BARNES & THORNBURG LLP

Cybercrime: How Insurance Can Protect Your Company

March 17, 2015 | | Cyber Insurance, Policyholder Protection

Scott N. Godes
Partner
Data Security and Privacy Co-Chair, Insurance Recovery and Counseling Group Co-Chair

Just when you thought that it could not get worse for companies in the context of cybersecurity and privacy issues … it does. Perhaps most significant, a court recently allowed banks to proceed against a retailer to pursue damages allegedly flowing from a cyberattack and data privacy incident involving payment card numbers. That same retailer disclosed hundreds of millions of dollars in losses as a result of the cyberattack and data privacy incident. Another retailer fell victim to a cyberattack and data privacy incident involving payment card numbers. Major entertainment businesses suffered cyberattacks, with one reportedly involving information about celebrities, corporate IP, and user names and passwords for social media accounts of the company. Distributed denial of service attacks (DDoS) are also on the rise. Below, we review the sobering news about cyberattacks and some tips when considering insurance for cyber risk in 2015. **How Bad Is It?** First, the decision involving banks and retailers is significant. *In In re Target Corp. Customer Data Breach Security Litigation*, the court refused to dismiss a complaint in the "Financial Institution Cases." *In re Target Corp. Customer Data Breach Security Litigation*, MDL No. 14-2522, slip op. [Dkt. 261] (D. Minn. Dec. 2, 2014). The refusal to dismiss a putative class action complaint against a corporate defendant in connection with a data privacy incident is not the eye-opening part. Rather, it's the identity of the plaintiffs. "Plaintiffs here are a putative class of issuer banks whose customers' data was stolen in the Target data breach." *Id.* at 2. Those banks have sued Target Corporation, alleging that Target was negligent in failing to secure payment card numbers, that Target violated Minnesota's Plastic Security Card Act, that there was negligence per se (because of the alleged statutory violation), and that the failure to tell the banks of Target's allegedly insufficient security practices was a negligent misrepresentation by omission. *Id.* There is little case law on this point, as the law is nascent and continues to be developed. Even less case law exists on the exact question of whether banks can pursue retailers for alleged losses resulting from a cyberattack and data privacy incident involving payment card numbers. Unfortunately for Target, however, the court ruled that the banks could proceed with their action. There can be little doubt that Target's defense costs will continue to mount. Second, the losses that Target has suffered already are noteworthy. Target disclosed in its Form 10-Q for the quarterly period ended Nov. 1, 2014, that it already had

RELATED PRACTICE AREAS

Insurance Recovery and Counseling

RELATED TOPICS

Cyberattack
cybersecurity
Data Privacy
Privacy
Target

“incurred $248 million of cumulative expenses” as a result of the cyberattack and data privacy incident. Target, Form 10-Q, at 9 (Nov. 26, 2014), available here. Third, Target is just one example in a continuing stream of news regarding retailers that have had payment card information stolen. In early December, 2014, Brian Krebs reported that international retailer Bebe Stores Inc. was another victim of a criminal cyberattack. Krebs wrote that Bebe had confirmed “[t]hat hackers had stolen customer card data from stores across the country in a breach that persisted for several weeks last month.” Brian Krebs, “Bebe Stores Confirms Credit Card Breach,” *Krebs on Security* (Dec. 5, 2014), available here. Click here to read more.