

Director Cyber Risk: Insights from Shareholder Derivative Lawsuits

By *Melissa J. Krasnow*

Shareholder derivative lawsuits regarding the Wyndham, Home Depot and Target cyber attacks provide insights on steps companies can take regarding director cyber risk.¹ These steps include: (1) determining fiduciary duties and monitoring shareholder derivative lawsuits for developments (this article covers both Delaware and Minnesota law), (2) reviewing organizational documents, applicable law and agreements, policies and insurance, (3) reviewing and considering company committee charters and privacy policies and Securities and Exchange Commission disclosures comprehensively and specifically regarding cyber risk, and (4) developing, implementing, testing, and updating incident response plans.

Determining Fiduciary Duties and Monitoring Shareholder Derivative Lawsuits for Developments

Delaware law is applicable in *Palkon v. Holmes* regarding Wyndham and *In re The Home Depot, Inc. Shareholder Derivative Litigation* regarding Home Depot because Wyndham and Home Depot are Delaware corporations. Delaware case law describes the director duty to monitor and oversee risks as derived from the duty of care and the duty of loyalty.²

Palkon v. Holmes addressed three cyber attacks against Wyndham between 2008 and 2010. The plaintiff was required to plead with particularity that the board's decision to refuse his demand to bring a lawsuit regarding the cyber attacks was in bad faith or not based on a reasonable investigation. The Wyndham board's decision to refuse the demand is under

the purview of the business judgment rule, under which there is a presumption that the board refused the demand on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company. Among other things, the defendants argued that the board's decision to refuse the demand was a good faith exercise of business judgment, made after a reasonable investigation.

The court dismissed the lawsuit with prejudice and described in a footnote the failure to act in good faith that is required to show director oversight liability (as part of the duty of loyalty):

Caremark requires that a corporation's "directors utterly failed to implement any reporting or information system...[or] consciously failed to monitor or oversee its operations thus disabling themselves from being informed." *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006). Yet Plaintiff concedes that security measures existed when the first breach occurred, and admits the Board addressed such concerns numerous times. (Compl. ¶¶ 46, 62, 63). The Board was free to consider such potential weaknesses when assessing the lawsuit.

The actions of Wyndham that were mentioned in this case included:

- (1) Board discussion of the cyber attacks, Wyndham's security policies, and proposed security enhancements at 14 meetings and audit committee discussion at 16 meetings between 2008 and 2012;
- (2) Wyndham hiring technology firms to investigate each cyber attack and issue recommendations on enhancing Wyndham's security;

Melissa J. Krasnow is a partner with Dorsey & Whitney LLP, a Certified Information Privacy Professional/US, and a National Association of Corporate Directors Fellow.

-
- (3) Wyndham beginning to implement such recommendations after the second and third cyber attacks, and
 - (4) Presentations of Wyndham's general counsel regarding the cyber attacks and Wyndham's data security generally at every quarterly board meeting.

The defendants' motion to dismiss filed on April 14, 2016, in *In re The Home Depot, Inc. Shareholder Derivative Litigation* states:

Loyalty claims based on alleged failure of oversight are widely recognized as "the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment." *In re Caremark Int'l., Inc. Deriv. Litig.*, 698 A.2d 959, 967 (Del. Ch. 1996). To state such a claim, a stockholder must plead particularized facts that the defendants "(a) utterly failed to implement any reporting or information system or controls or (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention. In either case, imposition of liability requires a showing that [defendants] knew that they were not discharging their fiduciary obligations." *Stone ex rel. AmSouth Bancorporation v. Ritter*, 911 A.2d 362, 370 (Del. 2006).

According to the defendants' motion to dismiss, the plaintiffs failed to state a duty of loyalty claim against any defendants.³

Target is a Minnesota corporation. The Minnesota corporate statute describes the standard of conduct for a director.⁴ Regarding *In re Target Corp. Shareholder Derivative Litigation*, the board of directors appointed a Special Litigation Committee to investigate the claims. The Special Litigation Committee completed its investigation and issued a report in March 2016, determining that it was not in Target's best interests to pursue the derivative claims and seeking dismissal of the claims with prejudice. On June 22, 2016, the Special Litigation

Committee and Defendants will move the court for approval and dismissal of the derivative actions with prejudice, asserting that

- (1) The members of the Special Litigation Committee were disinterested and independent, and
- (2) The Special Litigation Committee's investigative procedures and methodologies were adequate, appropriate and pursued in good faith, in satisfaction of the business judgment rule.⁵

The business judgment rule accords deference to the determination of the Special Litigation Committee regarding the derivative actions.

