Published on *The National Law Review* https://natlawreview.com

Court Finds Crime Insurance Covers Data Losses

Article By:

Bruce H. Raymond

A data breach resulting in the theft and use of customer credit card numbers results in significant expenses and penalties for the victim company. Many companies still do not have specific cyber liability coverage and thus can be on the hook for all expenses related to such a breach. The Sixth Circuit Court of Appeals recently held that such losses resulting from the cyber theft of customer data were recoverable under a commercial crime policy. *Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co.*, 691 F.3d 821 (6th Cir. 2012).

In 2005, hackers used an apparently unlocked wireless network at a DSW Shoe Warehouse store to obtain unauthorized access to DSW's computer systems and downloaded credit card and bank account information from over 1.4 million DSW customers. Subsequently, fraudulent transactions using the stolen customer payment information occurred. DSW incurred millions of dollars of expenses for customer communications, public relations, customer claims and lawsuits, and attorney fees in connection with investigations by seven State Attorneys General and the Federal Trade Commission (FTC).

DSW submitted a claim for coverage under a computer fraud rider to a "blanket Crime Policy" for losses related to the computer hacking. The rider provided coverage for Computer and Funds Transfer Fraud Coverage; specifically, any loss resulting from the theft of any insured property by computer fraud.

In subsequent litigation to determine whether the losses were covered by the commercial crime policy, DSW prevailed on summary judgment with respect to its claim that the hacking damages were covered under the policy. Defendant appealed arguing that the trial court erred by finding that the expenses incurred were a loss resulting directly from the theft of insured property by computer fraud. Defendant urged the Court to use the "direct means approach" which would require DSW to show the computer fraud to be the sole and immediate cause of the loss. DSW argued the District Court correctly utilized a traditional proximate cause standard.

The Appeals Court held that the District Court was correct in applying a proximate cause standard and did not err in finding that the loss was caused by the hacking. The Court also rejected the Defendant's argument that the theft of customer data was covered by an exclusion under the policy. The policy stated that coverage does not apply to any loss of proprietary information, trade secrets, confidential processing methods or other confidential information of any kind. The Court held that the stolen customer information was not proprietary information because it belonged to the customer and not DSW. Furthermore, the stolen information did not constitute trade secrets or confidential processing methods. Finally, the language "other confidential information of any kind" was held to be general and should apply only to secret information *of DSW*. Otherwise, it would swallow the entire coverage for computer fraud. Since the confidential information was credit card and bank account numbers which belonged to the customers themselves, no exclusion under the policy applied.

DSW did not have a specific cyber insurance policy yet was still able to obtain coverage based on language in its commercial crime policy. Businesses should review their existing coverage carefully and may find that coverage for data breach is not expressly covered.

National Law Review, Volume III, Number 51