legal violations that did or could subject the firm to a regulatory intervention that imperiled future revenues—such as a plant closure,[57] plane grounding,[58] cessation of pharmaceutical drug testing, mandated product recalls and prohibitions on future sales[59] or debarment or exclusion from sales to (or paid for by) federal agencies or programs (such as Medicare or Medicaid).[60]

Finally, and less frequently, Delaware courts have concluded a legal risk was mission critical when harm arising from the legal violation could entail destruction of one of the firm's vital means of production.[61]

When determining whether a legal risk is mission critical, Delaware appears to focus on the *potential* consequences of the risk—both customer loss and regulatory responses—rather than the *expected* consequences, which would take into account the probability that a violation would occur, be detected, and trigger substantial negative consequences. This is consistent with the idea that director oversight is needed to protect companies from the risk of long-term calamity.

D. Causation Requirement

To date, *Caremark* has been restricted to mission critical legal risk—as opposed to business risk. This is a natural consequence of *Caremark*'s proximate cause requirement which requires that the plaintiff show that the board could have prevented the harm had it satisfied its oversight duties.[62] Thus, to prevail in an oversight case, plaintiffs must show

---

consumers . . . were confident that its products were safe to eat."); *see In re* Boeing Co. Derivative Litig., No. 2019-0907 2021 WL 4059934 (Del. Ch. Sept. 7, 2021) (derivative action against Boeing for corporate harm from inadequate oversight of plane safety was filed in September 2020, before government officials filed legal actions against Boeing in January 2021). Yet while a nonlegal harm arising from a legal violation can serve as the basis for a mission critical risk determination, a legal violation nevertheless generally is required to establish proximate cause. *See infra* note 65 and text accompanying notes 63–65.

55. Alexander & Arlen, *supra* note 20, at 128–38.

56. Success is defined by cases where the plaintiff survived a motion to dismiss.

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

58. *Boeing*, 2021 WL 4059934, at *2 (explaining that the 737 Max was grounded and new production stopped until Boeing addressed the problem).

59. *In re* Clovis Oncology, Inc. Derivative Litig., No. 2017-0222, 2019 WL 4850188, at *1 (Del. Ch. Oct. 1, 2019) (explaining that the violation risked end of clinical trial of company's only drug).

60. Ont. Provincial Council of Carpenters' Pension Tr. Fund v. Walton, No. 2021-0827, 2023 WL 3093500, at *1 (Del. Ch. Apr. 26, 2023); Teamsters Local 443 Health Servs. & Ins. Plan v. Chou, No. 2019-0816, 2020 Del. Ch. LEXIS 274, at *5 (Del. Ch. Aug. 24, 2020) (explaining that the cost to ABC overall of failure to comply with health care laws could be debarment).

61. For example, safety violations that destroyed a company's vital oil pipeline were deemed mission critical. Inter-Marketing Grp. U.S.A. Inc., v. Armstrong, No. 2017-0030, 2020 WL 756965 (Del. Ch. Jan. 31, 2020).

62. *In re* Caremark Int'l Inc., 698 A.2d 959, 971 (Del. Ch. 1996). For a discussion of why Delaware properly imposes a proximate cause requirement in *Caremark* cases even though it does not do so in cases arising from

that the board would have detected the legal violation had it complied with its oversight duties and having done so would have terminated the legal violation that caused the company's harm.[63] In the case of legal risk, plaintiffs can establish proximate cause simply by showing that directors would have detected the misconduct had they satisfied their oversight duties.[64] There is no need to prove the board would have terminated the violation once it was detected because they would have been required to do so. By contrast, with business risk, the board, upon discovering the risk, retains business discretion to allow the company to encounter the risk if they rationally expect the firm to profit from it.[65]

E. The Failure of Traditional Caremark 2.0 Cybersecurity Cases

For many companies, inadequate cybersecurity clearly constitutes a mission critical risk,[66] as the Delaware Chancery court recently recognized in *SolarWinds*.[67] Deficient cybersecurity constitutes a mission critical risk because serious cyber-attacks and data breaches generally result from deficient cyber or data security practices and systems,[68] and

board decisions on behalf of the firm that resulted from the board's breach of its fiduciary duties, see Arlen, *supra* note 15.

63. *In re* Caremark, 698 A.2d at 971.

64. Arlen, *supra* note 4, at 205 n.69; H. Justin Pace & Lawrence J. Trautman, *Mission Critical:* Caremark*, Blue Bell, and Director Responsibility for Cybersecurity Governance*, 2022 WISC. L. REV. 887, 947 (noting that *Clovis* emphasizes that positive law violations are vital to *Caremark* claims because they establish the causal nexus between the breach of fiduciary duty and the corporate trauma); Roy Shapira, *A New* Caremark *Era: Causes and Consequences*, 98 WASH. U. L. REV. 1857, 1877–80 (2021); *but cf.* Shapira, *Conceptualizing* Caremark, *supra* note 5, at 485–97 (claiming that *Caremark* duties should extend to business risks that *could* impose disastrous long-run reputational harm without addressing the causation challenges if the company could have profited from the risk and the harm was unlikely to materialize).

65. For *Caremark* cases that require legal risk, and not business risk, see, e.g., Firemen's Ret. Sys. of St. Louis *ex rel.* Marriott Int'l, Inc. v. Sorenson, No. 2019-0965, 2021 WL 4593777 (Del. Ch. Oct. 5, 2021); Constr. Indus. Laborers Pension Fund v. Bingle, No. 2021-0940, 2022 WL 4102492 (Del. Ch. Sept. 6. 2022); *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 126 (Del. Ch. 2009) (noting that "[t]o 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."); Conte v. Greenberg, No. 2022-0633, 2024 WL 413430 (Del. Ch. Feb. 2, 2024). In theory, directors could face *Caremark* liability for bad faith failure to oversee business risk if plaintiffs could show that the directors bad faith breach allowed a business risk that constituted waste, in the sense that the board could not have concluded that the company would benefit from the risk.

66. Pace & Trautman, *supra* note 64, at 891 (cybersecurity is mission critical for virtually all companies).

67. *Bingle*, 2022 WL 4102492, at *1; SEC v. SolarWinds Corp., 741 F. Supp. 3d 37, 82 (S.D.N.Y. 2024); *see Marriott*, 2021 WL 4593777, at *11, *12 (noting that cybersecurity is "an area of consequential risk that spans modern business sectors" and that "corporate harms presented by noncompliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place.").

68. A substantial percentage result from poor cybersecurity hygiene, and not just bad luck. Keman Huang et al., *The Devastating Business Impacts of a Cyber Breach*, HARV. BUS. REV. (May 4, 2023), https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach [https://perma.cc/LN34-QHMM]. Effective cybersecurity also appears to reduce the impact of an attack and enabling a company's stock price to recover more quickly following an incident, unlike those with weak security. *Id.*

moreover occur regularly,[69] causing ruinous harm to companies and their customers.[70] Costs include ransomware payments, investigation costs, remediation costs,[71] private and government-imposed liability, credit-rating downgrades,[72] impaired relationships with sources of capital,[73] and increased insurance costs.[74] The harm to small- and mid-sized companies can be especially catastrophic[75] because many have neither cybersecurity insurance[76] nor sufficient financial wherewithal to survive a significant cyberattack.[77] Large companies also can face ruinous losses from cyber-events that trigger customer flight,[78] corruption/disablement of IT systems,[79] loss of intellectual property, and loss of financial assets, downgrading of the company's credit rating, and impaired relationship with the company's funders.

