SULLIVAN & CROMWELL LLP

S&C memo

September 19, 2022

Delaware Chancery Court Rejects *Caremark* Liability for Failure to Oversee Cybersecurity Risk

Court Classifies Cybersecurity Risk as a Business Risk for SolarWinds; Oversight of Business Risk, Even if "Mission Critical," Analyzed Under Business Judgment Rule, Not *Caremark* Standard

SUMMARY

On September 6, 2022, in *Construction Industry Laborers Pension Fund on behalf of SolarWinds Corporation, et al.* v. *Mike Bingle, et al.* ("*SolarWinds*"),[1] the Delaware Chancery Court granted a motion to dismiss a derivative suit against directors of SolarWinds Corporation, a provider of information technology infrastructure management software, for allegedly breaching their fiduciary duty of loyalty by failing to oversee the company's cybersecurity risk, which, plaintiffs claimed, resulted in a major cyber breach in 2020.

Vice Chancellor Sam Glasscock III held that plaintiffs failed to allege demand futility with sufficient particularity, as required to pursue litigation derivatively on behalf of the company. In reaching that decision, the court found that plaintiffs failed to plead sufficiently particularized facts from which to infer bad faith on the part of directors to support their failure of oversight claim. As a result, the court held demand was not futile because there was no substantial likelihood that a majority of the directors faced liability for acting in bad faith.

BACKGROUND

SolarWinds is the latest of many recent cases alleging failure of oversight under Delaware law against a company's board of directors following a prominent corporate trauma. SolarWinds develops software for businesses to help them manage their information technology infrastructure.[2] SolarWinds' base of 320,000

customers includes Fortune 500 companies, major technology companies such as Microsoft, and various United States government agencies, including the Federal Bureau of Investigation, Secret Service, and National Security Agency.[3]

In 2020, Russian hackers concealed malicious code in SolarWinds' software in order to gain entry to SolarWinds' customers' systems.[4] The attack, dubbed "Sunburst," affected up to 18,000 of SolarWinds' clients.[5] Following the company's announcement of the attack and subsequent drop in stock price, multiple class action lawsuits were filed, and investigations were opened by "numerous domestic and foreign law enforcement agencies."[6]

Plaintiffs filed suit alleging so-called "*Caremark* claims"[7] seeking to hold defendants liable for various failures leading up to the Sunburst attack. Plaintiffs alleged that the defendant directors were repeatedly warned about "the Company's weak passwords and basic cybersecurity deficiencies" but, despite these warnings, "utterly failed to conduct any reasonable oversight concerning the company's mission critical cybersecurity risks."[8]

Defendants moved to dismiss for failure to allege with particularity that a demand to the directors would have been futile.

DECISION

The Delaware Chancery Court dismissed the case for failure to plead demand futility, ruling that the complaint failed to demonstrate a substantial likelihood that a majority of SolarWinds' board faced liability on the merits of plaintiffs' *Caremark* claim.

At the outset, Vice Chancellor Glasscock noted that plaintiffs' theory of liability would hold defendants liable for a failure to oversee cybersecurity risk but that "no case in this jurisdiction has imposed oversight liability based solely on failure to monitor business risk," as opposed to monitoring the company's compliance with positive law, *i.e.*, statutes and regulations regarding particular conduct.[9] Pleading oversight liability requires plaintiffs to demonstrate "a sufficient connection between the corporate trauma and the actions or inactions of the board" and, in Delaware courts, that connection has historically only been satisfied where a board fails to oversee compliance with "positive-law regulation" and the company subsequently violates the same positive-law regulation.[10] The court noted that it "remains an open question" whether *Caremark* liability may attach to a director's failure to oversee business risk (such as cybersecurity risk), but declined to resolve that issue, holding that plaintiffs' *Caremark* claim was inadequately pled even assuming this theory is viable.[11]

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."[12] The court emphasized

that, under *Caremark*, "a lack of good faith is a necessary condition" to finding oversight liability where, as here, the company charter exculpates directors from liability for duty of care violations.[13] Delaware courts have found two paths to plead the bad faith necessary to support a viable *Caremark* claim. Plaintiffs may plead bad faith "by way of either prong one, when the directors completely fail to implement any reporting or information system of controls, or via prong two, when directors, having implemented such a system or controls, consciously fail to monitor or oversee its operations."[14]

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)."[15] Thus, plaintiffs must plead particularized facts showing that the directors had "actual or constructive knowledge that their conduct was legally improper."[16] A complaint may make this showing by pleading that a director (i) violated positive law, (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.[17] The court held that plaintiffs failed to allege facts sufficient to support finding bad faith under any of these three avenues.

