Shook, Hardy & Bacon L.L.P.

NOVEMBER 21, 2014

DATA SECURITY ALERT

Shook, Hardy & Bacon understands companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

For more information on SHB's data security and data privacy capabilities, please contact:

Al Saikali
(305) 960-6923
asaikali@shb.com

James Eiszner
(816) 559-2140
jeiszner@shb.com

Zach Chaffee-McClure
(816) 559-2404
zmcclure@shb.com

DIRECTOR AND OFFICER LIABILITY IN CYBERSPACE: INVESTIGATE AND INSURE

Today, any company that accepts credit cards is likely at some risk of a cyberattack or data breach. Threats to information security are like natural disasters in the sense that one can take every precaution and yet still not be 100-percent safe. And with each publicized data breach comes litigation, irrespective of whether or not any cardholder was actually harmed by the breach. Although data security litigation is a relatively new frontier, two new developments to date highlight potential ways to manage the risks of liability that may result from data breaches.

The Securities and Exchange Commission has warned companies that threats to data security are among the most significant risks that corporate directors and officers must manage carefully.[1] Some companies, among them the entities behind Wyndham Hotels and Target, suffered attacks on their computer systems that accessed customers' personally identifiable information (PII). Not surprisingly, derivative suits against these companies followed,[2] generating uncertainty in the board room about the liability risks from cyberattacks. But recent developments have helped to reduce that uncertainty.

First, the Wyndham Board of Directors recently prevailed in its cyber-derivative suit, with the court dismissing the derivative suit because the board had adequately investigated the derivative claim and decided it was not in the interests of the company to pursue it, under the business judgment rule.[3] The decision suggests that a board which adequately investigates a shareholder demand that the company take action against officers and directors for an alleged failure to protect the company from cyber-liability may find protection, even if the reasons for its refusal to take action are weak. This is a welcome finding for many corporate boards, but it remains to be seen whether the court presiding over the Target board's derivative suit[4] will reach a similar conclusion.

While companies can take heart that the opinion signals derivative suits may not be easy at the pleading stage, they should not relent in their efforts to protect the company and its shareholders from the risk of cyberattacks. Doing so not only protects the goodwill of individuals whose PII is in the possession of the company, it also deters shareholder allegations that company officers and directors have failed to protect the company from data security threats.

The second recent development highlights another way to enhance protection from derivative suits alleging a failure to protect the company from cyber-liability. Like any natural disaster, cyber threats can be insured against – officers and directors should investigate purchasing insurance that covers liability to customers for the loss of their PII. But carefully managing the pitfalls with cyber-insurance coverage is important. The newly filed case of *Travelers Indemnity Co. v. P.F. Chang's China Bistro, Inc.*[5] is not a derivative suit or a class action. It is an insurance coverage suit. P.F. Chang's suffered a hacking incident that resulted in the loss of customers' PII. Predictably, customers brought class action lawsuits alleging P.F. Chang's failed to protect their PII. P.F. Chang's then notified its commercial general liability insurer, Travelers, of these suits and asked the insurer to pay for the defense of these suits and to indemnify P.F. Chang's for any adverse judgment. That request prompted Travelers' move for a declaratory judgment that it had no duty to defend or indemnify P.F. Chang's under its commercial general liability policy.

Although in its infancy, this case bears careful watching because its outcome will significantly affect the defense of cyber-derivative suits. If the court determines that Travelers has a duty to defend under a commercial general injury liability policy, that decision will mean companies that have general commercial liability policies – as most do – have adequately managed the risk of cyber-liability by procuring the policy. Derivative lawsuits alleging a failure to protect the company from cyber-liability may be significantly scaled back. If, as seems likely,[6] the court determines that general commercial liability policies do not cover loss of customers' PII from cyber-attacks, then companies like P.F. Chang's[7] may find themselves subject to new derivative suits which allege that company officers wasted corporate assets by failing to procure adequate coverage against liability arising from a cyberattack that results in the loss of customers' PII.

Companies are always urged to protect their computer systems from incursion by hackers. That advice remains solid, but it is incomplete. As the *Travelers* lawsuit indicates, companies should also ensure they have adequate coverage for the costs associated with cyberattacks and that they should do so *before*, rather than after, a cyberattack occurs. Doing so not only manages the risk to the company from cyber-liability but also prevents the company from being in the untenable position of having to defend a derivative suit for failure to manage that liability where "Exhibit 1" to the derivative complaint is the decision in the insurer's declaratory judgment action indicating the company

has no coverage because it failed to understand the terms of its policy. While the Wyndham board's victory suggests that the business judgment rule significantly limits the risk of derivative suit liability for cyberattacks, courts may not find that the board's investigation of the risks of cyber-liability was adequate if the company's own coverage suit indicates that the company did not understand its insurance coverage for cyber-liability.

