Proskauer

SolarWinds: A Lesson on How Companies Victimized by Data Breaches Can Quickly Become the Target of Litigation and Regulatory Investigations

Proskauer on Privacy Blog on **November 16, 2022**

In 2020, SolarWinds Corp., a company that provided information technology software to private and government entities, was the victim of a cybersecurity breach. Russian hackers are believed to have slipped malicious code into a SolarWinds software product called Orion, which was then used to infect, and in certain cases, compromise, SolarWinds customers. As a consequence, SolarWinds found itself the target of litigation, including a derivative suit before the Delaware Court of Chancery in *Construction Industry Laborers Pension Fund v. Bingle*.

There, stockholders brought claims against the board of directors of SolarWinds for its alleged failure to oversee the company's cybersecurity risk. The plaintiff stockholders in *Bingle* argued that the defendant directors breached their fiduciary duty of loyalty by purportedly failing to adequately prevent the 2020 breach. According to the plaintiffs, the board violated these duties by, among other things, allegedly ignoring warnings about cybersecurity deficiencies.

After carefully considering the plaintiffs' allegations, the court concluded that dismissal was appropriate on Chancery Court Rule 23.1 grounds. The gist of this rule is that stockholders who allege wrongdoings that have harmed a corporation must first ask the board to look into the matter before bringing a lawsuit and, if they do not, they must satisfy rigorous pleading standards. These standards require plaintiffs to plead with specificity facts suggesting a reasonable inference that a majority of the directors consciously disregarded their duties over an extended period of time, and, therefore, a demand on the board to first investigate the matter would have been futile.

In holding that the *Bingle* plaintiffs failed to plead demand futility, the court explained that, under Delaware law, the "pertinent question is not whether the board was able to prevent a corporate trauma, here because of a third-party criminal attack. Instead, the question is whether the board undertook its monitoring duties (to the extent applicable) in bad faith." A showing of bad faith "requires conduct that is qualitatively different from, and more culpable than, the conduct giving rise to a violation of the fiduciary duty of care (i.e., gross negligence)."

Put differently, plaintiffs must plead particularized facts showing that the directors had "actual or constructive knowledge that their conduct was legally improper." They can do so in one of three ways by pleading that a director: (*i*) violated positive law (*i.e.*, a statute or regulation mandating certain conduct); (*ii*) intentionally acted with a purpose inimical to the corporation's best interest, or (*iii*) consciously disregarded their duties by ignoring red flags so vibrant that scienter is implied or by utterly failing to put into place any mechanism for monitoring or reporting risk. The court examined each of these points, starting with the plaintiffs' allegation that the board violated positive law.

Violation of Positive Law

In support of their allegations that the board behaved contrary to positive law, the plaintiffs relied on, among other things, a 2018 Securities and Exchange Commission interpretive guidance, which included a statement that "'[c]ompanies are required to establish and maintain appropriate and effective disclosure controls and procedures[,] including those related to cybersecurity[.]'" "While this guidance is certainly indicative of requirements regarding public company disclosures," the court noted, "it does not establish positive law with respect to cybersecurity *procedures* or how to manage cybersecurity risks." The court stressed that plaintiffs who plead oversight failures must demonstrate "a sufficient connection between the corporate trauma and the actions or inactions of the board" and, in Delaware courts, such a connection has only been satisfied where a board has failed to monitor compliance with positive law, and the company thereafter violates said law. As the court observed, "no case in this jurisdiction has imposed oversight liability based solely on failure to monitor business risk," as opposed to failure to monitor the company's compliance with positive law. Leaving open the question of whether board liability could be predicated on a failure to oversee business risk (such as cybersecurity risk), the court held that the plaintiffs had "not alleged that legal and regulatory frameworks have evolved with respect to cybersecurity, such that SolarWinds's corporate governance practices must have followed."

Intentional Action with a Purpose Inimical to the Corporation

Turning to the second prong, the court held that the plaintiffs failed to plead this prong with particularity because the plaintiffs did not plea any allegations that the board intentionally acted with a purpose inimical to the corporation's best interests.

Ignorance of Red Flags or Lack of an Effective Reporting System

Examining the third prong, the court quickly dispensed with the plaintiffs' allegations that the board ignored red flags. At the outset, the court rejected the plaintiffs' allegations that a cybersecurity briefing presented to the board's Nominating and Governance Committee ("NGC") was a red flag that was ignored. According to the court, the presentation warned of cybersecurity threats and risks but "was not indicative of an imminent corporate trauma." The presentation was, accordingly, not a "red flag" but rather an instance of board-level oversight, and the complaint failed to plead that the presentation "made action by the Board necessary." The court also refused to countenance other allegations about other purported "red flags," including concerns allegedly raised by a former employee and allegations about use of an insufficient password, noting that the plaintiffs failed to plead these flags were before the board during the relevant period of time.

The court next addressed the plaintiffs' argument that the above and other allegations suggested the absence of an effective reporting system. In this regard, the plaintiffs alleged that the board "did not conduct a single meeting or have a single discussion about the company's mission critical cybersecurity risks" in the two years preceding attack. The court noted that, during the relevant period of time, the board charged two board committees with responsibility for oversight of cybersecurity risks. As the court explained, delegation of oversight responsibility of a "particular risk in a particular year" to a "non-sham, functioning Committee" does not indicate that the board intentionally disregarded its oversight responsibilities in bad faith. Further, while the committees' failure to report to the board indicated a "subpar reporting system" that should have been of concern to the directors, it did not represent an "utter failure to attempt to assure" that a reporting system existed, and thus did not indicate "an *intentional* 'sustained or systematic failure' of oversight, particularly given directors are *presumed* to act in good faith." Having concluded that the complaint failed to plead facts supporting a reasonable inference of bad faith by SolarWinds's directors, the court held that the plaintiffs' claim was "not viable," and, therefore, that the plaintiffs had failed to plead demand futility. The court, accordingly, dismissed the complaint.

The *Bingle* court's decision—while favorable for SolarWinds—appears to be just a stepping stone in what is likely to be long series of proceedings. Indeed, on November 3, 2022, SolarWinds announced that it is facing an investigation from the SEC. Notably, the SEC is not alone in investigating companies that have experienced a data breach. The Federal Communications Commission, the Federal Trade Commission, and the New York Department of Financial Services, among others, also have aggressively investigated and taken enforcement actions against companies. Often, investigations by these regulators are conducted in parallel, requiring a company to simultaneously navigate jurisdictional, regional, and sectoral nuances as well of investigations of potentially different scope. It is reasonable to expect that the list of regulators in the cyber space will continue to grow along with their security requirements, as enforcement continues to increase and fines and penalties become more severe. Accordingly, a critical aspect of post-breach practice is collaborating with regulators to manage burden, leading to a more efficient processes and outcomes for both the target, the regulators, and ultimately, consumers.

View original.

Related Professionals

- **Margaret A. Dale**
  Partner
- **Nolan M. Goldberg**
  Partner
- **Michelle M. Ovanesian**
  Associate