Yet Delaware courts have consistently rejected *Caremark* claims against directors for inadequate oversight of cybersecurity, even in cases where it appears that deficient cyber-

69. Indeed, one study found that approximately 83% of organizations experienced at least one data breach during 2022. *Id.*

70. Ani Petrosyan, *Average Cost of Data Breach in US from 2006 to 2024*, STATISTA (Oct. 24, 2024), https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach [https://perma.cc/T8U3-DHQV]; Steve Morgan, *Cybercrime to Cost the World $10.5 Trillion Annually by 2025*, CYBER CRIME MAG. (Nov. 13, 2020), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ [https://perma.cc/WQ32-33FX]; Nicodemus, *infra* note 71; Huang et. al, *supra* note 68.

71. Aaron Nicodemus, *Report: Average Data Breach Costs Public Companies $116M*, COMPLIANCE WK. (June 9, 2020), https://www.complianceweek.com/cybersecurity/report-average-data-breach-costs-public-companies-116m/29037.article (on file with the *Journal of Corporation Law*). For example, Facebook spent $5 billion and Equifax spent $2 billion on remediation alone. *Id.*

72. Huang et al., *supra* note 68. In 2018, Moody's announced that it would evaluate companies' cybersecurity practices when assigning credit ratings. Kate Fazzini, *Moody's is Going to Start Building the Risk of a Business-end Hack into its Credit* Ratings, CNBC (Nov. 12, 2018) https://www.cnbc.com/2018/11/12/moodys-to-build-business-hacking-risk-into-credit-ratings.html [https://perma.cc/XZQ7-2F67]. It downgraded Equifax in 2019 following its 2017 data breach. Kate Fazzini, *Equifax Just Became the First Company to Have its Outlook Downgraded for a Cyber Attack*, CNBC (May 22, 2019) https://www.cnbc.com/2019/05/22/moodys-downgrades-equifax-outlook-to-negative-cites-cybersecurity.html [https://perma.cc/LBM5-SC58].

73. Nicodemus, *supra* note 71.

74. Paolo Dal Cin et al., *Private Equity: The Rising Cost of Cyberattacks*, ACCENTURE (Mar. 4, 2023) https://www.accenture.com/us-en/insights/strategy/private-equity-rising-cost-cyberattacks [https://perma.cc/MWU6-37BJ].

75. Morgan, *supra* note 70.

76. Dal Cin et al., *supra* note 74.

77. Mastercard estimates that two-thirds of SMBs had at least one cyber incident in a two-year period. Morgan, *supra* note 70. Moreover, 60% of these businesses fail within six months of falling victim to a data breach or hack. *Id.*

78. *See infra* Part II.E.

79. Press Release, Dep't of Just., North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions (Sept. 6, 2018), https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and [https://perma.cc/3BF3-W8N6]; Alex Vakulov, *UnitedHealth Data Breach Escalates: 190 Million Americans Affected*, FORBES (Jan. 27, 2025), https://www.forbes.com/sites/alexvakulov/2025/01/27/unitedhealth-data-breach-escalates-190-million-americans-impacted/ [https://perma.cc/ZA7J-U7XL]; Pace & Trautman, *supra* note 64, at 897 (ransomware demands are a daily occurrence).

security was a mission critical risk and the company's cybersecurity apparently was woefully inadequate.[80] These *Caremark* actions have failed—and future such *Caremark* actions are likely to fail—for two reasons. First, to date, directors in these cases did assert some minimal oversight over cybersecurity,[81] even if it appears that they did not ensure they were adequately informed about deficiencies in the company's practices or did not ensure that they were promptly informed about potential breaches.[82] Second, and more important, plaintiffs' claims were dismissed because they predicated their claim on recovery for harms from inadequate cybersecurity systems, yet companies' cybersecurity deficiencies generally do not violate positive U.S. law.[83] This latter issue should arise in many future cases as the U.S. currently does not impose any generally-applicable substantive legal requirements on companies' cybersecurity systems; nor are most companies required to adopt systems that conform to generally accepted best practices and protocols, such as those set forth in the National Institute of Standards and Technology Cybersecurity Framework ("NIST").[84] While some regulations impose requirements on companies in certain industries[85] or which have specific types of data,[86] most companies are not subject to such requirements and even these requirements cover only a subset of the effective measures firms should take.[87] Thus, deficient cybersecurity itself generally will not support a *Caremark* action because inadequate cybersecurity is usually not unlawful.

The *SolarWinds* case illustrates how directors can escape *Caremark* liability even when cybersecurity is a mission critical risk and directors apparently failed to ensure they were promptly informed about cybersecurity deficiencies. [88] SolarWinds designed and sold

---

80. *See, e.g.*, Firemen's Ret. Sys. of St. Louis *ex rel.* Marriott Int'l, Inc. v. Sorenson, No. 2019-0965, 2021 WL 4593777 (Del. Ch. Oct. 5, 2021); Constr. Indus. Laborers Pension Fund v. Bingle, No. 2021-0940, 2022 WL 4102492 (Del. Ch. Sept. 6. 2022).

81. *Marriott,* 2021 WL 4593777, at *12–13 (finding prong 1 claims were unavailable because both the audit committee and the board received regular updates on the company's cybersecurity and responded to evidence of problems).

82. *Bingle*, 2022 WL 4102492, at *11.

83. *Id.* at *1; *Marriott*, 2021 WL 4593777, at *19; *see* Pace & Trautman, *supra* note 64, at 932–33 (discussing how the *Caremark* doctrine was applied in the Marriott Derivative Action case).

84. *See generally* Nat'l Inst. of Standards & Tech., THE NIST CYBERSECURITY FRAMEWORK (CSF) 2.0 (2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf [https://perma.cc/C9SE-M84H].

85. For example, the New York Department of Financial Services mandates that regulated entities adopt multi-factor authentication, data encryption in transit and at rest, hiring of a CISO and cybersecurity staff, Pen testing and vulnerability assessments and training, among other measures. *See Cybersecurity, Privacy and Data Protection 2022 Year in Review*, KRAMER LEVIN (Jan. 24, 2023), https://www.kramerlevin.com/en/perspectives-search/cybersecurity-privacy-and-data-protection-2022-year-in-review.html [https://perma.cc/NJ79-5WSC]. These measures only cover a subset of the features of a full and robust cybersecurity system.

86. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 24(a), § 248(b), 113 Stat. 1338 (1999) (Financial Services Modernization); *see also* Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (1996) (HIPAA); FTC Standards for Safeguarding Customer Information, 16 C.F.R. § 314 (2023); CAL. CIV. CODE § 1798.81.5(b) (West 2022) (the California Consumer Privacy Act requires companies collecting consumers' personally identifiable information to implement "reasonable security procedures and practices," without specifying which procedures are reasonable).

87. *E.g.*, SEC v. SolarWinds Corp., 741 F.Supp. 3d 37, 88 (S.D.N.Y. 2024); *Bingle*, 2022 WL 4102492, at *4.

