The consumer may not be your worst enemy in the case of a data breach

SUMNER & GASKINS PUBLISH DATA BREACH LITIGATION ARTICLE
InsideCounsel
11.2014

Charleston Litigation Member Robert Sumner and Litigation Associate Brandon Gaskins were published by *InsideCounsel* on November 3. Their article, "The consumer may not be your worst enemy in the case of a data breach," points out that businesses must think beyond the consumer data breach lawsuits that are so prominent across headlines, and consider potential claims from business partners and shareholders. It can be seen below in its entirety.

The consumer may not be your worst enemy in the case of a data breach

Businesses must think beyond the consumer data breach lawsuits that dominate the headlines and consider potential claims from business partners and shareholders

Hardly a month passes without headlines of a prominent business, from retail giants like Target and Home Depot to sophisticated financial institutions like JPMorgan Chase, experiencing a data breach involving the unauthorized disclosure of consumers' personal and financial information. Those headlines are routinely followed by reports of class-action lawsuits being filed on behalf of consumers within weeks and sometimes days of the public release of the breach.

It should be no surprise then that data breach lawsuits are on the rise across the nation. What may be surprising is that businesses may face their most significant data breach liability threat not from consumers but from their business partners and shareholders. With increasing frequency, banks, payment card issuers and shareholders are suing companies that suffer a data breach for business and investor losses resulting from the disclosure of consumer information.

While consumers have had only limited success in data breach lawsuits because of the difficulty in establishing actual rather than speculative monetary injury, non-consumer plaintiffs do not face this challenge because they can more easily identify compensable losses in the form of lost business expenses resulting from the breach. Accordingly, businesses should be equally, if not more, concerned about data breach lawsuits brought by parties other than their customers.

The recent Target data breach, which involved the theft of 40 million payment card numbers, provides a good example of the multi-front litigation that businesses can expect from a data breach. In addition to facing the class-action claims filed by consumers, Target is being sued by 29 payment card issuers who allege that

THE CONSUMER MAY NOT BE YOUR WORST ENEMY IN THE CASE OF A DATA BREACH

Target's negligence in securing its computer network cost them millions dollars in reissuing payment cards and reimbursing the victims of fraud. In September 2014, Target moved to dismiss the banks' claims, arguing that it had no common-law tort duty to the banks and card issuers. The court has yet to rule on Target's motion, but its resolution of these claims could have a significant impact on how similar claims are asserted and resolved in the future.

Board directors of Target, Wyndham Worldwide Corp. and other companies have also been sued in shareholder derivative suits arising from data breaches. Generally, these lawsuits allege that directors breached their fiduciary duties to the companies and shareholders by failing to take reasonable steps to maintain customers' personal and financial information in a secure manner. The shareholder plaintiffs seek damages associated with the loss of share value and waste of company assets arising from legal costs, liability, and government investigations. If these lawsuits are successful, the damages will be significant. For example, Target recently announced in a SEC filing that it expects its data breach expenses to reach $148 million.

Companies suffering a data breach involving the theft of payment card information can also expect fines from payment card companies, such as Visa, Mastercard and American Express. Under their contracts with payment card issuers and processors, such as banks and credit unions, payment card companies require merchants who accept their payment cards to comply with the Payment Card Industry Data Security Standard (PCI-DSS), which establishes information security standards for payment processes, systems, networks, software and applications. Merchants who fail to comply with PCI-DSS are subject to fines and reimbursement assessments from the payment card companies. Although the fines vary depending on the volume of payments processed by the merchant and the number of violations, companies that experience a data breach can be fined and assessed millions of dollars.

Some retailers are challenging these fines and assessments in court. For example, in*Genesco, Inc. v. Visa U.S. A., Inc.*, which is currently pending in federal court in the Middle District of Tennessee, apparel retailer Genesco, Inc. is suing Visa after being fined and assessed for violations of PCI-DSS. In that case, hackers installed software on Genesco's computer network to obtain cardholders' unencrypted account data that was transmitted to Wells Fargo and Fifth Third banks. After the breach, Genesco retained an information security firm to investigate the breach. The investigation report, which was provided to Visa, found three violations of the PCI-DSS requirements. As a result, Visa assessed Wells Fargo and Fifth Third over $13 million in fines and reimbursement costs for Genesco's PCI-DSS violations under its contracts with the banks. Genesco indemnified the banks, and the banks assigned their claims against Visa for the fines and assessments to Genesco.

Genesco subsequently sued Visa as the banks' assignee and subrogee for recovery of the fines and assessments, asserting claims of breach of contract and implied covenants of good faith and fair dealing, unjust enrichment, restitution, and violation of California's Unfair Competition Act. Genesco alleges that Visa lacked a factual basis for its fines and assessments and imposed them in violation of Visa's agreements with the banks. Genesco's claims are still pending, and the court refused to dismiss its claim for violation of the Unfair Competition Act. According to the court, "[I]f Visa's contracts impose assessments based upon possible risk of injuries in the event of a breach of a cardholder's data, without an actual theft of such data, then that assessment may be an unenforceable penalty."

THE CONSUMER MAY NOT BE YOUR WORST ENEMY IN THE CASE OF A DATA BREACH

These recent developments demonstrate that when assessing cybersecurity risks businesses must think beyond the consumer data breach lawsuits that dominate the headlines and consider potential claims from business partners and shareholders. Companies must ensure that their information systems and networks are secure and comply with prevailing security standards and contractual requirements. Companies should also obtain cybersecurity and D&O liability insurance that covers data breaches and include data breach protections into contracts with vendors, suppliers and other business partners. Finally, businesses should continually monitor the rapidly developing law relating to data breaches to ensure they have adequately prepared to preserve all litigation options and defenses in the event they face lawsuits filed by their business partners and shareholder as a result of a data breach.