BRYAN CAVE
A Broader Perspective
Bulletin

Data Privacy & Security Team

To: Our Clients and Friends August 26, 2013

General Liability Insurance May Not Cover Cyber Risks

With the cost of data breaches on the rise, businesses should evaluate whether they have a need for cyber insurance. On August 14, 2013, Liberty Mutual Insurance Company ("Liberty Mutual") filed a declaratory judgment action in connection with eight data breach lawsuits and five written demands against its insured, Schnuck Markets, Inc. ("Schnucks"), a private supermarket chain. Seven of the lawsuits seek class certification. According to a press release from Schnuck dated April 15, 2013, approximately 2.4 million credit and debit cards used at 79 out of 100 of its stores may have been compromised by a data breach.

According to Liberty Mutual's Complaint, Schnucks sought coverage for the lawsuits and demands from Liberty Mutual under its excess commercial general liability policy ("CGL Policy") with a liability limit of $1.5 million, subject to a self-insured amount of $500,000 and a $20 million general aggregate limit. In the declaratory judgment lawsuit, Liberty Mutual's position is that coverage does not apply under the CGL Policy because electronic data is not tangible property and, if there is coverage, its indemnification obligations are limited. Among the reasons that Liberty Mutual alleges are that there are no allegations of "bodily injury" or "property damage" against Schnucks, there is no "occurrence," the relief sought does not constitute "damages," and the damages were not because of "personal and advertising injury" or oral or written publication or material.

As the *Schnucks* case illustrates, a company's general liability insurance policy may not provide coverage for the liabilities that a company can face if a data breach occurs, and a company will likely face additional litigation in the form of a coverage action with its insurer if it seeks coverage under a typical general liability policy. Businesses should consider purchasing cyber insurance to provide greater certainty of coverage against a hacker attack and other types of cyber-related incidents. Cyber insurance policies may cover crisis management expenses, such as notifying affected parties after a data breach, public relations, and forensic investigations. In addition, cyber insurance policies may cover the costs of defending lawsuits, regulatory response costs, lost revenue, or the restoration of lost or stolen data. The majority of states have data breach laws in place, and cyber insurance policies may cover certain response expenses required to comply with notification regulations as well as costs necessary to mitigate any damage to the company's reputation.

Businesses must also be mindful of who ultimately foots the bill for losses resulting from a data breach. In a typical credit or debit card transaction, the customer's information is sent to the merchant's

acquiring bank or credit card processor.[1] From there, the transaction passes to the large credit card company and then to the bank that issued the card. When a customer discovers fraudulent charges, the issuing bank is required to compensate the customer under its agreement with the large credit card company. An issuing bank can then pursue the merchant for reimbursement. If the merchant can prove that it abided by all Payment Card Industry Data Security Standards, the merchant bank may absorb the losses. However, the issue of who pays frequently leads to a lawsuit between the bank and the merchant. In addition, as shown by the *Shnucks* case, retailers are often sued by their customers when a data breach occurs. Thus, issuing banks and retailers appear to carry the costs associated with a data breach, while credit card companies appear to be shielded by contract.[2]

According to a recent article by *The Wall Street Journal*, at least 470 companies, government agencies, and other institutions acknowledged data breaches to their computer networks in 2012.[3] In 2013, 343 of those companies have disclosed a network breach, and the number is on pace to reach 588 by the end of this year.[4] Moreover, according to a cyber claims study by NetDiligence that analyzed claims data provided by insurance companies, the average cost per breach in 2012 was $3.7 million.[5]

Companies that are considering whether to purchase cyber insurance should carefully examine the policy wording to determine the scope of coverage. Whether a company is large or small, it is critical to evaluate the need for cyber insurance based on the type of business, the type of data at risk, and the liabilities and costs that may be incurred in the event of a security breach. The coverage provided by cyber insurance policies varies by insurance carrier. There is no "one-size-fits-all" cyber insurance policy. Businesses should also consider whether the cyber insurance policy provides coverage for breaches that occur on their own network or whether coverage is also provided for breaches occurring to third-parties that might affect their business, such as cloud providers or other vendors. Due to the intricacies of these policies, businesses should consult an insurance professional to ensure that they have the coverage they need.

Bryan Cave's Data Privacy and Security Team and Insurance Team have the expertise to help you assess your company's need for and negotiate cyber insurance. Our Insurance Team is also on the cutting edge of litigating cyber insurance claims. Please contact Bruce Oetter at 314-259-2336 about our experience handling claims for coverage. For more information about the topics in this article, please contact Dave Zetoony at 202-508-6030 or Maria Vathis at 312-602-5127.

For more information about trends in data privacy and security litigation or regulatory enforcement, or to receive Bryan Cave's data bulletins automatically, please contact Bryan Cave's Data Privacy and Security Team.

---

[1] *See* Georgina Gustin, "Schnucks Breach Will Likely Cost Millions," *St. Louis Post-Dispatch*, April 7, 2013.
[2] *Id.*
[3] James Willhite, "On Alert Against Cybercrime," *The Wall Street Journal*, Aug. 13, 2013.
[4] *Id.*, using data from the Identity Theft Resource Center.
[5] Mark Greisiger, "Cyber Liabilities & Data Breach Insurance Claims," NetDiligence, October 2012.