88. *SolarWinds Corp.*, 741 F.Supp. 3d at 48. The facts are based on the derivative complaint and SEC complaint against SolarWinds. Complaint, *In re* Bingle Inc., No. 2021-0940 (Del. Ch. Nov. 4, 2021); Complaint, SEC v. SolarWinds Corp., No. 23-cv-9518 (S.D.N.Y. Oct. 30, 2023).

network monitoring software and cybersecurity products.[89] Its Orion software platform was its crown jewel, accounting for 45% of its revenues in the first nine months of 2020.[90] Thousands of companies and many government agencies used Orion to manage their information technology infrastructure, giving it access to their networks.[91] Adopting Orion thus created a cybersecurity risk for customers if SolarWinds failed to prevent malicious actors from infecting Orion with malware.

SolarWinds' financial welfare depended on convincing its customers that Orion was safe from infection by malicious actors. To do this, it published a security statement on its website, and made statements to customers, stating that it followed the NIST framework in designing and maintaining its software.[92] In fact, this statements was materially misleading as SolarWinds failed to follow much if not most of the NIST framework, as its own internal cybersecurity audits revealed.[93] Of particular importance, SolarWinds allegedly left an easily-guessed password, SolarWinds123, on its systems.[94]

Russian hackers utilized SolarWinds' vulnerabilities to access its Orion software, planting malicious code that later enabled them to infiltrate SolarWinds' government agency (including the DoD) and corporate customers, causing them substantial harm. The cyber hack—and revelation of SolarWinds' cybersecurity deficiencies—also caused substantial, long-term, harm to SolarWinds. "[I]ts license revenue declin[ed] by twenty-seven percent, and . . . [the company] incur[red] direct expenses of $34 million," and it faced investigations and/or claims from the DOJ, SEC, state AGs, and customers.[95] The stock initially lost almost 40% of its value;[96] as of January 2025 the stock price was down over 65% from where it was five years earlier.[97]

A derivative plaintiff filed a claim against the board under *Caremark*, asserting that cybersecurity was a mission critical risk for SolarWinds—a risk which the board breached its duties to oversee in bad faith.[98] The Delaware Chancery Court agreed that cybersecurity is a mission critical risk for SolarWinds; yet it nevertheless dismissed the complaint because the plaintiff did not alleged that SolarWinds' inadequate cybersecurity systems violated positive law.[99] The court also dismissed the plaintiff's oversight claims because the

89. *Bingle* Complaint, *supra* note 88, at 3.

90. *Id.* at 19.

91. *Id.* at 8–9.

92. *SolarWinds* Complaint, *supra* note 88, at 16.

93. *See infra* Part IV.B.

94. *See infra* notes 163–66.

95. Pace & Trautman, *supra* note 64, at 934–35.

96. *Id.* at 934.

97. *Investors Who Have Held SolarWinds (NYSE:SWI) Over the Last Five Years Have Watched Its Earnings Decline Along with Their Investment,* SIMPLY WALL ST. (Jan. 29, 2025), https://simplywall.st/stocks/us/software/nyse-swi/solarwinds/news/investors-who-have-held-solarwinds-nyseswi-over-the-last-fiv [https://perma.cc/NP9C-67Y8].

98. Constr. Indus. Laborers Pension Fund v. Bingle, No. 2021-0940, 2022 WL 4102492, at *1 (Del. Ch. Sept. 6. 2022).

99. *Id.* at *1, *9. The derivative plaintiff alleged that the company violated positive law by violating SEC guidance relating to cybersecurity. Complaint at 69, *In re* Bingle Inc., No. 2021-0940 (Del. Ch. Nov. 4, 2021). The court nevertheless dismissed because these violations were not the basis of plaintiff's claims. *Bingle*, 2022 WL 4102492, at *5, *14. Derivative plaintiff did not predicate their claim on the company's materially misleading statements to consumers and agencies. *See generally* Complaint, SEC v. SolarWinds Corp., No. 23-cv-9518 (S.D.N.Y. Oct. 30, 2023).

board had "at least a minimal reporting system about corporate risk, including cybersecurity [risk]," having delegated oversight of cybersecurity to two committees which received reports from management.[100] Prong 2 claims failed because plaintiffs did not credibly allege that the board—as opposed to management—was aware of SolarWinds' cybersecurity deficiencies.[101]

III. CAREMARK LIABILITY FOR BAD FAITH OVERSIGHT OF CYBERSECURITY DISCLOSURE

Although directors' bad faith inadequate oversight of mission critical cybersecurity generally does not trigger liability under *Caremark*, this Section shows that in circumstances where a company is harmed by deficient mission critical cybersecurity, directors should face *Caremark* liability for corporate trauma if the company made unlawful materially misleading statements to its customers about its cyber or data security, subsequently suffered a cyber-event from a deficiency the company mislead its customers about, such materially misleading statements to business and government customers constituted a mission critical legal risk to the firm, and directors did not satisfy their *Caremark 2.0* duties to oversee the veracity of the company's cybersecurity disclosures. In this situation, directors would face potential liability under *Caremark 2.0* for all corporate trauma proximately caused by the materially misleading statements to consumers. These costs include those from government enforcement actions and private civil actions predicated on the company's materially misleading statements aimed at consumers (even if brought by shareholders), litigation costs, loss of customers, and potential debarment or exclusion resulting from the unlawful statements.

A. Laws Prohibiting Lying to Consumers About Cybersecurity Quality

Companies that make products or services that could put their business or government customers at substantial cybersecurity risk regularly attest to the quality of their cybersecurity and data security practices, both on their websites and directly to consumers. Managers of companies with deficient cybersecurity may make such attestations, even when they are materially misleading, to enable their company to survive in a competitive market. When they do so, the managers and the company violate multiple laws prohibiting defrauding consumers; when these statements reach federal authorities, they also may violate the law by making false statements and false claims to the federal government if they make unqualified positive statements about the company's cybersecurity, without noting the company's material cybersecurity deficiencies.[102]

---

100. *Bingle*, 2022 WL 4102492, at *2.

101. *Id.* at *11; *see* Pace & Trautman, *supra* note 64, at 934–35 (discussing why the claims against SolarWind's directors ultimately failed).

