Articles + Publications | October 12, 2021

Delaware Court of Chancery Highlights Seriousness of Cybersecurity Concerns While Maintaining High Standard for Caremark Claims

WRITTEN BY

Ronald Raether, Jr. | Christopher B. Chuff | Jay A. Dubow | Emily L. Wheatley

On October 5, the Delaware Court of Chancery issued a decision in *Firemen's Retirement System of St. Louis v. Sorenson, et al.*, C.A. No. 2019-0965-LWW, dismissing breach of fiduciary duty claims brought against various Marriott International, Inc. (Marriott) directors arising out of a massive, multiyear data hack that leaked the personal information of 500 million Marriott guests. The plaintiff alleged that the Marriott board of directors (Board) had failed to take appropriate measures to prevent such a severe data breach. Vice Chancellor Lori W. Will held that certain of the plaintiff's claims were time-barred and that the plaintiff had failed to allege particularized facts sufficient to show a complete failure of oversight on the part of the Board. The plaintiff's complaint was dismissed in its entirety. The court's decision is available here.

Background and Analysis

In September 2016, Marriott acquired Starwood Hotels and Resorts Worldwide, Inc. (Starwood). Two years later, in 2018, Marriott learned it had suffered a major data security breach. The cyberattack targeted Starwood's reservation database, which Marriott had acquired as part of the 2016 acquisition. As part of the fallout from the data breach, the plaintiff brought this derivative action for breach of fiduciary duty against all but one of the directors who served on both the pre- and post-acquisition Boards. According to the plaintiff, the directors breached their duties by (1) failing to undertake appropriate cybersecurity due diligence before the acquisition, (2) failing to implement adequate internal controls post-acquisition, and (3) failing to publically acknowledge the data breach until November 2018, two months after Marriott first learned of the issue.

In one of the first cases to apply the newly minted *Zuckerberg* demand futility standard, Vice Chancellor Will considered whether a majority of the Marriott Board in place at the time the complaint was filed face a substantial likelihood of liability for the claims asserted.[1] Vice Chancellor Will quickly disposed of any claims related to the Board's failure to engage in appropriate cybersecurity due diligence prior to closing the deal because such claims were brought after the analogous statute of limitations had run. In other words, all pre-acquisition claims were stale.

Thus, the court was left to grapple with the plaintiff's *Caremark* claim that the post-acquisition Board had failed to implement and/or monitor adequate cybersecurity oversight. At the start, Vice Chancellor Will noted the extreme difficulty any plaintiff faces when attempting to prevail in asserting any type of *Caremark* claim, *i.e.*, a plaintiff must plead particularized facts showing that the directors either (1) utterly failed to implement any sort of internal

controls or other oversight or (2) consciously failed to monitor or oversee the controls that were in place, turning a blind eye to the risks or problems at hand.

After a brief discussion of recent high-profile data breaches and the growing threat of cyberattacks, Vice Chancellor Will acknowledged that "[t]he corporate harms presented by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place." She went on to note, however, that the serious risks posed by cybersecurity threat do not "lower the high threshold that a plaintiff must meet to plead a *Caremark* claim." Under the stringent *Caremark* standard, the plaintiff's allegations fell short and failed to demonstrate that the Marriott directors "completely failed to undertake their oversight responsibilities, turned a blind eye to known compliance violations, or consciously failed to remediate cybersecurity failures." Only where a board has wholly failed to institute any sort of oversight or has consciously chosen to remain idle in the face of "red flags" signaling potential corporate misconduct will a plaintiff prevail in asserting a *Caremark* claim.

The court was no more persuaded by the plaintiff's argument that the directors had breached their fiduciary duties by failing to immediately notify the public of the data breach when it was first discovered in September 2018. Vice Chancellor Will held that the plaintiff had not alleged particularized facts to show that Marriott appreciated the extent of the data breach and the amount of personal information that had been compromised before November 2018 when it went public with the news of the breach.

In the final paragraphs of her decision, Vice Chancellor Will acknowledged the momentousness of the data breach at issue, but squarely placed any blame for the breach on the hacker himself, stating that "Marriott was the victim of an illegal act rather than the perpetrator." Despite that fact that Marriot arguably could have done more to prevent the data breach, Vice Chancellor Will reminded that "the difference between a flawed effort and a deliberate failure to act is one of extent and intent," and to adequately allege a *Caremark* claim the plaintiff must demonstrate the latter.

Takeaways

In a world where cyberattacks and data breaches have become increasingly prevalent, the Court of Chancery's recognition that "corporate governance must evolve to address" these risks is important, and perhaps signals an increased emphasis on a board's duty to implement cybersecurity measures and safeguard against such events. However, it is equally important to note that the court made clear that the security challenges posed by the ever-evolving world of 21st century technology in no way lower the rigorous standard that a plaintiff must meet to successfully plead a *Caremark* claim.

---

[1] The plaintiff did not claim that any director received a material personal benefit from the challenged conduct and only challenged the independence of four members of the 14-member Board. Therefore, the court needed to only analyze the second factor of the *Zuckerberg* test, whether the director faces a substantial likelihood of liability on any of the claims that would be the subject of the litigation demand.

RELATED INDUSTRIES + PRACTICES

- Business Litigation
- Consumer Financial Services

- Delaware Court of Chancery Litigation