Bloomberg BNA

Privacy and Security Law Report®

Cybersecurity for Directors

As the world of cybersecurity risk evolves, companies and their directors and officers should continue to engage in and enhance cyber risk oversight practices and to monitor and consider developments in shareholder derivative lawsuits regarding cyberattacks, regulatory enforcement actions and legal, regulatory and industry developments and cyber events, the author writes.

Developments in Director Oversight of Cybersecurity Risk

BY MELISSA KRASNOW

This article provides an update on developments in director oversight of cybersecurity risk in 2016. The first part of this article notes a data security regulatory enforcement action and covers the dismissals of shareholder derivative lawsuits regarding the Wyndham Worldwide Corp., Home Depot Inc. and Target Corp. cyberattacks and the shareholder derivative lawsuit filed regarding the Wendy's Co. cyberattack (Wyndham, Home Depot, Target and Wendy's are public companies). The second part of this article addresses steps that public companies and their directors are taking regarding cybersecurity as reported by the 2016-2017 NACD Public Company Governance Survey.

Melissa J. Krasnow is a partner with VLP Law Group LLP, in Minneapolis, Minn., and practices in the areas of domestic and cross-border privacy and data security, technology transactions, and mergers and acquisitions. Krasnow is a Certified Information Privacy Professional/U.S. and a National Association of Corporate Directors Board Leadership Fellow.

Data Security Regulatory Enforcement Action and Shareholder Derivative Lawsuits

Dwolla Data Security Regulatory Enforcement Action

Director cybersecurity responsibility has garnered regulator attention. In February 2016, the Consumer Financial Protection Bureau (CFPB) issued its first data security enforcement action against online payment platform Dwolla Inc., a Delaware corporation. The consent order describes requirements for Dwolla's board of directors in addition to data security measures that Dwolla must take. According to the CFPB, ''. . .[Dwolla's] Board will have the ultimate responsibility for proper and sound management of [Dwolla] and for ensuring that it complies with Federal consumer financial law and this consent order.'' *See In the Matter of Dwolla, Inc.*, File No. 2016-CFPB-0007 (CFPB Feb. 27, 2016). *See also* Melissa Krasnow, ''CFPB Issues First Data Security Action,'' International Risk Management Institute (March 2016).

Shareholder Derivative Lawsuits

Following dismissals of the shareholder derivative lawsuits regarding the Wyndham, Home Depot and Target cyberattacks, a shareholder derivative lawsuit regarding the Wendy's cyberattack was filed. Wynd-

 ISSN 1538-3423

ham, Home Depot and Wendy's are Delaware corporations, whereas Target is a Minnesota corporation.

Wyndham Shareholder Derivative Lawsuit Dismissal (Delaware Law)

Directors owe fiduciary duties to the corporation—the duty of care and the duty of loyalty. Delaware case law describes the director duty to monitor and oversee risks as derived from the duty of care and the duty of loyalty. *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006).

In 2014, the U.S. District Court for the District of New Jersey dismissed the Wyndham shareholder derivative lawsuit in *Palkon v. Holmes* with prejudice and described the failure to act in good faith (as part of the duty of loyalty) that is required to show director oversight liability in a footnote:

> 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.

Palkon v. Holmes, No. 2:14-CV-01234 (D.N.J. Oct. 20, 2014).

According to the Delaware Supreme Court in *Stone v. Ritter*, ''The failure to act in good faith may result in liability because the requirement to act in good faith 'is a subsidiary element[,]' i.e., a condition, 'of the fundamental duty of loyalty.' It follows that because a showing of bad faith conduct, in the sense described in Disney Co. and Caremark, is essential to establish director oversight liability, the fiduciary duty violated by that conduct is the duty of loyalty.'' *Stone v. Ritter*, 911 A.2d 362, 369-370 (Del. 2006).

Home Depot Shareholder Derivative Lawsuit Dismissal (Delaware Law)

In *In re The Home Depot, Inc. Shareholder Derivative Litigation*, the plaintiffs' primary claim for liability was that the directors breached their duty of loyalty to Home Depot regarding the breach of Home Depot's payment data systems as confirmed by Home Depot in 2014.

According to the U.S. District Court for the Northern District of Georgia, Atlanta Division:

> . . .the [p]laintiffs essentially need[ed] 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. This is an incredibly high hurdle for the [p]laintiffs to overcome, and it is not surprising that they fail[ed] to do so.

In re The Home Depot, Inc. Shareholder Derivative Litig., No. 1:15-CV-2999 (N.D. Ga. Nov. 30, 2016).

