CARLTON FIELDS

Courts May Still Be Expanding Coverage for Liability of Computer Hacking Victims

August 30, 2012

August 30, 2012 -- Large retailers and other traditional businesses face significant risks for failure to secure their customers' credit card information. The risks include tort and statutory liability to the customers themselves, as well as contractual liability to credit card networks and acquiring banks, which may require merchants to pay the cost of unauthorized purchases. Because computer crimes are still relatively new, businesses often seek coverage for these losses under traditional policies that were not intended to cover computer hacking or third-party liability. Recent decisions by the U.S. Court of Appeals for the Sixth Circuit suggest ways in which the scope of traditional coverage may be expanding. These cases underscore the necessity of clearly delineating the limits of third-party coverage in policies for conventional businesses that routinely handle sensitive customer information. **Blanket Crime Policy Covers Liability for Hacking** ***Retail Ventures v. National Union Fire Insurance Company of Pittsburgh*** arose out of the theft of customer information from a chain of shoe stores, DSW. Hackers used the local wireless network at one DSW outlet to access the computer system for the entire chain and to download credit card and checking account information of more than 1.4 million consumers. In addition to incurring expenses for customer communications and public relations, DSW had to defend and settle customer lawsuits and respond to investigations by seven state Attorneys General and the Federal Trade Commission. Additionally, DSW suffered more than $4 million in costs associated with charge backs, card reissuance, account monitoring and "fines" for which it was liable under network agreements with VISA and MasterCard. DSW's **blanket crime policy** contained a **computer fraud endorsement**, which covered "**[l]oss which the Insured shall sustain resulting directly from . . . [t]heft of any Insured property by Computer Fraud**." The insurer, National Union, conceded that the hacking incident constituted theft of insured property by computer fraud. At issue was whether DSW's losses had "**result[ed]** ***directly***" from that incident. The Sixth Circuit, applying Ohio law, found that this was a matter of first impression. Although the policy did not expressly limit coverage to losses caused by employees, National Union asserted that it was a **fidelity bond**, because it was modeled on a Standard Form of the Surety Association of America, because the coverage applied "only with respect to . . . [p]roperty located on [DSW's] premises," and

because certain exclusions indicated the insurer's intent to provide first-party coverage only. The insurer cited cases from a number of states other than Ohio that have applied a **"direct-means-direct" approach** to determining which losses are covered by fidelity bonds—an approach that excludes coverage for the insured's liability to third parties. The Sixth Circuit's analysis began by observing that "**the label given to a policy is not determinative of coverage**." While acknowledging that DSW had not purchased a liability policy, the Court found that neither the language of the policy nor the exclusions cited by National Union unambiguously limited coverage to first-party losses. The Court also noted that Ohio courts had applied a "**proximate cause**" standard to identifying "direct" losses under other types of first-party coverage, and it found that the hacking of DSW's computers had proximately caused all the losses at issue. Consequently, the Court held that the Ohio Supreme Court would find that DSW's losses had "result[ed] directly" from the hacking scheme and were covered by the computer fraud endorsement. **Fidelity Bond Covers Liability for Consequential Damages** *Retail Ventures* was decidedjust three weeks after the Sixth Circuit had arguably expanded coverage under fidelity bonds in another way. ***First Defiance Financial Corp. v. Progressive Casualty Insurance*** did not involve computer hacking; the insured was an investment company, and one of its employees had transferred funds from clients' discretionary brokerage accounts into his own bank account. The company's fidelity bond covered "[l]oss **resulting directly** from dishonest or fraudulent acts committed by an [e]mployee," including "loss of **property . . . owned and held by someone [other than the insured] under circumstances which make the [i]nsured responsible** for the [p]roperty . . . ." The policy **excluded** coverage for "**potential income, including, but not limited to interest and dividends, not realized by the [i]nsured**." Applying Ohio law, the Sixth Circuit found that the insured had been "responsible" for the stolen funds in a way that made them covered property under the policy. It then explained: "If property qualifies as 'covered property,' and a dishonest employee steals it, the employee '**directly**' causes the loss. It is as simple as that, and that is true under **any** definition of 'directly.'" Perhaps more significantly, the Court went on to find that Progressive was responsible for covering the insured's liability to its customers for their **lost interest and unrealized income**. The Court held that the interest exclusion in the policy "**speaks to lost interest not realized by the insured, not to interest payments owed to customers**." The Court held, in other words, not only that a traditional fidelity bond covered losses suffered by third parties, but that the scope of that coverage could be **broader** than the policy's first-party coverage. Since fidelity bonds may now respond to claims based on computer hacking, this ruling has taken on added importance. **Traditional Exclusions are Not Enough** Cases now pending in New York and California are testing whether a commercial general liability policy covers liability for a 2011 hacking incident that exposed information about 100 million customers of Sony's online entertainment and gaming networks. Those cases are not construing any policy language that specifically addresses the risks inherent in gaining access to massive quantities of customer data; they will be decided, rather, on the basis of whether the claims of Sony's customers fall within a conventional definition of "advertising injury." They therefore illustrate the importance of crafting policy terms that deal directly with issues of protecting customer information. What the recent decisions of the Sixth Circuit show is that this problem is not limited to Internet businesses or liability

policies. Conventional retailers are now susceptible to massive data breaches, and they are successfully seeking coverage under policies that have traditionally been limited to first-party claims.

Authored By

John C. Pitblado