

Data Breach Insurance Coverage Lawsuit Highlights Necessity for Cyber Liability

By Andrew Martin

In August of 2012, the Sixth Circuit ruled on a case that determined who is responsible for the costs associated with loss of data arising from a hacking incident in *Retailer Ventures, Inc. v. Nat'l Union Fire Ins. Co.*, -- F.3d --, 2012 WL 3608432 (6th Cir. Aug. 23, 2012). In this matter, DSW Shoe Warehouse was targeted by computer hackers who successfully accessed their systems and harvested the credit card and checking account information for more than 1.4 million DSW customers. In its efforts to conduct thorough investigations into the incident and comply with the numerous state and federal data breach notification requirements, DSW incurred expenses of more than \$5M.

DSW sought to offset these costs (which, by the way, are not at all atypically large for a data breach of this size), by making a claim on its insurance policy under an endorsement called "Computer & Funds Transfer Fraud Coverage." While this endorsement may seem like a no-brainer policy to make a data breach claim under, the language of the policy provided coverage for loss "resulting directly" from theft as a result of computer fraud. Here, however, the insurance provider refused to cover the loss, claiming that any loss sustained did not "result directly" from the hacking event. On appeal, the Sixth Circuit affirmed the lower court's award in favor of DSW that the insurance provider had breached the contract with DSW when it refused to cover DSW's claim as the language of the policy was ambiguous, and thus should be construed in a light most favorable to the non-drafting party.

While DSW ultimately prevailed, this case highlights how important it is to have a cyber liability policy in place that is written to specifically cover the costs associated with a data breach event. When forced to rely on non-cyber liability endorsements, the insured may find itself having to engage in legal gymnastics to argue that it is entitled to coverage of associated breach costs. Even for events involving a fraction of the number of users, costs can quickly extend to the 6 figures and beyond. If your company routinely handles sensitive customer information, be sure you and your vendors have cyber liability policies in place to cover the costs related to these unfortunate events.



About the author Andrew Martin:

As an associate attorney with extensive prior experience advising information technology start-ups, Andrew's practice focuses on finding solutions for his clients' intellectual property issues. Due to his extensive experience in the software and technology industries, Andrew understands both the practical and legal issues involved in IP licensing agreements and disputes. In addition to licensing, Andrew helps his clients find new ways to use existing technologies to assist his clients in areas such as data privacy compliance. Andrew uses his diverse background which includes founding a record label and working for a world-wide concert promoter when counseling the firm's entertainment clients.

Get in touch: amartin@scottandscottllp.com | 800.596.6176