Finally, both breach of fiduciary duty claims and waste of corporate assets claims were made in *Palkon v. Holmes, In re The Home Depot, Inc. Shareholder Derivative Litigation* and *In re Target Corp. Shareholder Derivative Litigation*. According to Delaware case law, a "claim of waste will arise only in the rare, 'unconscionable' case where directors irrationally squander or give away corporate assets."⁶

In re The Home Depot, Inc. Shareholder Derivative Litigation and *In re Target Corp. Shareholder Derivative Litigation* should be monitored for developments, as should any other shareholder derivative lawsuits regarding cyber attacks.

Reviewing Organizational Documents, Applicable Law and Agreements, Policies and Insurance

According to the defendants' motion to dismiss in *In re The Home Depot, Inc. Shareholder Derivative Litigation*, Home Depot's Certificate of Incorporation contains language that precludes a duty of care claim against its directors.⁷ According to an order filed on May 23, 2016, Plaintiffs must file and serve their opposition to Defendants' motion to dismiss by June 30, 2016 and Defendants must file and serve their reply brief in further support of their motion to dismiss by July 20, 2016.

However, neither the Delaware corporate statute nor the Minnesota corporate statute permits eliminating or limiting the personal liability of a director to a corporation or its shareholders for monetary damages for breach of fiduciary duty for any breach of the director's duty of loyalty to the corporation or its shareholders or for acts or omissions not in good faith or that involve intentional misconduct or a knowing violation of law, among other things.⁸

Companies should review their organizational documents and applicable law and their indemnification agreements or policies and directors and officers liability insurance and cyber liability insurance coverage.

Reviewing and Considering Committee Charters, Privacy Policies, and SEC Filings

Palkon v. Holmes, In re The Home Depot, Inc. Shareholder Derivative Litigation, and *In re Target Corp. Shareholder Derivative Litigation* reference the companies': (1) audit committee charters, (2) Securities and Exchange Commission disclosures regarding cyber risk and attacks and (3) privacy policies, including language about the companies using industry standard methods to protect customer information.

Company committee charters and privacy policies and Securities and Exchange Commission disclosures should be reviewed comprehensively and specifically regarding cyber risk and attacks, including in terms of litigation.⁹ The foregoing also can be reviewed against similar items of companies in the same industry or that have experienced cyber attacks.

Developing, Implementing, Testing and Updating Incident Response Plans

Palkon v. Holmes, In re The Home Depot, Inc. Shareholder Derivative Litigation, and *In re Target Corp. Shareholder Derivative Litigation* address preparation regarding and response to cyber risk and attacks. Companies should develop, implement, test via simulated cyber

attack exercises, and update incident response plans in light of insights obtained from testing and legal, business, technological, and public relations developments to bolster preparation regarding and response to cyber risk and attacks.

Directors could ask the following questions regarding incident response plans:¹⁰

- (1) What is the date of the plan and what was the most recent date of testing the plan?
- (2) How frequently is the plan is tested or updated?
- (3) What was the situation that was the subject of the testing?
- (4) What are the results of and insights from the testing or updating of the plan?
- (5) Who are the members of the incident response team?
- (6) Who are the external team members (including service providers)?
- (7) What are team member responsibilities?
- (8) What are the lines of communication?
- (9) What communications, disclosures, and notifications are being considered?
- (10) What is the nature of and how frequently is employee security training and awareness provided?

Conclusion

In re The Home Depot, Inc. Shareholder Derivative Litigation and *In re Target Corp. Shareholder Derivative Litigation* should be monitored for developments, as should any other shareholder derivative lawsuits regarding cyber attacks. Companies also should: (1) determine fiduciary duties; (2) review organizational documents, applicable law, indemnification agreements or policies, directors and officers liability

insurance, and cyber liability insurance coverage; (3) review committee charters, privacy policies, and Securities and Exchange Commission disclosures in a comprehensive and specific manner regarding cyber risk and attacks, and (4) develop, implement, test via simulated cyber attack exercises, and update incident response plans.

Notes

1. See *Palkon v. Holmes*, No. 2:14-CV-01234 (D.N.J. Oct. 20, 2014); *In re The Home Depot, Inc. Shareholder Derivative Litigation*, No. 1:15-CV-2999 (N.D. Ga.) and *In re Target Corp. Shareholder Derivative Litigation*, No. 0:14-cv-00203 (D. Minn.).

2. *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006).

