Watch Out! Privacy Litigation Damages Becoming More Viable

Feb 01 2009

Posted By: Mark F. Foley

Practice Area: Information Technology, Data Privacy and Security

Until now, lawsuits seeking to recover significant damages based on the loss of, or unauthorized access to, sensitive personal information have not been especially successful for plaintiffs. Most companies suffering data breaches have escaped by offering affected consumers inexpensive credit monitoring services.

But two recent cases show plaintiffs a way to expose many previously safe companies to substantial claims for damages. Any company that thinks there are no risks in employing less than best practices for data privacy and security needs a wake up call.

The headlines are all too familiar. Some well known consumer services company (or less known wholesale data processor) announces that millions of individual records containing names, Social Security numbers, account numbers and other sensitive information were left in a dumpster, saved to a stolen, unencrypted laptop, or stored on a misplaced USB drive or backup tape. The press is terrible, the company's stock takes a temporary plunge, and sometimes the Federal Trade Commission enters into a consent decree where the company promises to never do it again.

But when affected individuals or groups of consumers tried to sue for damages, they seldom recover significant amounts. These cases have not often succeeded because the plaintiffs have been unable to prove actual pecuniary losses resulting from the security breach. Sure, if identify theft occurs the affected individuals can suffer significant emotional trauma, loss of time, etc. But Courts have been unwilling to award damages for anxiety, fear, and other emotional harm that can result from a data breach, for the risk of future identify theft, or for actual identity theft when the plaintiff could not prove that the theft occurred as a direct result of a data breach at a particular source. Most companies facing claims based on data breaches have been able to settle cheaply by offering to provide credit monitoring services, which most consumers do not use, resulting in only minimal expenses for the company whose data were lost or stolen.

On The Case

Two recent cases may make such circumstances much more dangerous. In *Pinero v. Jackson Hewitt Tax Service, Inc.,* No. 08- 3535 (E.D. La. Jan. 7, 2009), a U.S. federal court refused to dismiss a claim for damages by a consumer whose tax returns were found by a third party in an unsecured dumpster outside a tax preparer's office. No actual identity theft had occurred and the plaintiff had suffered no provable pecuniary loss; so the Court dismissed the usual panoply of breach of contract, emotional distress, negligence, and invasion of privacy claims that often flow from such facts.

But the Court left standing Pinero's allegations that using false promises of data protection to lure customers to enter into a consumer services contract was an unfair trade practice under the Louisiana "Little Federal Trade Commission" law. The court also recognized that a claim based on a common law "fraudulent inducement" theory could stand, if properly pled. This case is significant not just because it establishes a basis for an individual consumer to assert a real damages claim, but because it also opens the door to class action lawsuits based on such theories. Since some state unfair and deceptive practices laws provide for statutory treble damages, the doors are now open to substantial recoveries.

The second case, *In Department of Veterans Affairs Data Theft Litigation,* No. 06-0506, (D. D.C. Jan. 27, 2009), involves the settlement of multiple consolidated class action lawsuits against the U.S. Department of Veterans Affairs. In 2006, an analyst for the agency took home a laptop with Social Security numbers and other sensitive data concerning 26 million veterans and 2.2 million active duty military personnel. The laptop was stolen from the analyst's home during a burglary. The laptop was recovered a short time later, and forensic analysts from the FBI determined that it probably had not been accessed. There have been no press reports with information tying any identity theft incidents to the breach. Nevertheless, lawyers brought a class action suit seeking damages for those who incurred out of pocket expenses.

The suit settled in late January with an agreement that the Veterans Administration would create a $20 million fund to pay the expenses of anyone directly affected by the breach, including credit-monitoring expenses and mental health costs for those who found themselves in extreme emotional distress as a result of the breach. Payments will range upward to $1,500; every person who files a valid claim will receive at least $75. The fund will also be used to pay $5.5 million in attorneys fees and expenses. Any funds not used for these purposes will be paid to veterans' charities.

This case is noteworthy because of the size of the settlement and the VA's willingness to pay a large amount even though there would likely never be any actual damages resulting from the breach or any evidence to support a causal connection between any actual damages and the breach. The case is also noteworthy because of the fact that the total amount of the settlement is not just available for payments, but is actually committed. That is, many sources of data breach in the past have escaped significant expenses by offering credit monitoring services that were never accepted or paid for. Here, in contrast, VA will pay the full $20 million to someone.

What's The Damage?

What both cases show is that class action plaintiffs are devising new ways to successfully assert larger damage claims against companies that suffer data privacy and security breaches. Companies should renew their efforts to deploy and implementing effective data privacy and security protections.
