

The Growing Wave of Data Breach Litigation

by Robert T. Horst, John F. Mullen, Sr. and Mark H. Rosenberg

Data breaches—the theft, loss or unintended exposure of personally identifiable information—have compromised hundreds of millions of personal records in recent years. In 2009, the trend continued with two of the largest breaches in history. In January, as many as 100 million credit card records were exposed when it was discovered that hackers broke into the network of credit card processor Heartland Payment Systems. And in October, the personal information of more than 70 million U.S. military veterans was compromised when an improperly erased hard drive was sent out for repair.

These breaches, and others like them, only scratch the surface of the problem. A study by Gartner Inc. found that financial fraud affected 7.5% of all Americans in 2008, and data breaches spawned 19% of that fraud. The Identity Theft Resource Center (ITRC) reported that data breaches in 2008 increased by 47% over the previous year. And by November, the ITRC had reported more than 400 breaches affecting 220 million records in 2009—an amount of records nearly equal to the previous four years combined.

Given the scope of the problem, it should be no surprise that data breaches have led to expensive litigation, including attempted class actions. So far, however, these actions have met with little legal success (as distinguished by sizable costs and settlements). But considering the scope of the risk, it would be wise for companies to be familiar with the important decisions in this area.

Proof of Harm

One of the first major decisions pertaining to a data breach class action was issued by the United States Court of Appeals for the Ninth Circuit in *Stollenwerk v. Tri-West Healthcare Alliance*. The case concerned the theft of computer servers containing the personal information of customers. Of the three named plaintiffs, only one person claimed to have suffered identity theft related to the burglary. Relying upon case law recognizing claims for medical monitoring by plaintiffs who have been exposed to hazardous substances but had not yet sustained injury, the remaining two defendants sought compensation for the premium credit monitoring service they had purchased following the identity theft.

The trial court sided with the defendants. But, on appeal, the Ninth Circuit reversed the trial court ruling regarding the one plaintiff who claimed to have suffered identity theft. The court held that it was possible that a causal relationship existed between the burglary and identity theft. The court did not reverse the ruling for the two other plaintiffs, however, because it did not see any evidence that the plaintiffs were harmed by the exposure of their information.

Following the Ninth Circuit's decision, the trial court denied the plaintiffs' motion for class certification, primarily on the grounds that a determination of whether the data breach resulted in instances of identity theft required an analysis of factual issues unique to each putative class member. Although viewed as a victory for the defense, *Stollenwerk* cracked open the door for future plaintiffs to gather and assert more information about identity thefts in an effort to build a stronger case.

A similar attempt at a cyber-breach class certification was addressed by the United States Court of Appeals for the Seventh Circuit in *Pisciotta v. Old Nat. Bancorp*. The case concerned allegations that due to a bank's failure to take appropriate steps to secure personal information of customers obtained through its website, a third party hacker was able to obtain access to the website and acquire the personal information of thousands of individuals, including names, addresses, social security numbers, driver's license numbers and credit card account numbers. On behalf of a putative class, the plaintiffs brought negligence claims against the bank and the company who hosted the website, a claim for breach of

implied contract against the bank, and a claim for breach of contract against the company.

The Pisciotta plaintiffs did not contend that any of the putative class members or even any of the named plaintiffs had sustained actual and immediate losses due to the alleged breach (although they might have, had they learned of Stollenwerk). Rather, the plaintiffs based their complaint upon the claim that the alleged breach resulted in "substantial potential economic damages and emotional distress and worry that third parties will use [the plaintiffs'] confidential personal information to cause them economic harm, or sell their confidential information to others who will in turn cause them economic harm." As in Stollenwerk, the plaintiffs primarily sought relief in the form of an economic monitoring procedure that would promptly inform class members of any attempt to utilize the confidential information at issue.

The United States Court of Appeals for the Seventh Circuit reviewed the plaintiffs' claims and noted that under the applicable law of the state of Indiana, claims for negligence and breach of contract both require plaintiffs to establish a compensable injury. In analyzing whether Indiana courts would hold that a data breach alone constitutes a compensable injury, the court focused on a recently enacted Indiana statute regarding computer database breaches. The court emphasized that this statute "require[s] only that a database owner disclose a security breach to potentially affected consumers; [it does] not require the database owner to take any other affirmative act in the wake of a breach."

The court further noted that the statute "creates no private right of action against the database owner by an affected customer," and "imposes no duty to compensate affected individuals for inconvenience or potential harm to credit that may follow." The court concluded that the "narrowness of the defined duties imposed, combined with state-enforced penalties as the exclusive remedy, strongly suggest that Indiana law would not recognize the costs of credit monitoring that the plaintiffs seek to recover in this case as compensable damages."