102. Two types of laws govern cybersecurity disclosure: (1) those prohibiting materially misleading statements or claims relating to the company's cybersecurity or data privacy and (2) those mandating disclosure regarding cybersecurity or data integrity. This Article focuses on materially misleading disclosures about the company's cybersecurity quality because those violations have the greatest potential to be a mission critical risk. Companies also could violate the law by making materially misleading statements about a cyber-attack. *See* Press Release, SEC, SEC Charges Four Companies with Misleading Cyber Disclosures (Oct. 22, 2024)

Federal mail and wire fraud statutes, Section 5 of the Federal Trade Commission Act, and various state laws prohibit companies from making materially misleading statements to customers, including misleading statements about the quality of the company's cybersecurity practices and systems that impact the expected quality of the product for consumers.[103] Federal mail/wire fraud criminalizes the use of mails or wires (including the internet) to make materially misleading statements in order to obtain money or property from customers, for example, by misleading them into purchasing products they otherwise might have eschewed or purchasing products at an excessive price because of inflated cybersecurity quality claims.[104] Section 5 of the FTC Act prohibits companies from making such statements that could mislead a consumer and cause them substantial injury, for example, because of a cyberattack resulting from deficiencies in the company's cybersecurity about which it misled its customers. Section 5 focuses on resulting harm and does not require evidence that the company intentionally made the material misrepresentation to obtain money or property from consumers, as mail and wire fraud do.[105] Both prohibitions extend to statements about the company's cybersecurity, whether made in person, on the company's website, by email or mail, or in contracts with customers. State anti-fraud and consumer protection laws also prohibit similar types of materially misleading statements to consumers.[106]

Companies also can violate the law by making materially misleading statements about the company's cybersecurity to, or within the jurisdiction of, federal government agencies

---

https://www.sec.gov/newsroom/press-releases/2024-174 [https://perma.cc/7SSU-BRBG]. These violations are considerably less likely to constitute mission critical risks and thus are not the focus of this Article. When they do, the analysis in this Article would apply.

103. 18 U.S.C. §§ 1341, 1343; 15 U.S.C. § 45 (2006).

104. 18 U.S.C. §§ 1341, 1343.

105. Section 5 of the Federal Trade Commission Act prohibits companies from employing unfair or deceptive acts or practices in or affecting commerce. 15 U.S.C. § 45 (2006). "Deceptive" practices are defined in the Commission's *Policy Statement on Deception* as involving a material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances. Letter from FTC to United States Congress Committee on Energy and Commerce, FTC, FTC Policy Statement on Deception, (Oct. 14, 1983) https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [https://perma.cc/ZM5A-BKA2]. An act or practice is "unfair" if it "causes or is likely to cause **substantial injury** to consumers which is **not reasonably avoidable** by consumers themselves and **not outweighed by countervailing benefits** to consumers or to competition." 15 U.S.C. § 45(n) (emphasis added). *See generally A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FTC (May 2021), https://www.ftc.gov/about-ftc/mission/enforcement-authority [https://perma.cc/Z6TT-ALRL].

106. Press Release, Letitia James, N.Y. State Att'y General, Attorney General James Holds Equifax Accountable by Securing $600 Million Payment in Largest Data Breach Settlement in History (July 22, 2019), https://ag.ny.gov/press-release/2019/attorney-general-james-holds-equifax-accountable-securing-600-million-payment [https://perma.cc/R56H-YC6V]; Press Release, Matthew Platkin, N.J. Att'y General, NJ to Receive Roughly $500K from $16M Settlements Over 2012 and 2015 Experian Data Breaches, (Nov. 7, 2022), https://www.njoag.gov/nj-to-receive-roughly-500k-from-16m-settlements-over-2012-and-2015-experian-data-breaches/ [https://perma.cc/7NXS-UGA2]; Press Release, Letitia James, N.Y. State Att'y General, Attorney General James Announces $52 Million Multistate Settlement With Marriott Over Data Breach. (Oct. 9, 2024), https://ag.ny.gov/press-release/2024/attorney-general-james-announces-52-million-multistate-settlement-marriott-over [https://perma.cc/CJ2A-8KQW]; Press Release, SEC, Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay $35 Million (Apr. 24, 2018), https://www.sec.gov/newsroom/press-releases/2018-71 [https://perma.cc/3H3D-KRVE].

or departments, when contracting to provide goods or services to the government or submitting invoices to such federal agencies or departments. Federal agencies and departments regularly require federal contractors to attest their compliance with a host of cybersecurity measures as a prerequisite to contracting with the government.[107] Companies that make materially misleading statements about their compliance with such requirements in the course of contracting often violate numerous federal laws, including mail and wire fraud and the False Statements Act.[108] Companies with government contracts also can violate the False Claims Act if they submit requests for payment knowing that their cybersecurity systems do not substantially comply with the promises, warranties and statements in their government contracts.[109] Government contractors also can violate the False Claims Act by failing to comply with legal duties to "rapidly report" cyber incidents.[110]

B. Defrauding Consumers about Cybersecurity can Constitute Mission Critical Risk

Materially misleading statements to business and government customers about the company's cybersecurity can constitute a mission critical risk for certain companies by threatening substantial harm to the firm's on-going welfare.[111]

Companies that lie to customers risk greatly exacerbating the customer flight potentially triggered by a cyber-attack or data breach as customers substantially harmed by the company's deficient cybersecurity are more likely to flee if they learn the company lied to them and thus cannot be trusted to protect them in the future. Materially misleading statements also can cause on-going harm if they trigger regulator interventions that threaten future revenues. This threat is particularly great in the case of materially misleading statements about cybersecurity to government agencies. Yet not all such statements are mission critical risks. This Part discusses when materially misleading statements to business consumers or government agencies constitute mission critical risks and when they do not.

---

107. *See* FAR 4.1903 (2024); FAR 52.204-21 (2024).

108. *See* 18 U.S.C. §§ 1341, 1343; 18 U.S.C. § 1001 (2006).

109. False Claims, 31 U.S.C. § 3729 (2009); *see* Press Release, Dep't of Just., Deputy Attorney General Lisa O. Monaco Announces a New Civil Cyber-Fraud Initiative (Oct. 6, 2021) https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative [https://perma.cc/S8XE-5Y7Y]; David Bitkower et al., *New Civil Cyber-Fraud Initiative Uses False Claims Act to Enforce Cybersecurity Requirements*, COMPLIANCE & ENF'T (Oct. 22, 2021), https://wp.nyu.edu/compliance_enforcement/2021/10/22/new-civil-cyber-fraud-initiative-uses-false-claims-act-to-enforce-cybersecurity-requirements/ [https://perma.cc/4PVR-N4EN].

110. 48 C.F.R. § 252.204-7012(c) (2024).

111. Materially misleading statements to consumers also can reach shareholders potentially constituting securities fraud. Yet when the harm arising from directing these statements to consumers and government agencies does not constitute a mission critical risk, the additional harms arising from securities fraud violations will not trigger mission critical risk statutes as they generally simply trigger substantial one-time costs but do not impact long-run profits. Securities fraud violations could constitute a mission critical risk if they are so severe that they could cause the SEC to delist the company or if they might cause a ruinous impairment of the firm's ability to raise capital in the future. This tends to be unlikely, especially given the multiple avenues available to firms for reputational repair vis-à-vis securities markets. *See generally* Alexander & Arlen, *supra* note 20.

