CARLTON FIELDS

Home Depot Cyber Derivative Action Shuttered: Another Data-Breach Derivative Suit Fails to Clear Fundamental Corporate Law Hurdles

CYBERSECURITY AND PRIVACY | SECURITIES AND DERIVATIVE LITIGATION | TECHNOLOGY | DECEMBER 7, 2016

John E. Clabby

Erin J. Hoyle

The recent dismissal of a Home Depot derivative action ends a string of high-profile derivative suits stemming from large-scale corporate data breaches. On November 30, the Northern District of Georgia dismissed a shareholder derivative action arising out of the September 2014 theft of millions of customers' credit card data from Home Depot's systems.[1] This follows earlier dismissals of derivative actions stemming from data breaches at Wyndham Worldwide Corporation[2] and Target Corporation.[3]

As in those earlier cases, traditional principles of corporate governance defeated claims that the company's officers and directors breached their fiduciary duties. In *Home Depot*, the court held that plaintiffs failed to fulfill the demand requirement before bringing the action and, in so holding, the court explained some of what the directors had done to meet their cyber duties.

Delaware law authorizes directors, not shareholders, to control the right to bring claims against officers and directors for breaches of corporate duties. Accordingly, pre-suit demand on the board is mandatory in derivative suits, absent plaintiffs' showing demand futility. Such a showing requires a shareholder-plaintiff to demonstrate that it would be impossible for a majority of the directors to exercise independent and disinterested business judgment when deciding whether to pursue the claims.

In *Home Depot*, plaintiffs alleged that the defendants breached their duty of loyalty by failing to institute sufficient internal controls to oversee cybersecurity risks and by disbanding a board committee that oversaw those risks. Plaintiffs also brought claims of corporate waste and inadequate proxy disclosures. Plaintiffs' claims included challenges to certain board decisions, but also complained of board inaction. Ultimately, the court agreed with the defendants and dismissed the complaint for plaintiffs' failure to fulfill the demand requirement.

To evaluate demand futility, the court applied to the three claims one or both prongs of the *Aronson* test, under which demand is excused only where the complaint alleges particularized facts creating reasonable doubt that (1) the directors are disinterested and independent on the subject or (2) the challenged transaction was otherwise the product of a valid exercise of business judgment.

First, the court considered the duty of loyalty claim, which was alleged as "a failure of oversight on the part of the Board." The court found that plaintiffs, to show demand futility for such a claim, "essentially need to show with particularized facts beyond a reasonable doubt that a majority of the Board faced substantial liability because it consciously failed to act in the face of a known duty to act." Plaintiffs failed to overcome what the court characterized as an "incredibly high hurdle."

Plaintiffs alleged that Home Depot's Infrastructure Committee, which had managed cybersecurity, was disbanded and that the Audit Committee, which was supposed to assume those responsibilities, had not amended its charter accordingly. The court saw past this formalism, explaining that, in fact "the Audit Committee received regular reports from management on the state of Home Depot's data security, and the Board in turn received briefings from both management and the Audit Committee."

Plaintiffs further alleged that while Home Depot had a plan in place to remedy deficiencies in Home Depot's data security, "in Plaintiffs' opinion it moved too slowly." The court explained that an allegation that "the Board's plan was not good enough" failed to meet a standard that required directors to "knowingly and completely fail[] to undertake their responsibilities." In language that should be a call to action for every public company board, the court explained:

> But in this case, the Complaint acknowledges that the Board acted before the Breach occurred. The Board approved a plan that would have fixed many of Home Depot's security weaknesses and it would be fully implemented by February 2015. With the benefit of hindsight, ***one can safely say that the implementation of the plan was probably too slow, and that the plan probably would not have fixed all of the problems Home Depot had with its security***. But the "Directors' decisions must be reasonable, not perfect." While the Board ***probably should have done more***, "[s]imply alleging that a board incorrectly exercised its business judgment and made a 'wrong' decision in response to red flags…is not enough to plead bad faith." (Emphases added.)

Second, the court considered plaintiffs' corporate waste claim, namely that the board made "insufficient reaction to the threat posed by the holes in Home Depot's data security," which caused losses to the company. As a threshold matter, the court noted that there was no transaction challenged by plaintiffs. This determination is important because corporate waste claims typically involve a gift, "an exchange of corporate assets for no corporate purpose" and a fact not alleged in this complaint. Accordingly, the court held that the "leisurely pace" in which the board upgraded Home Depot's cyber security was "squarely within the discretion of the Board" and therefore protected by the business judgment rule.

Third and finally, the court considered the alleged violations of Section 14(a) of the Securities Exchange Act, as to material omissions in the proxy disclosures. The court held that these allegations were subject to the demand requirement and governed under *Aronson*'s first prong, because the decision to include or omit statements in a proxy is a legal, not a business, decision. Applying the heightened pleading standards of the Private Securities Litigation Reform Act, the court held, among other things, that plaintiffs failed to identify the allegedly misleading false statements in the 2014 and 2015 proxy statements, failed to show the materiality of the purported omissions, and failed to explain how the alleged omissions caused the alleged losses. For these reasons, the court held that plaintiffs did not show beyond a reasonable doubt that defendants would have been interested in the litigation, because plaintiffs did not show a substantial likelihood of liability.

Accordingly, the court dismissed the derivative action, making *Home Depot* the latest in a series of unsuccessful attempts by shareholders to pursue derivative claims in the wake of a data breach.

The dismissal order in *Home Depot* looked a lot like that of *Palkon Homes*, the Wyndham data breach case. They were both demand futility cases that still took the opportunity to explore what conduct should be considered reasonable for a board facing cybersecurity risks. Both boards were active, considered cyber issues, and met frequently.

By contrast, the Target suit was dismissed not for demand futility but only after a 21-month investigation by a special litigation committee resulted in a determination that bringing claims against the board was not in the corporation's best interests.

Despite this string of successes for boards facing so-called "cyber *Caremark*" complaints, or, perhaps, *because of* the instruction contained within the dismissal opinions, boards should continue to make and document their responsible and reasoned decisions in tackling cybersecurity risks. And they should do so before, during, and after a breach. The *Home Depot* opinion shows that nearly any board action on cybersecurity beats doing nothing in the face of a known risk.

[1] *In re the Home Depot Inc. Shareholder Derivative Litigation* , Civil Action File No. 1:15-cv-0299-TWT, 2016 WL 6995676 (N.D. GA Nov. 30, 2016).

[2] *Palkon v. Holmes*, 2:14-CV-01234 SRC, 2014 WL 5341880 (D.N.J. Oct. 20, 2014).

[3] *Davis et al. v. Steinhafel et al.*, No. 14-cv-203 (D. Minn. July 7, 2016).