The coverage issues relating to cyber-liability will require vigilence. The insurance industry will surely react to the recent litigation over coverage and will alter their policies to be sure they limit their exposure only to the cyber-liabilities they intend to cover. Companies must watch policy language and monitor the evolving case law to be sure they are getting the coverage they seek. For example, coverage may or may not extend to the costs the company incurred in complying with varying state laws requiring notification requirements for data breaches or losses stemming from reputational harm to the company's image.[8] Moreover, cyber-liability coverage for the company may not insure against the costs of defending directors and officers from the costs of defending derivative suits arising from data breaches, and companies cannot simply assume a D&O policy will automatically provide such complete protection.[9]

If data breaches continue to make the news, and if lawsuits continue to follow, courts can be expected to develop the law on just how much diligence and forethought (or lack of it) "business judgment" will excuse. Officers and directors who appropriately investigate the risks of cyber-liability and require that their companies obtain appropriate cyber-liability insurance coverage may protect customers' PII and themselves at the same time.

By James Eiszner and Zach Chaffee-McClure

OFFICE LOCATIONS
Denver, Colorado
+1-303-285-5300
Geneva, Switzerland
+41-22-787-2000
Houston, Texas
+1-713-227-8008
Irvine, California
+1-949-475-1500
Kansas City, Missouri
+1-816-474-6550
London, England
+44-207-332-4500
Miami, Florida
+1-305-358-5171
Philadelphia, Pennsylvania
+1-215-278-2555
San Francisco, California
+1-415-544-1900
Seattle, Washington
+1-206-344-7600
Tampa, Florida
+1-813-202-7100
Washington, D.C.
+1-202-783-8400

1. Securities & Exchange Commission, Corporate Finance Disclosure Topic No. 2, Cybersecurity (October 11, 2011).
2. Law 360, "Target Execs Slapped With Investor Suit Over Data Breach," (January 29, 2014); LexisNexis Legal Newsroom, "Wyndham Worldwide Board Hit With Cyber-Breach Derivative Lawsuit," (May 7, 2014).
3. Palkon v. Holmes, No. 2:14-cv-01234 (SRC), 2014 U.S. Dist. LEXIS 148799 (D.N.J. Oct. 20, 2014).
4. Collier v. Steinhafel, No. 0:14-cv-00203 (D. Minn. Jan. 21 2014).
5. Complaint, Travelers Indem. Co. v. P.F. Chang's China Bistro, Inc., Case No. 3:14-cv-01458-VLB (D. Conn. Oct. 2, 2014).
6. A search of the Travelers website reveals that the company offers policies and riders that will extend coverage to cover cyber-liability. In addition, Travelers' complaint cites to policy definitions that would appear to exclude theft of PII as a covered injury under its general commercial liability policy.
7. P.F. Chang's is not the first company to find that its insurance coverage might not cover cyber intrusions. See, e.g., United Westlabs, Inc. v. Greenwich Ins. Co., Docket 09C-12-048(MMJ), 2011 WL 2623932 (Del. Super. Ct. June 13, 2011) (granting declaratory judgment of no coverage of cyber-extortion threat); Retail Ventures, Inc. v. Nat'l Union Fire of Pittsburgh, 691 F.3d 821 (6th Cir. 2012) (denial of coverage breached the policy because there was an adequate link between the insured's losses and the data intrusion); Zurich Am. Ins. Co. v. Sony Corp. of Am., Index No. 651982/2011 (N.Y. Sup. Ct. Feb. 21, 2014) (upholding coverage denial because covered injuries from publication of privacy information must be done by insured, not the hackers).
8. See E. McGinn, T. Sporkin, A. Lutch, & J. Shreve, "The Board of Directors and Cybersecurity: Setting Up the Right Structure," 83 U.S. Law Week. 744 (Nov. 18, 2014).
9. Kevin Kalinich & Michael Becker, "Cyber Risk: Are Boards the New 'Target'?" http://ww2.cfo.com/risk-management/2014/04/cyber-risk-boards-new-target/.