The court noted that the complaint ''. . .details numerous instances where 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. Based on those facts alone, there can be no question that the Board was fulfilling its duty of loyalty to ensure that a reasonable system of reporting existed.'' *Id*.

The court further stated, ''. . .Delaware courts have held that '[b]ad faith cannot be shown by merely showing that the directors failed to do all they should have done under the circumstances.' *Wayne Cty. Employees' Ret. Sys. v. Corti*, No. CIV.A. 3534-CC (Del. Ch. July 24, 2009), *aff'd*, 996 A.2d 795 (Del. 2010). Rather, they use language like 'utterly' and 'completely' to describe the failure necessary to violate the duty of loyalty by inaction.'' *See Lyondell*, 970 A.2d at 243-44 (''knowingly and completely failed to undertake their responsibilities,'' and ''the inquiry should have been whether those directors utterly failed to attempt to obtain the best sale price.''). *Id*.

According to the court: ''...'Directors' decisions must be reasonable, not perfect.' *Lyondell*, 970 A.2d at 243. 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.' '' Melbourne Mun. Firefighters' Pension Trust Fund on Behalf of Qualcomm, Inc. v. Jacobs, C.A. No. 10872-VCMR (Del. Ch. Aug. 1, 2016). *Id*.

On Nov. 30, 2016, the court granted plaintiffs' motion to dismiss because plaintiffs failed to show that demand was futile on any of the claims alleged, including the duty of loyalty claims. *Id*.

Wendy's Shareholder Derivative Lawsuit (Delaware Law)

In the Wendy's shareholder derivative lawsuit in *Graham v. Peltz*, the plaintiff alleged that the defendants breached their fiduciary duties of loyalty, care and good faith, among other things, relating to a point-of-sale systems breach that was acknowledged by Wendy's in January 2016. *Graham v. Peltz*, No. 1:16-CV-1153 (S.D. Ohio Dec. 16, 2016).

Target Shareholder Derivative Lawsuit Dismissal (Minnesota Law)

In *In re Target Corp. Shareholder Derivative Litig.*, the plaintiffs alleged that the defendants breached their fiduciary duties to Target regarding an intrusion by hackers into Target's point-of-sale systems that was announced by Target in 2013. Target's board of directors established a Special Litigation Committee pursuant to Minnesota law to investigate the claims, allegations and requests for relief made in the derivative action, to analyze the rights and remedies of Target and to determine whether and to what extent Target should pursue any such claims. In March 2016, the Special Litigation Committee issued a report to Target's board that concluded it would not be in the best interests of Target to pursue any of the alleged derivative claims and that the derivative action and the alleged derivative claims should be dismissed. The business judgment rule accords deference to the determination of the Special Litigation Committee regarding a derivative action. In July 2016, the U.S. District Court for the District of Minnesota granted the motions to dismiss the derivative action of the Special Litigation Committee, Target and the defendants and ordered that the derivative action be dismissed with prejudice. *In re Target Corp. Shareholder Derivative Litig.*, No. 0:14-CV-00203 (D. Minn. July 7, 2016).

The Minnesota corporate statute describes the standard of conduct for a director. According to the Minnesota corporate statute: ''A director shall discharge the

   ISSN 1538-3423

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.

Eighty-nine percent of respondents indicated that cybersecurity is discussed regularly during board meetings, according to 2016-2017 the National Association of Corporate Directors Public Company Governance Survey.

While the Delaware and Minnesota corporate statutes, respectively, provide for a provision in a corporation's articles of incorporation eliminating or limiting the personal liability of a director to a corporation or its shareholders for monetary damages for breach of fiduciary duty as a director, neither 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. *See* Del. Gen. Corp. Law § 102(b)(7); Minn. Stat. § 302A.251, Subd. 4. *See also*, Melissa Krasnow, ''Director Cyber Risk: Insights from Shareholder Derivative Lawsuits,'' The Corporate Governance Advisor (July/August 2016). Companies should review their organizational documents and applicable law and their indemnification agreements or policies and directors and officers liability insurance and cybersecurity liability insurance coverage.

Steps Public Companies and Their Directors are Taking Regarding Cybersecurity

In December 2016, the National Association of Corporate Directors (NACD) issued the **2016-2017 NACD Public Company Governance Survey** which provides information about: (1) board and committee oversight of cyber risk, (2) frequency of director discussion of cybersecurity, (3) reporting to the board about cybersecurity, (4) satisfaction with information about cybersecurity and (5) 15 cyber risk oversight practices performed by the board in the last 12 months.