1. Materially Misleading Statements to Business Customers as Mission Critical Risks

Materially misleading statements to consumers about cybersecurity quality only constitutes a mission critical risk if the defects that the company lied about could enable a cyber-event that seriously harms consumers, and the joint revelation of the deceptive statement and the harmful cyber-event could substantially impair long-run profits, generally by triggering either consumer flight or a regulatory intervention (such as exclusion).[112]

A cyberattack is likely to trigger ruinous customer flight if three conditions are met. First, criminals' access to the company's products, systems, or data could cause substantial harm to customers (especially business or government agencies) who account for a substantial portion of the company's revenues. This harm is particularly likely if the deficiencies could lead to a cyber-event that undermines the integrity of business or government customers' systems, their vital data, assets, or the safety of their own customers' vital information. Second, the attacked company's inadequate cybersecurity or data management could enable a serious cyber-event (and in this case would enable it). Third, the company could expect more customer flight following a cyber-event if it misleads its customers about either the quality of the company's cybersecurity and data protections pre-attack or the timing, nature, or scope of the cyber-event itself, as this could lead customers to conclude that they cannot rely on the company to safeguard their interests in the future.[113]

Lying to consumers about material cybersecurity deficiencies whose existence could cause business and government consumers substantial harm is likely to increase customer flight following a cyber-event because consumers are likely to predicate their willingness to deal with the firm in the future on their expected risk of harm from using the company's products or services in the future. This expectation will depend on both the seriousness of the company's cyber-security deficiencies revealed by the attack and on whether the customers believe they can trust the company's statements regarding cybersecurity reforms. Trust matters because following an attack, companies often can retain customers by remediating the problems with their cyber security systems. Yet in order for remediation to assuage customers' concerns, customers must trust that the company actually is implementing, and will maintain, the promised reforms. Customers are less likely to trust a company that previously lied to them and thus should be more likely to seek alternative providers following a cyber-attack. Accordingly, materially misleading cybersecurity disclosures should often constitute a mission critical risk for companies which derive substantial revenues from business or government consumers who could be seriously harmed should the company's deficient cybersecurity enable a malicious cyber event.

By contrast, materially misleading statements relating to the cybersecurity protections afforded to individual consumers' ordinary personally identifiable information[114] generally do not constitute a mission critical risk as they are unlikely to risk long-term harm to

112. *See supra* note 54 and accompanying text; *supra* Part II.C (consumer reaction to the harm associated with the legal risk serves as the substantial harm that supports mission critical risk status).

113. For a discussion of when companies can expect to suffer enormous costs from reputational damage from legal violations see, e.g., Arlen & Alexander, *supra* note 20, at 97–107 (discussing when corporate violators are likely to incur costs from reputational damage).

114. This discussion focuses on ordinary personally identifiable information, such as name, address, email, phone number and social security number, each of which have been appropriated in massive previous breaches.

the company. The confluence of a cyber-event that appropriates such data and materially misleading statements is unlikely to cause customers flight because customers generally should expect their ordinary personal information to be already on the dark web. Accordingly, materially misleading statements about cybersecurity protections for individual consumers generally only constitute mission critical risk if the cybersecurity deficiencies could enable malicious actors to steal financial assets, intellectual property, or other valuable, currently private information from individuals.

In theory, companies also face potential mission critical risk from false or materially misleading statements to business consumers about cybersecurity if they might trigger regulatory agencies to intervene to reduce future sales, for example, through debarment, exclusion, delicensing, or an injunction. Multiple statutes prohibiting fraud grant the relevant regulator authority to impose injunctions to protect their consumers. This source of risk generally is unlikely to constitute a mission critical risk as the central enforcement authority's injunction authority tends to be limited to forcing the firm to correct its disclosure, as opposed to blocking future sales.[115]

Nevertheless, materially misleading statements about cybersecurity could create a mission critical risk through the threat of regulatory intervention if the statements enable product sales that create significant risk to health, safety, or national security as a result of cybersecurity deficiencies that the company may not be able to fully remediate. This is particularly a concern for companies that sell products that could enable a hack on a hospital's life support equipment or airline.[116]

2. False Statements and Claims to Government Customers as Mission Critical Risks

Companies also regularly sell products or services to government agencies. Some of these products can cause substantial harm to the government—and also to national security—should the company employ deficient cybersecurity in the product's development or

---

This discussion does not include important personal information such as health conditions, that could be used to as the basis for blackmail and other harm.

115. For example, materially misleading statements to individual or business customers can result in the FTC seeking and obtaining an injunction. *See* 15 U.S.C. § 53(b) (2005); FTC v. On Point Cap. Partners LLC, 17 F.4th 1066 (11th Cir. 2021) (affirming an FTC injunction under 15 U.S.C. § 53(b) for material misrepresentations made to consumers). The risk of such injunctions generally is not a mission critical risk as the FTC tailors its injunctions to remediating the breach and thus focuses on requiring companies to implement a "reasonable" cybersecurity regime and provide accurate disclosures, as opposed to enjoining the company from selling its products. *See* Randy Milch & Sam Bieler, *A New Decade and New Cybersecurity Orders at the FTC*, LAWFARE (Jan. 29, 2020) https://www.lawfaremedia.org/article/new-decade-and-new-cybersecurity-orders-ftc [https://perma.cc/C8YJ-PHKN]. Nevertheless, an FTC disclosure violation could constitute a mission critical risk if the company lied about its compliance with EU-US Data Privacy Framework Principals and the company's future welfare depends on its ability to transmit data from the EU to the US, since such a violation would risk exclusion from such transfers. *See Data Privacy Framework*, FTC https://www.ftc.gov/business-guidance/privacy-security/data-privacy-framework [https://perma.cc/L3YM-DGXK].

116. Indeed, a company that uses materially misleading statements to induce hospitals to purchase products or services with cyber deficiencies that could harm the hospital, and its patients potentially commits felony health care fraud, which could trigger mandatory, company-wide debarment from future dealings with—or receiving future payments from—Health and Human Services. *See generally* Arlen & Alexander, *supra* note 20, at 128–38.

on-going operations. This risk is particularly great with software, hardware, and data storage. Recognizing the importance of cybersecurity, federal authorities regularly impose detailed cybersecurity requirements on companies selling products whose weak cybersecurity could threaten government interests. Compliance with these requirements often is a precondition for contracting with certain federal agencies; companies seeking payment under such contracts warrant that they continue to comply with these requirements.[117]

Companies violate the False Statements Act[118] and/or the False Claims Act[119] if, in the course of contracting with, or submitting claims for payment to federal authorities, they make materially misleading statements about their cybersecurity quality. The risks posed by such materially misleading statements to federal authorities can constitute a mission critical risk if federal authorities constitute a substantial part of the company's revenues, because defrauding federal agencies can result in mandatory or permissive debarment or exclusion of the company from contracting with government agencies or in markets vital to its welfare.[120] The potential threat of such sanctions constitutes a mission critical risk even if rarely imposed, as the mission critical risk determination focuses on the *potential* peril to the company of a legal violation, and not what actually occurred.

C. Directors' Oversight of Mission Critical Cybersecurity Disclosure

Directors can face a significant risk of liability under *Caremark 2.0* in situations where defrauding consumers about cybersecurity quality constitutes a mission critical risk for the company. *Caremark 2.0* imposes explicit, well-defined oversight duties on directors with respect to oversight of the veracity of the company's disclosures relating to its cybersecurity quality. Adherence to these duties requires greater engagement by directors with cybersecurity quality than many likely usually undertake in their periodic meetings with the company's Chief Information Security Officer (CISO).