In addition, the court noted that the Indiana Supreme Court has held that since no cause of action for asbestos exposure accrues until a plaintiff could reasonably have been diagnosed with an exposure-related illness, the courts would be similarly reluctant to recognize a cause of action for "credit monitoring" before an actual injury has occurred. Finally, the court noted that causes of action for credit monitoring had been rejected by other courts, including the Stollenwerk court.

The court concluded that "without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy." Accordingly, the court affirmed the trial court judgments in favor of the defendants.

Hannaford Fallout

More recently, a data breach at grocery retailer Hannaford Bros. from December 2007 to March 2008 led to the exposure of up to 4.2 million debit and credit card account numbers and other personally identifiable information. At least 2,000 cases of fraud have been linked to the incident.

Unlike previous data breaches involving unauthorized access to databases, the account numbers in the Hannaford Bros. case were obtained through malware installed on store servers, which allowed hackers to intercept data stored on the magnetic strips of the cards being swiped by customers at checkout. In so doing, the breaching parties exploited the fact that account information is typically not encrypted while it is transferred from point-of-sale devices to store servers.

Understandably, the incident at Hannaford Bros. led to class action litigation. In re Hannaford Bros. Co. Customer Data Security Breach Litigation involved six putative class actions consolidated into a single action in Maine asserting, among other charges, that Hannaford Bros. breached an implied contract to protect customer data. The plaintiffs sought compensatory damages and injunctive relief.

The court found that no such contract existed and eventually dismissed all of the complaints. The court determined that the plaintiffs who did not have fraudulent items posted to their accounts could not recover for emotional distress or under any other theory. In addition, plaintiffs who had fraudulent charges that were removed by their card issuers did not have a claim for damages, as the consequential

damages that these plaintiffs allegedly suffered as a result of the theft (including overdraft fees, the time expended on rectifying charges and the loss of accumulated reward points) were remote, speculative and/or not reasonably foreseeable.

The court also rejected the plaintiffs' demand for an injunction ordering Hannaford to disclose the information that was exposed to breach and provide credit monitoring services. As all of the named plaintiffs cancelled the affected accounts, the court held that they had no standing to pursue such an injunction.

The case may not end there, however, as the judge has asked the state Supreme Court to review Maine's data breach law to determine if a consumer's lost time and effort spent in dealing with a data breach constitutes a recoverable injury—a decision that could drastically affect retailer's liability in a data breach.

An Expensive Exposure

Until the Maine court reaches a decision, however, existing data breach verdicts should provide some reassurance to corporations and their insurers concerned about potential liability arising out of incidents of data breach. But these decisions do not eliminate all liability for breaches.

Tremendous media coverage was devoted to the 2005 theft of more than 45 million individual records from the computer system of TJX Corporation, a retailer operating major chains such as TJ Maxx and Marshalls. This scheme ultimately led to criminal charges against 11 people from around the world, who were accused of engaging in a complex plan to hack into computer systems of at least nine major retail chains. The financial loss from this incident has been estimated to range in the hundreds of millions of dollars.

In *In re TJX Companies Retail Sec. Breach Litigation*, the United States Court of Appeals for the First Circuit allowed a bank seeking to represent a putative class to pursue a claim under the Massachusetts unfair trade practices statute against TJX (as well as the bank that processed the credit and debit card transactions on TJX's behalf) for damages sustained due to the data breach incident. This included damages arising from the reimbursement of fraudulent charges resulting from the data breach. These rulings paved the way for a \$40.9 million settlement by TJX with many of the affected banks.

In re TJX Companies suggests that the risk of liability exposure arising from losses to customers affected by a data breach may be equaled or overshadowed by the risk of exposure arising from banks that compensated customers or reissued credit and bank cards as a result of these losses. As a large-scale data breach incident may easily result in thousands of fraudulent charges to customers of a single bank, an action by a single bank seeking compensation for such charges may result in losses that rival or exceed any potential verdict in a consumer class action.

Accordingly, whether at risk from bank, consumer or employee classes, companies must remain vigilant in their efforts to recognize and plan for the risk of exposure arising from large-scale data breaches. Regardless of case law, data security is a critical enterprise risk issue and a growing threat to balance sheets, risk profiles and company reputations.

Robert T. Horst is a partner with Nelson Levine de Luca & Horst, LLC and represents insurers in complex coverage disputes, bad faith litigation, class action defense and the investigation of suspected fraud. **John F. Mullen, Sr.** is a partner with Nelson Levine de Luca & Horst, LLC and the chair of the firm's complex litigation practice group. **Mark H. Rosenberg** is an associate with Nelson Levine de Luca & Horst, LLC, specializing in the defense of complicated insurance practice and bad faith disputes and frequently advises insurance clients regarding business practices and regulatory developments.