Survey respondents were from the following types of companies: 18 percent were from companies with equal to or greater than $10 billion in market capitalization, 30 percent were from companies with $2 billion to less than $10 billion in market capitalization, 34 percent were from companies with $300 million to less than $2 billion in market capitalization and 18 were percent from companies with less than $300 million in market capitalization. Sixty-eight percent of respondents were independent directors, 17 percent were general counsels/corporate secretaries, 11 percent were CEOs/other corporate executives and 3 percent were non-independent directors. Twelve percent of respondents serve as the chair or lead director of their board and 41 percent chair at least one board committee.

Board and Committee Oversight Over Cyber Risk

Fifty-one percent of respondents indicated that cyber risk is allocated to the audit committee, whereas 41 percent said that cyber risk is allocated to the full board. 11 percent said that cyber risk is allocated to a specialized risk committee and 4.5 percent said that cyber risk is allocated to a technology committee.

Frequency of Director Discussion of Cybersecurity

Eighty-nine percent of respondents indicated that cybersecurity is discussed regularly during board meetings. The frequency of these discussions varies, from once per year to once per month. Boards hold a median of three discussions per year about cybersecurity.

According to Aggregate Survey results, 14 percent of respondents said that cybersecurity was discussed during board meetings after a breach in their company's industry, 13 percent said that cybersecurity was discussed during board meetings after an internal breach and 7 percent said that cybersecurity matters were not discussed at the board level.

Reporting to the Board About Cybersecurity

The following percentages of respondents indicated that the following report to the board about cybersecurity: (1) the chief information officer (62 percent), (2) the head of internal audit (38 percent), (3) the CEO (37 percent), (4) the chief information security officer (CISO) (31 percent), (5) the general counsel (25 percent), (6) the head of risk (21 percent) and (7) compliance officer (11 percent).

Satisfaction With Information About Cybersecurity

Though 61 percent and 15 percent of respondents indicated that they were satisfied and very satisfied, re-

spectively, with the information about cybersecurity, 24 percent expressed dissatisfaction with the quality of cyber risk information provided to the board by management.

The respondents who were dissatisfied cited the following reasons for dissatisfaction, with percentages. The information the respondents receive: (1) does not allow for effective benchmarking (46 percent), (2) does not provide enough transparency concerning performance issues (33 percent), (3) is difficult to interpret (24 percent), (4) is filtered for the board (19 percent), (5) is not timely enough (18 percent), (6) is too retrospective (5 percent) and (7) is too numbers-focused, making it difficult to glean real insight (5 percent).

15 Cyber Risk Oversight Practices Performed by the Board in the Last 12 Months

The following percentages of respondents described 15 cyber risk oversight practices performed by the board in the last 12 months:

(1) reviewed the company's current approach to protecting its most critical data assets (77 percent);

(2) reviewed the technology infrastructure used to protect the company's most critical data assets (74 percent);

(3) communicated with management about the types of cyber risk information the board requires (64 percent);

(4) reviewed the company's response plan in the case of a breach (59 percent);

(5) assessed risks associated with third-party vendors or suppliers (50 percent);

(6) assessed risks associated with employee negligence or misconduct (45 percent);

(7) assigned clearly defined roles to its standing committees regarding cyber risk oversight (44 percent);

(8) discussed the legal implications of a breach (37 percent);

(9) leveraged internal advisors, such as internal auditors or the general counsel, for in-depth briefings (37 percent);

(10) reviewed the scope of cyber coverage in the case of an incident (33 percent);

(11) assigned clearly defined roles to the full board regarding cyber risk oversight (32 percent);

(12) attended continuing education events on cyber risk (31 percent);

(13) leveraged external advisors, such as consultants or government agencies (e.g., FBI), to understand the risk environment (31 percent);

(14) conducted a post-mortem review following an actual or potential incident (21 percent); and

(15) participated in a test of the company's response plan (12 percent).

See also Melissa Krasnow, ''Guidance for Guidance for Incident Response Plans,'' International Risk Management Institute (May 2015); Federal Trade Commission, ''Data Breach Response: A Guide for Business'' (September 2016); and National Institute of Standards and Technology Special Publication 800-184, ''Guide for Cybersecurity Event Recovery'' (December 2016)..

Conclusion

As the world of cybersecurity risk evolves, companies and their directors and officers should continue to engage in and enhance cyber risk oversight practices and to monitor and consider developments in the Wendy's shareholder derivative lawsuit in Graham v. Peltz and other shareholder derivative lawsuits regarding cyberattacks, regulatory enforcement actions and legal, regulatory and industry developments and cyber events.

  PVLR ISSN 1538-3423