Directors of companies for which issuing materially misleading statements about cybersecurity to business consumers or government agencies constitutes a mission critical risk are subject to three oversight duties under *Caremark 2.0*. First, they must ensure that the company adopts compliance protocols for its cybersecurity disclosures that are both designed to ensure the accuracy of the company's cybersecurity disclosures and require management to report regularly to the board or a specific committee about any deficiencies in the oversight systems and any material detected instances of materially misleading cybersecurity disclosures.[121] Second, the designated unit of the board must in fact engage in on-going oversight of the veracity of those company disclosures about cybersecurity quality whose inaccuracy could constitute a mission critical risk.[122] To satisfy this duty, the directors must ensure that management reports to the board, on an ongoing basis, on any

117. *See e.g.*, FEDRAMP, https://www.fedramp.gov/ [https://perma.cc/VV43-5KHB]. For example, a Department of Defense (DoD) proposed rule requires defense contractors to certify their compliance with the Cybersecurity Maturity Model Certification (CMMC) 2.0 as a prerequisite to contracting the DoD. 48 C.F.R. 204.7503 (2023). Failure to comply would preclude a company from contracting with the DoD. *Id.*

118. 18 U.S.C. § 1001 (2006).

119. 18 U.S.C. 287 (2025).

120. *See generally* Arlen & Alexander, *supra* note 20, at 128–38 (discussing debarment and exclusion).

121. *See*, *e.g.*, Marchand v. Barnhill, 212 A.3d 805 (Del. 2019); *In re* Boeing Co. Derivative Litig., 2021 WL 4059934 (Del. Ch. Sept. 7, 2021).

122. *Marchand*, 212 A.3d at 809; *Boeing*, 2021 WL 4059934, at *28.

material deficiencies in the cybersecurity disclosure oversight systems and on any detected materially misleading disclosures that could constitute a mission critical risk.[123] To satisfy this duty directors generally should require the executives in charge of information security to review the company's public statements and contractual obligations and specifically highlight any materially misleading statements.[124] Directors also must insist that management report detected materially misleading statements about data and cyber security quality, as well as evidence that the company is not complying with requirements in its government contracts, promptly to the board.[125] Third, should the board receive a report of a red flag, directors must exercise direct oversight of the investigation and cannot simply delegate to management.[126] Finally, upon learning about any materially misleading statements, directors' *Massey* duties are triggered: they must terminate the violation, either by correcting the statements or bringing the company's cybersecurity into compliance with its pronouncements.[127]

Imposition of these *Caremark 2.0* is likely to improve impacted company's cybersecurity disclosures and also their cyber and data security practices and systems. Companies' mission critical cybersecurity disclosures are disclosures about protections in products or services that could put customers in genuine peril and concern features of those systems that could deter or enable a malicious cyber-event.[128] Seeking a standardized way to warrant safety, companies regularly advertise that their practices are in line with NIST and/or federal cybersecurity requirements. These standards for best practices set forth a detailed list of features to improve cybersecurity.[129] Companies that attest compliance with these standards can and do obtain internal and third-party audit of their systems to identify the ways in which their systems do not align with best practices.[130] To satisfy their *Caremark 2.0* duties, directors arguably should ensure that management conducts and reports on the results of an audit prior to making positive statements about the company's cybersecurity systems and should require that directors receive the results of, and a management report on, subsequent audits. These audits would not only enable directors to improve cybersecurity disclosure but would significantly improve the quality of information that many boards receive about the company's cybersecurity systems, enabling them to improve the company's cybersecurity when necessary to enable the type of positive disclosures required by customers.

---

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

124. *Id.* at *32.

125. *Id.* at *30–31.

126. *See*, *e.g.*, *Marchand*, 212 A.3d at 809; *Boeing,* 2021 WL 4059934, at *33.

127. *See generally* Arlen, *supra* note 4.

128. Erik Gerding, Dir., Div. of Corp. Fin., SEC, Cybersecurity Disclosure (Dec. 14, 2023), https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-disclosure-20231214 [https://perma.cc/9JB6-K8Y2].

129. NIST is a set of best practices. Companies can have good cybersecurity without complying with every feature. NIST divides cyber and data privacy protections into different buckets or categories. A company that has advertised its compliance with NIST should add corrective disclosure to identify deficiencies if it claims to be "NIST compliance" but scores less than "good" in its systems or practices in any one of the categories of protection. Otherwise, customers would reasonably conclude that the company has inadequate systems in at least one of the NIST buckets. This would alter the total mix of information that is usually associated with a company that is NIST compliant. *See* Nat'l Inst. of Standards & Tech*., supra* note 84.

130. Nat'l Inst. of Standards & Tech*., supra* note 84, at 3–4.

In turn, these *Caremark 2.0* duties regularly should enable derivative plaintiffs to succeed in their *Caremark* 2.0 actions against directors for corporate trauma proximately caused by the confluence of a malicious cyber-event and mission critical materially misleading cybersecurity disclosures that mislead customers and government agencies about material cybersecurity deficiencies. Such materially misleading statements about material deficiencies are most likely to result from directors' breach of their oversight duties. After all, directors who insist on receiving regular audits of the veracity of the company's cybersecurity disclosures generally should learn about and remediate cybersecurity weaknesses (or the disclosures). While it is true that such deficiencies could exist if management consistently lied to the board, and presented them with doctored audit reports,[131] absent such lies the existence of the unremediated cybersecurity deficiencies that render the company's public statements about mission critical risks materially misleading would appear to indicate that the board either knowingly retained a cybersecurity deficiency that the company claimed not to have (a *Massey* violation)[132] or failed to ensure that management audited the company's systems and reported about any material discrepancies between the company's statements to consumers and its actual systems.

D. Establishing a Causal Connection between Oversight Breach and Corporate Harm

To prevail, derivative plaintiffs must establish that the directors' bad faith failure to oversee cybersecurity *disclosure* were a proximate cause of the corporate harm the plaintiffs seek to recover for.[133] Thus, the claimed harms must be proximately caused by the firm's materially misleading statements; they cannot be *solely* attributable to the company's deficient cybersecurity or the cyber-event itself.[134]

To satisfy the proximate cause requirement, derivative plaintiffs must show that the company's materially misleading statements about its cybersecurity would not have occurred but for the directors' breach of their *Caremark 2.0* duties to oversee the accuracy of the company's materially misleading cybersecurity disclosures, and that these disclosure violations were a substantial factor in causing the harm for which plaintiffs seek recovery on behalf of the firm.

In situations where the first requirement is met, derivative plaintiffs can necessarily establish the second proximate cause requirement when they seek recovery for corporate trauma that arises from the materially misleading statements. Recoverable damages should include the litigation and liability costs arising from government enforcement actions or private litigation predicated on the company's materially misleading statements about its cyber-security quality. This should include securities fraud enforcement actions or private litigation predicated on the company's materially misleading statements to consumers (and in turn shareholders) about cybersecurity as these statements are the but-for and foreseeable cause of this litigation. Directors also could face liability for lost revenues from customer

131. Such lies would support a *Caremark* action against the executives who lied. *In re* McDonald's Corp. S'holder Derivative Litig., 289 A.3d 343, 349 (Del. Ch. 2023) (officers can be held liable under *Caremark*).

132. *See supra* notes 29–30.

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

134. *Id.*

flight substantially caused by the companies materially misleading statements to customers, and well as lost revenues from any debarment or exclusion resulting from false or fraudulent statements made to government agencies or consumers.

