Traditional Insurance Products and Cyber-Liability Claims

Peter Selvin

(This article was published in the February 17, 2014 issue of Claims Journal).

The recent data breach incident involving Target Corporation highlights the exposure that companies, and their officers and directors, have in connection with such incidents. Among the risks present in such a scenario are these:

- Under the pertinent state and federal rules, a company whose data has been stolen or compromised will be liable for remediation-related expenses, such as costs associated with large charge backs, card reissuance, account monitoring and fines imposed by the credit card companies.

- The company will also face liability, often in the form of class-action lawsuits, from customers whose personal information has been compromised. *Anderson, et al. v. Hannaford Brothers Co*., 659 F.3d 151 (1st Cir. 2011). It will also face liability from the financial institutions who may be obligated to reissue their customers' cards and reimburse them for fraudulent transactions. *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litigation*, 834 F.Supp.2d 566 (S.D. Texas 2011).

- The company, and also its officers and directors, will face liability from its shareholders for failing either to prevent the data breach incident or accurately disclose its cybersecurity risks. Indeed, shareholders of Target recently filed two shareholder derivative lawsuits against the company and its officers and directors. In essence those shareholders claim that neither the company nor its officers or directors took reasonable steps to maintain its customers' personal and financial information or to implement adequate internal controls to detect and prevent such a data breach. See "Target Directors and Officers Hit with Derivative Suits Based on Data Breach".

To mitigate against these risks, the insurance industry has developed new cyber-security insurance policies which are designed to address a number of liability situations, including a large-scale data breach. While these policies play a key role, some traditional insurance policies may provide unexpected protection in such instances.

For example, in one recent case a company that was victimized by computer hackers successfully obtained reimbursement for remediation-related expenses following a data breach under its "Blanket Crime Policy", which contained an endorsement for "Computer & Funds Transfer Fraud Coverage". Although the insurer denied the company's tender, the company successfully sued the insurer for a determination of coverage in federal court. The Court held that under the company's policy the insurer was responsible for reimbursing the company for its losses in connection with the theft of customer information. *Retail Ventures, Inc. v. National Union Fire Ins. Co. of Pittsburgh, PA*, 691 F.3d 821 (6th Cir. 2012).

In data theft cases, a company's customers may bring civil claims against the company based on the violation of the customers' right of privacy. Importantly, the "personal injury" coverage afforded under a standard Comprehensive General Liability (CGL) policy is often triggered by "injury … arising out of … oral or written publication…of material that violates a person's right of privacy". Although there are few reported cases which have dealt definitively with this issue, some cases suggest that coverage for such customer lawsuits might be available in these circumstances.

Thus, in one recent case, the court found a violation of a customer's right of privacy, and hence personal and advertising injury coverage under a CGL policy, where a vendor had failed to redact customer credit card information from receipts. *Creative Hospitality Ventures, Inc. v. United States Liability Ins. Co.*, 655 F.Supp.2d 1316 (S.D. Fla. 2009), reversed in part, 444 Fed. Appx. 370 (11th Cir. 2011). In another case, the court found that tracking of web site visits by an internet service provider violated customers' right of privacy and hence constituted a personal injury offense, thereby triggering coverage under the policy. *Netscape Communications Corp. v. Federal Ins. Co.*, 343 Fed. Appx. 271 (9th Cir. 2009).

Another source of legal risk would be claims by a company's shareholders against the company's directors and officers for failing to accurately disclose its cybersecurity risks. In this regard, the SEC issued a written guidance on this subject in October, 2011. The emerging obligation on the part of company's directors and officers to include in its securities filings an assessment of a company's cybersecurity risk means that SEC enforcement actions and shareholder suits (such as those already filed against Target) based on alleged inadequate disclosure in this area will inevitably follow.

Where, as in the case of Target Corporation, shareholders bring claims against the company or its directors and officers, Directors and Officers Liability Insurance (so-called D & O insurance) will often come into play. Such a policy might provide coverage for suits against a company arising from a data breach where the policy provides "entity coverage". Where such "entity coverage" is broad, it may encompass liabilities for privacy breaches and cyber risks. Thus, "this type of insurance may be applicable in limited circumstances where an officer or director is sued directly in connection with a privacy breach - perhaps for lack of supervision or personal involvement in dissemination of confidential information". *Proskauer on Privacy*, § 17:2.3[A] at p. 17-15.

In the event that a company's officers or directors are sued in connection with data breaches, D & O insurance would also apply. As reflected in the recently filed suits against Target's officers and directors, the basic claim is that the company's officers and directors breached their fiduciary duties to the company by failing to take reasonable steps to maintain its customers' personal and financial information or to implement adequate internal controls to detect and prevent such a data breach. Subject to specific policy, especially the policy's exclusions, ordinary D & O insurance should provide in such an instance to the company's officers and directors.

While traditional insurance policies are not an adequate substitute for the newer policies that are specifically designed to provide protection against instances of data breach or cyber-fraud, attorneys and insurance professionals should be aware that are circumstances in which such traditional policies may provide unexpected benefits.