3. Regarding the failure to implement any reporting or information system or controls, the plaintiffs' complaint pleads that "... (i) the Audit Committee was established to assist the Board in reviewing and monitoring the Company's compliance programs (Comp., ¶ 49); (ii) the Audit Committee has 'primary responsibility for overseeing risks related to IT and data privacy and security at Home Depot' (*id.*, ¶ 278); (iii) internal audits were conducted on the Company's data security systems (*id.*, ¶¶ 141, 164, 205, 279); and (iv) the Company's IT Security and internal audit departments frequently reported to the Board and Audit Committee regarding cybersecurity issues (*id.*, ¶¶ 86–88, 97, 99, 103, 116, 120–123, 139–142, 150–153, 155, 157, 158, 160–163, 200, 205–209). Regarding showing that the defendants acted in bad faith by consciously failing to monitor or oversee its operations, the plaintiffs' allegations negate any claim that the defendants acted in bad faith in breach of the duty of loyalty":

- M. Carey "met regularly with Home Depot's Audit Committee and its full Board of Directors and provided the Board with updates regarding Home Depot's data security systems." (Comp., ¶97).
- M. Carey additionally briefed the Board on data breaches at other large retailers. (Comp., ¶¶76, 77).
- Management conducted regular scans and internal audits of the Company's cybersecurity systems, and reviewed those results with the Audit Committee and the Board. (Comp., ¶¶86, 150, 151, 162, 206, 207).
- Based on these scans and audits, M. Carey and his department planned and executed remedial measures and "enhancements" to the Company's data security systems. (Comp., ¶¶ 88, 118, 121, 150, 152, 200, 202–206, 230, 238, 239).
- Third-party consultants were retained to advise the Company on its cybersecurity measures and "to perform a 'health check' on its computer systems." (Comp., ¶¶101, 104, 136).

4. According to the Minnesota corporate statute:

A director shall discharge the duties of the position of director in good faith, in a manner the director reasonably believes to be in the best interests of the corporation, and with the care an ordinarily prudent person in a like position would exercise under similar circumstances. A person who so performs those duties is not liable by reason of being or having been a director of the corporation. Minn. Stat. § 302A.251, Subd. 1.

The Minnesota corporate statute further states:

(a) A director is entitled to rely on information, opinions, reports, or statements, including financial statements and other financial data, in each case prepared or presented by:

- (1) one or more officers or employees of the corporation whom the director reasonably believes to be reliable and competent in the matters presented;
- (2) counsel, public accountants, or other persons as to matters that the director reasonably believes are within the person's professional or expert competence; or
- (3) a committee of the board upon which the director does not serve, duly established in accordance with section 302A.241, as to matters within its designated authority, if the director reasonably believes the committee to merit confidence.

(b) Paragraph (a) does not apply to a director who has knowledge concerning the matter in question that makes the reliance otherwise permitted by paragraph (a) unwarranted. Minn. Stat. 302A.251, Subd. 2.

Good faith is defined in the Minnesota corporate statute as "honesty in fact in the conduct of the act or transaction concerned." Minn. Stat. § 302A.011, Subd. 13.

5. "Minnesota case law requires a court to 'defer to an SLC's decision to settle a shareholder derivative action if (1) the members of the SLC possessed a disinterested independence and (2) the SLC's investigative procedures and methodologies were adequate, appropriate, and pursued in good faith.'" *In re UnitedHealth Group Inc. Shareholder Derivative Litigation*, 754 N.W.2d 544, 559 (Minn. 2008).

6. *In re Walt Disney Co. Derivative Litigation*, 906 A.2d 27, 74 (Del. 2006). Under the Minnesota corporate statute, "[a] court may grant any equitable relief it deems just and reasonable in the circumstances... (b) In an action by a shareholder when it is established that... (5) the corporate assets are being misapplied or wasted...." Minn. Stat. § 302A.751, Subd. 1.

7. According to Article 9 of Home Depot's Certificate of Incorporation:

No director of the Corporation shall be liable to the Corporation or its stockholders for monetary damages for breach of fiduciary duty as a director, except for liability (i) for any breach of the director's duty of loyalty to the Corporation or its stockholders, (ii) for acts or omissions not in good faith or which involve intentional misconduct or a knowing violation of law, (iii) under Section 174 of the Delaware General Corporation Law, or (iv) for any transaction from which the director derived an improper personal benefit.

8. Del. Gen. Corp. Law § 102(b)(7); Minn. Stat. § 302A.251, Subd. 4.

9. See Division of Corporation Finance, US Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011); Melissa Krasnow, "The Securities and Exchange Commission's Guidance on Cybersecurity and Cyber Incident Disclosure," *BNA Privacy & Security Law Report* (Oct. 31, 2011).

10. See Melissa Krasnow, "Guidance for Guidance for Incident Response Plans," International Risk Management Institute (May 2015).