In rare cases, derivative plaintiffs might be able to prove that the materially misleading statements harmed the firm by causing it to retain deficient cybersecurity. In this case, the misleading statements would be the proximate cause of corporate losses arising from its deficient cybersecurity. Derivative plaintiffs can establish this if they can prove that directors exerting good faith oversight over cybersecurity disclosure would have learned about cybersecurity deficiencies that were so serious that the directors could not in good faith have remediated the misleading disclosures by simply telling customers the truth. The only recourse available to them, in the exercise of good faith Business Judgement, would have been to remediate the deficiencies with the company's cybersecurity system—deficiencies that enabled the malicious cyber-event. Derivative plaintiffs often will not be able to satisfy this requirement but may be able to in some circumstances.

E. Summary

Accordingly, this in-depth assessment of *Caremark 2.0* reveals that materially misleading statements about cybersecurity constitutes a mission critical risk for companies whose deficient cybersecurity could result in egregious harm to business consumers or government agencies. In such circumstances, Delaware law requires directors to assert direct oversight over cybersecurity quality; in particular, they must insist that management compare the company's disclosures against its actual systems and report all material deviations or omissions to the board. Boards that fail to do this risk being held liable for corporate trauma proximately caused by the confluence of the company's materially misleading statements and a malicious cyber-event.

IV. SOLAR WINDS DIRECTORS' POTENTIAL LIABILITY REASSESSED

The liability-enhancing potential of predicating a cybersecurity *Caremark* action on the directors' breach of their duty to exert oversight to deter, and ensure they are informed of, materially misleading cybersecurity disclosures is perhaps best elucidated by re-assessing the *SolarWinds* case. This Section analyzes the facts of *SolarWinds*, as set forth by the derivative plaintiffs and the SEC,[135] and shows that derivative plaintiffs likely could have prevailed had they sought recovery for the board's bad faith failure to oversee the firm's compliance with its legal obligations not to materially mislead its business and government customers about the quality of its cybersecurity.

A. Misleading Cybersecurity Disclosure as a Mission Critical Legal Risk

For SolarWinds, making materially misleading statements about its cybersecurity to business and government customers constituted a mission critical legal risk. SolarWinds'

135. *See* SEC v. SolarWinds Corp., 741 F.Supp. 3d 37, 50 (S.D.N.Y. 2024); Constr. Indus. Laborers Pension Fund v. Bingle, No. 2021-0940, 2022 WL 4102492, at *2–5 (Del. Ch. Sept. 6. 2022).

revenues depended substantially on sales to large corporations and government agencies.[136] SolarWinds main product integrated into customers' systems in ways that left customers vulnerable to substantial harm should SolarWinds have cyber deficiencies that enabled malicious actors to infect its software.[137] Thus, as SolarWinds recognized, to market its product it needed to satisfy customers that it implemented best practices relating to cybersecurity.[138] Moreover, its government agency customers required it to make specific attestations about its cybersecurity quality as a condition of contracting with them.[139] For SolarWinds, lying in these cybersecurity statements could constitute an existential threat to the firm—threatening serious long-term losses from customer flight and regulatory interventions such as exclusion from government contracting vital to the firm's future.

Consistent with the conclusion that SolarWinds' materially misleading statements to customers undermined their trust in the firm, leading to customer flight, it appears that SolarWinds' license revenue declined by more than 25% following the attack[140] and the stock initially lost 40% of its value;[141] as of January 2025 the stock price was down 65% from where it was five years earlier.[142] Companies with massive cyber-events which did not materially mislead their business or government customers about cyber-deficiencies that could cause them egregious harm fared much better after disclosing a massive cyber-event. For example, Marriott's stock price recovered quickly following its disclosure in November 2018 that it suffered a massive cyber-event.[143]

B. SolarWinds' *Alleged Unlawful Materially Misleading Statements About its Cybersecurity*

Although it was imperative for SolarWinds not to lie to its business and government customers about its cybersecurity systems and practices, it appears, based on allegations in actions against it, that the company made materially misleading statements about its cybersecurity that violated at least four laws governing cybersecurity disclosure: (1) wire fraud, (2) Section 5 of the FTC Act,[144] (3) the False Statements Act,[145] and (4) the False Claims Act.[146]

---

136. *SolarWinds*, 741 F. Supp. 3d at 50.

137. *See id.*

138. *Id.* at 50–51.

139. *See Bingle*, 2022 WL 4102492, at *9.

140. Pace & Trautman, *supra* note 64, at 934.

141. *Id.*

142. SIMPLY WALL ST., *Investors who have held SolarWinds (NYSE: SWI) over the last five years have watched its earnings decline along with their investment,* (January 29, 2025), https://simplywall.st/stocks/us/software/nyse-swi/solarwinds/news/investors-who-have-held-solarwinds-nyseswi-over-the-last-fiv [https://perma.cc/GU8G-X2VQ].

143. Brian Sozzi, *Why Marriott's Stock Has Surged After 500 Million of its Customers got Hacked*, YAHOO! FIN. (July 16, 2019), https://finance.yahoo.com/news/why-marriotts-stock-has-surged-after-500-million-of-its-customers-got-hacked-191836866.html? [https://perma.cc/5TPQ-WSUL].

144. 15 U.S.C. § 45 (2006).

145. 18 U.S.C. § 1001 (2006).

146. The latter two legal violations assume that the SolarWinds' government contracts required it to comply with various cybersecurity protocols which it did not in fact comply with. The firm also appears to have violated securities laws prohibiting materially misleading statements to the public, both about the quality of its cybersecurity processes and its initial public disclosures relating to the hack. Complaint at 1–4, SEC v. SolarWinds Corp., No. 23-cv-9518 (S.D.N.Y. Oct. 30, 2023). Derivative plaintiffs could recover for harm from these violations

SolarWinds allegedly made materially misleading statements to customers in the "Security Statement" it posted on the Trust Center of its website from late 2017 until 2020.[147] In this statement, SolarWinds asserted that it (1) followed the National Institute of Standards and Technology ("NIST") Cybersecurity Framework for evaluating cybersecurity practices; (2) used a secure developmental lifecycle to create its software products; (3) employed network monitoring; (4) had strong password protections; and (5) maintained good access controls.[148] SolarWinds also distributed this statement to customers seeking information on whether the company's systems satisfied their requirements.[149] This statement was drafted in part by Timothy Brown, Vice President of Security & Architecture and head of its Information and Security Group.[150]

Yet, as Brown knew, this Security Statement was (allegedly) materially misleading.[151] SolarWinds' claim that it followed the NIST framework allegedly was materially misleading because the company failed to disclose that it did not in fact follow many parts of the NIST framework that are material to customers.[152] Indeed, SolarWinds own 2017 assessment of its NIST compliance found that it was deficient in 3 of the 5 core areas covered by NIST.[153] Indeed, the firm scored 0 (no evidence of compliance) or 1 (ad-hoc compliance) on multiple areas.[154] In its 2018 NIST assessment, the firm scored 0 on 25 specific controls; and 1 on 50 others.[155] A 2019 NIST assessment also gave SolarWinds inadequate scores, including in important areas like "Authentication, Authorization and Identity Management."[156] Consistent with the conclusion that these deficiencies were material omissions, the author of the Security Statement, Brown, privately stated that SolarWinds' "current state of security leaves [the company] in a very vulnerable state for our critical assets.'[157]

SolarWinds also publicly claimed that it employed a "Secure Development Lifecyle" for its products, designed to prevent malicious computer code from being inserted into its software.[158] Evidence suggests this statement also was materially misleading, as its managers knew. For example, the firm received an inadequate score on its compliance with "Secure Software Development" in its 2019 NIST audit.[159] Engineers specifically flagged

---

should they show directors violated *Caremark*, but these violations are not among those that constitute a mission critical risk for the firm.

