When D&O Coverage Becomes A Significant Asset in Response to a Data Breach

By Matthew L. Jacobs and Sabrina N. Guenther

It seemed like not a month went by in 2014 without the announcement of a large or high-profile breach of consumer data. There were enough data breaches that 60 Minutes termed 2014 "The Year of the Data Breach." Home Depot estimated that 56 million payment cards were likely compromised in the cyberattack at its stores, making it a larger data breach than the Target breach in 2013. Through June 2014, Target had incurred costs of $148 million related to its breach, in which hackers stole at least 40 million payment card numbers and 70 million other pieces of customer data. As compared to 2013, the number of incidents detected by respondents increased by 48 percent in 2014 data, climbing to 42.8 million.[1] That number comes out to 117,339 incoming attacks each day. Moreover, the annual average financial loss for cybersecurity incidents for 2014 was $2.7 million, a 34 percent increase over the previous year.[2] Although 2014 has ended, every indication suggests businesses will continue to face challenges in 2015 to their data security and that, with the continued proliferation of consumer data, responding effectively to those challenges will become increasingly critical and expensive.

At minimum, businesses that suffered data breaches in 2014 will continue to face fallout from those breaches. Credit card issuing and acquiring banks incur millions of dollars in replacing credit cards, providing credit monitoring services to their customers and reimbursing customers for unauthorized transactions. Those banks then pursue the retail businesses whose points of sales were compromised, pursuant to agreements they have with such businesses allowing the use of various credit and debit cards at the retail establishments. In addition to the costs of remediating their own data breaches, notifying consumers, and responding to regulators – and possibly paying significant fines and penalties - several companies that fell victim to data breaches in 2014 also must defend against putative class action lawsuits, including derivative lawsuits brought by shareholders.

Plaintiffs have sued Target, Wyndham, Home Depot, and most recently, Sony Pictures – among others – in connection with the data breaches those businesses suffered in the past few years. Some of these complaints specifically target the companies' directors and officers – alleging that those directors and officers breached fiduciary duties by failing to take appropriate steps to protect the personal consumer information that had been stolen as a result of the various data breaches.

For example, one complaint against Target's directors and officers alleges that those directors and officers breached their fiduciary duties to shareholders by "failing to implement a system of internal controls to protect customers' personal and financial information" and "causing or allowing [Target] to conceal the full scope of the data breach, which affected at least seventy million customers."[3] The defendants have not yet answered or moved to dismiss the complaint, but on December 10, 2014, the parties submitted a joint report to the Court, in which they agreed that all shareholder actions should be stayed until March 16, 2015, to allow a Special Litigation Committee appointed by Target's Board of Directors to complete its investigation.[4] In the meantime,

several non-shareholder claims arising from the Target breach have survived motions to dismiss.[5]

The November 2014 hack of Sony Pictures' employees' personal information offers another example of a data breach that led to putative class action suits. One such complaint against Sony Pictures alleges, among other things, that Sony failed to secure its network and adequately protect employees' data.[6] Sony Pictures has until February 9, 2015, to answer that complaint.[7] As of January 7, 2015, Sony Pictures faces a total of seven class action complaints arising from the November 2014 hack. So far, none of the plaintiffs include Sony Pictures' shareholders.

Some business victims of cyberattacks have succeeded in defending against similar claims following data breaches. On October 20, 2014, the U.S. District Court for the District of New Jersey dismissed a shareholders' derivative action against Wyndham Worldwide Corporation's directors and officers. The plaintiff had sued the directors and officers in connection with the data breaches suffered by Wyndham from 2008 to 2010. In granting Wyndham's motion to dismiss, Judge Chesler applied the business judgment rule to the defendants' refusal of the plaintiff's demand, specifically noting that the Wyndham board had met multiple times regarding the breaches and ordered its own investigation of the incidents.[8]

No matter the outcomes, the lawsuits against Target, Sony Pictures and Wyndham convincingly demonstrate what data privacy and data security experts – including federal regulators – have highlighted as a board-level issue and one that merits C-suite attention. It therefore follows that liability insurance at the board and C-suite levels – namely, directors and officers insurance (D&O Policies) – may be implicated.

Directors and officers insurance affords coverage at several levels. D&O Policies typically include Side A, B, and C coverage. Side A coverage protects a corporation's directors and officers when the corporation cannot or will not indemnify those directors and officers. Side B coverage protects the organization by affording reimbursement when it indemnifies its directors and officers, thereby protecting the corporation's balance sheet. Finally, Side C coverage – also known as "entity" coverage – typically affords coverage to the entity itself when the entity is sued, along with directors and officers, but often only in the context of a securities action. Each of these types of coverage normally includes coverage, or advancement, of defense costs, both for litigation and for criminal and regulatory investigations that qualify as "claims" under the policies. These coverages could be critical for companies like Target, Sony Pictures and Wyndham, who have faced or continue to face multiple inquiries and lawsuits arising from data breaches.

Thus far, there have been no reported cases regarding the application of D&O Policies to class action lawsuits arising out of data breaches. D&O Policies are designed to cover acts that directors and officers take in their roles as directors and officers. The allegations in the Target, Sony Pictures, and other lawsuits discussed above appear to fall directly within that purpose, sufficient to justify notice to the insurer and to fall within the coverage grant of the policies. The ultimate availability of coverage, however, always will depend upon the application of the policy's terms, conditions, provisions and exclusions as applied to the specific facts of the claim for which coverage is being sought.

Businesses inevitably will continue to face challenges to their data security. Protecting against those challenges will continue to merit scrutiny and attention at the highest levels of all businesses, and not just within the Risk Management or Treasury Departments. In responding to these incidents and minimizing potential hits to the bottom line, businesses should look to their insurance portfolios in addition to their infrastructure and data security measures. Specifically, businesses should reassess their current coverages, including their D&O Policies, in light of the various risks posed by potentially significant data breaches. Business also should consider adding insurance claims notifications – including those made under both cyberinsurance policies and D&O Policies – to their incident response plans for cyber breaches.

[1] PricewaterhouseCooper, The Global State of Information Security Survey 2015, p.7 (Sept. 30, 2014).

[2] *Id.* at p.10.

[3] Complaint ¶ 76, *Kulla v. Steinhafel, et al.*, No. 14-cv-00203-SRN-JSM (D. Minn. Jan. 21, 2014) .

[4] Dkt. 51, *Kulla v. Steinhafel, et al.*, No. 14-cv-00203-SRN-JSM (D. Minn. Dec. 10, 2014).

[5] *In re Target Corp. Data Sec. Breach Litig.*, --- F.Supp.3d ----, 2014 WL 7192478 (D. Minn. Dec. 18, 2014); *In re Target Corp. Data Sec. Breach Litig.*, --- F.Supp.3d ----, 2014 WL 6775314 (D. Minn. Dec. 2, 2014).

[6] Complaint ¶ ¶ 99-100, *Corona, et al. v. Sony Pictures Entmt., Inc.*, No. 14-cv-09600 (C.D. Calif. Dec. 15, 2014).

[7] Dkt. 28, *Corona, et al. v. Sony Pictures Entmt., Inc.*, No. 14-cv-09600 (C.D. Calif. Jan. 2, 2015).

[8] *Palkon v. Holmes*, No. 14-cv-1234, 2014 WL 5341880 (D.N.J. Oct. 20, 2014).

CONTACT US

Matthew L. Jacobs, Partner, Jenner & Block

Phone: 202 639-6096 Email: mjacobs@jenner.com Download V-Card

Sabrina N. Guenther, Associate, Jenner & Block

Phone: 312 840-7299 Email: sguenther@jenner.com Download V-Card