CLAIMS JOURNAL

View this article online: http://www.claimsjournal.com/magazines/special-report/2014/02/17/244533.htm

Traditional Insurance Products and Cyber Fraud Claims

By Peter S. Selvin | February 17, 2014

- Article
- Comments

The recent data breach incident involving Target Corp. highlights the exposure that companies, and their officers and directors, have in connection with such incidents. Among the risks present in such a scenario include 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 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. It will also face liability from the financial institutions who may be obligated to reissue their customers' cards and reimburse them for fraudulent transactions.
- 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 cyber security risks. Indeed, just a few days ago, shareholders of Target filed two shareholder derivative lawsuits against the company and its officers and directors. 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.

Unexpected Protection

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.

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 and 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.

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, there are a number of cases which 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. In another case, the court found that tracking of website visits by an Internet service provider violated customers' right of privacy and hence constituted a personal injury offense, thereby triggering coverage under the policy.

Where, as in the case of Target Corp., shareholders bring claims against the company or its directors and officers, directors and officers liability insurance (D&O) 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.

D&O Coverage

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 there are circumstances in which such traditional policies may provide unexpected benefits.

A word from our sponsor:

More from Claims Journal

Today's Insurance Headlines | Most Popular | Special Report