147. SEC v. SolarWinds Corp., 741 F. Supp. 3d 37, 51 (S.D.N.Y. 2024).

148. *Id.* at 51–52.

149. *Id.* at 51.

150. *Id.*

151. *Id.* at 52. Indeed, managers within SolarWinds openly complained about SolarWinds failure to comply with its own Security Statement. *Id.* ("In January 2018, managers complained that 'we don't do some of the things that are indicated in' the Security Statement.").

152. *SolarWinds*, 741 F. Supp. 3d at 52. A disclosure is materially misleading if the statement omits a fact (e.g., broad non-compliance with NIST) whose disclosure would alter the total mix of information provided to a reasonably prudent person by the original statement. TSC Indus., Inc. v. Northway, Inc. 426 U.S. 438, 449 (1976).

153. *SolarWinds*, 741 F. Supp. 3d at 55.

154. *Id.*

155. *Id.* at 55–56.

156. *Id.* at 56.

157. *Id.* at 50.

158. *SolarWinds*, 741 F. Supp. 3d at 56.

159. *Id.* at 57.

that the Orion platform was not being developed in conformity with SDL requirements.[160] The problems with Orion included its use of public code already known to contain vulnerabilities and its poor password processes.[161] In 2017 and 2018 the firm gave itself a 0 for its Cloud business segments "Security Continuous Monitoring" control.[162]

Of particular importance, the company's Security Statement asserted that the company employed "password best practices," including the use of complex passwords and regular password changes for "all applicable information systems, applications, and databases."[163] As Brown and others knew, this was materially misleading. Early in Orion's development, SolarWinds employed an easily hacked default password, SolarWinds123, which it retained for some systems.[164] Both the 2019 and the 2020 audits determined that the company was deficient in 27 of 100 internal controls tests, many relating to access and passwords.[165] The company also knew that password deficiency was a risk, learning as early as November 2019 that the password to one of its servers was publicly available.[166]

The company also appears to have made misleading statements when contracting with and seeking payment from government agencies. In contracting with multiple government agencies, SolarWinds attested that it complied with several government agencies' requirements about cybersecurity.[167] Yet its 2019 NIST 800-53 assessment of whether it complied with the Federal Risk and Authorization Management Program (Fed RAMP) showed that it could only demonstrate compliance with 6% of the requisite controls; it did not have the requisite protocols or programs in place for 198 (61%) of the 325 controls tested.[168] Thus, any statements made by SolarWinds to federal authorities that it complied with FedRAMP were materially misleading.

C. Did Directors Violate their Oversight Duties?

SolarWinds' directors arguably were obligated under *Caremark* to implement procedures designed to ensure that its public statements about its cyber-security were accurate and that directors were informed about any material deviations between its statements and its actual practices. The existing record does not establish whether plaintiffs can satisfy these requirements, but the gulf between the company's public statements and its actual practices was so great that it would appear that the derivative plaintiffs should be able to show that either (1) the SolarWinds board did not require management to report on deviations between its cybersecurity disclosures and its actual systems, and did not require management to provide the board with the audits of the company's NIST compliance, or (2) the board did satisfy its oversight duties, knew the company was making misleading disclosures, and did not terminate them. On either of these facts, the board would have violated their *Caremark* duties.

160. *Id.*
161. *Id.* at 59–60.
162. *Id.* at 55–56.
163. *SolarWinds*, 741 F. Supp. 3d at 59.
164. *Id.* at 83.
165. *Id.* at 60.
166. *Id.* at 58.
167. *Id.* at 51.
168. *SolarWinds*, 741 F. Supp. 3d at 56.

It is possible, of course, that the directors actively sought to exert oversight over the accuracy of SolarWinds' cybersecurity disclosures but did not learn the truth because they were lied to by management and presented with doctored audit reports. Yet this seems unlikely. First, there is no hint that audit reports were doctored. Second, the SolarWinds' board included directors who owned SolarWinds when it was a private company and then stayed on after taking it public.[169] These directors would have been unusually well-informed about the firm. Finally, the firm hired third-party cybersecurity auditors from whom a diligent board could have obtained reports directly.[170]

D. Causation

Should derivative plaintiffs show that SolarWinds' board breached its *Caremark 2.0* duties to oversee the veracity of the firm's cybersecurity disclosures and as a result failed to detect and prevent the company from making unlawful materially misleading statements about deficiencies that contributed to the cyberattack, the directors would face liability for all corporate trauma that resulted from their breach. This would include the litigation costs and any eventual settlements arising from government enforcement actions and private class actions predicated on the company's misleading statements, including securities fraud actions predicated on the company's materially misleading statements to customers that reached the securities markets. They also should be liable for corporate trauma from the customer flight attributable to the company's lies to consumers.

V. CONCLUSION

Never have companies and people in the U.S. been more dependent on technology or more vulnerable to catastrophic losses as a result of inadequate cybersecurity. This vulnerability often arises from the cybersecurity deficiencies of companies that make either the IT products that companies and government agencies use or the equipment and systems on which they depend to safeguard their property or people's lives. It therefore is vital to motivate such companies to implement adequate measures to safeguard their products. Doing this requires that directors be induced to exert adequate oversight over cybersecurity.

For a select set of firms, *Caremark* can potentially provide this incentive, by providing directors with a strong personal motivation to exert oversight to ensure the company does not lie to its customers about its cybersecurity. This should lead companies to improve their cybersecurity quality in the situations where directors face a genuine threat of liability because cybersecurity is a mission critical risk. The affected companies are those whose cybersecurity deficiencies could seriously harm business consumers or government agencies. These customers will tend to eschew a company with weak cybersecurity. As a result, requiring director oversight of cybersecurity disclosure would likely also improve cybersecurity quality as directors made aware that the company cannot lawfully provide consumers with the quality attestations that they demand often will be compelled by competitive market pressures to improve the company's cybersecurity, rather than openly disclose that the company's cybersecurity is inadequate. In addition, requiring accurate disclosure to con-

169. *See id.* at 53–54.
170. *Id.* at 72.

sumers should reduce the harm from malicious cyber-events by giving consumers the information they need to determine whether they should obtain the desired goods or services from a safer firm, potentially reducing future losses should the firm be breached. The resulting application of *Caremark 2.0* should enhance firm welfare by reducing mission critical risks; it also should enhance social welfare by enabling the market to function effectively to induce companies to invest in cybersecurity when it is most needed.

While the present Article focuses on cybersecurity, its conclusions about the applicability of *Caremark 2.0* to materially misleading consumer disclosures that constitute mission critical risks could be applied in other contexts, for example to materially misleading disclosures to consumers about the safety of products with the potential to cause significant numbers of consumer deaths.