The court found that plaintiffs failed to adequately allege a violation of positive law, ruling that the Securities Exchange Commission's ("SEC") 2018 interpretative guidance requiring companies to "establish and maintain appropriate and effective disclosure controls and procedures, including those related to cybersecurity . . . does not establish positive law with respect to required cybersecurity *procedures* or how to manage cybersecurity risks."[18] Neither was the cybersecurity guide issued by the New York Stock Exchange – where SolarWinds' stock is listed – binding or positive law.[19]

Plaintiffs did not allege that the directors "intentionally acted with a purpose inimical to the corporation's best interest."[20]

Lastly, the court addressed the "stronger argument" that the facts as pled demonstrated a "lack of effective reporting system" because, according to plaintiffs, 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 leading up to the Sunburst attack.[21] During the relevant time period, the board charged two committees with oversight responsibility of the company's cybersecurity risks.[22] The court held that delegating oversight responsibility of a "particular risk in a particular year" to a "non-sham, functioning Committee" does not give rise to the inference that the board intentionally disregarded its oversight duties in bad faith.[23] Further, although the committees' failure to report to the full board regarding cybersecurity risk illustrated a "subpar reporting system" and "should have been, to a prudent director, of concern" because "good corporate practice requires director consideration of potential risks to customers; particularly so, perhaps, regarding cybersecurity," it did not amount to an "utter failure to attempt to assure" that a reporting system exists and, thus did not support an inference of an intentional sustained or systematic failure of oversight.[24] As to the liability of any committee member, the court held that it was "simply unwarranted" to hold committee

members liable for failing to "discuss one particular business risk with the full board over a period of 26 months while contending with the transition to life as a public company and the novel coronavirus pandemic."[25] According to the court, which issues a committee chooses to escalate to the full board is an exercise of business judgment protected by SolarWinds' exculpatory charter provisions.[26]

IMPLICATIONS

The court's decision in *SolarWinds* is significant because it analyzes the discharge of director duties in the context of navigating cybersecurity risk, which has come to the forefront for many companies in recent years. In 2021, the Delaware Court of Chancery in *Firemen's Retirement System of St. Louis on behalf of Marriott International, Inc*. v. *Sorenson*, while dismissing derivative "prong two" *Caremark* claims against directors of Marriott International, Inc. for failure to oversee cybersecurity risk following a data security breach exposing 500 million customers' personal information, noted that cybersecurity "is an area of consequential risk that spans modern sectors" and that the "corporate harms presented by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place."[27] The court clarified that the "growing risks posed by cybersecurity threats do not, however, lower the high threshold that a plaintiff must meet to plead a *Caremark* claim."[28]

The court in *SolarWinds* likewise acknowledged that cybersecurity presents a "peculiar kind of business risk" for online service providers such as SolarWinds because they "depend[] on their customers sharing access to the customers' information."[29] The resulting relationship makes cybersecurity "mission critical."[30] However, despite the significance of cybersecurity risk, the court held that cybersecurity is a "business risk" and emphasized that a director's failure to oversee business risk ordinarily is a protected exercise of business judgment that, without more, does not establish bad faith.[31]

Although plaintiffs failed to adequately allege violations of positive law in *SolarWinds*, companies in certain industries may be obligated by regulation to follow specific cybersecurity practices. Depending on the industry, the business, and the applicable regulations, cybersecurity could potentially be viewed not only as a business risk but as a central compliance risk that might, in certain circumstances, be sufficient grounds to support a Caremark claim.

Finally, while the court declined to find that the lack of reporting to the full board of directors on cybersecurity amounted to the intentional disregard by the board of its oversight duties in bad faith, companies should take notice of the *SolarWinds* court's characterization of the "subpar" reporting system between the board committees and the full board, and emphasis on the importance of director consideration of cybersecurity and other risks to customers. Particularly in light of emerging regulation, including the SEC's proposed cybersecurity rules, which underscore the role of the board in cybersecurity governance, companies should ensure they have a system in place for periodic reporting to the full board on cybersecurity.

* * *

ENDNOTES

1 *Construction Industry Laborers Pension Fund on behalf of SolarWinds Corporation, et al.* v. *Mike Bingle, et al.*, 2022 WL 4102492 (Del. Ch. Sept. 6, 2022).

2 Compl. ¶ ¶ 2, 19, 34 – 35.

3 *Id*. ¶ 33.

4 *Id*. ¶ 4.

5 *Id*. ¶ 4.

6 *SolarWinds*, 2022 WL 4102492, at *5.

7 *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959, 967 (Del. Ch. 1996).

8 Compl. ¶ ¶ 69, 102.

9 *SolarWinds* at *7 – 9.

10 *Id.* at *6 – 7.

11 *Id.* at *7 – 8.

12 *Id.* at *7.

13 *Id.* at *3, 8.

14 *Id.* at *9 (citing *Marchand* v. *Barnhill*, 212 A.3d 805, 820 – 24 (Del. 2019)).

15 *Stone* v. *Ritter*, 911 A.2d 362, 369 (Del. 2006).

16 *SolarWinds* at *9 (citing *In re Walt Disney Co. Derivative Litigation*, 906 A.2d 27 (Del. 2006) (emphasis in original)).

17 *Id.* at *10.

18 *Id.* at *9 (emphasis in original).

19 *Id.* at *9.

20 *Id.* at *10.

21 *Id.* at *11.

22 *Id.* at *11.

23 *Id.* at *11 – 13.

24 *Id.* at *13 – 14.

25 *Id.* at *13.

26 *Id.* at *13.

27 *Firemen's Retirement System of St. Louis on behalf of Marriott International, Inc.* v. *Sorenson*, 2021 WL 4593777, at *11 – 12 (Del. Ch. Oct. 5, 2021).

28 *Marriott*, 2021 WL 4593777, at *12.

29 *SolarWinds* at *1.

30 *Id.* at *1 (citing *Marchand*, 212 A.3d 805).

31 *Id*. at *1, 7, 13.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.