

Legal Updates & News

Bulletins

Seventh Circuit Dismisses Security Breach Class Action

October 2007

Privacy Law Bulletin, October 9, 2007

Following a data security breach, businesses can frequently look forward to a consumer class action or two. To date, these class actions have been largely unsuccessful, and several federal district courts have dismissed consumer actions following a breach for failing to state a claim upon which relief can be granted. See, e.g., *Kahle v. Litton Loan Servicing, LP*, 486 F. Supp. 2d 705 (S.D. Ohio 2007); *Bell v. Acxiom Corp.*, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006); *Key v. DSW, Inc.*, 454 F. Supp. 2d 684 (S.D. Ohio 2006); *Guin v. Brazos Higher Educ. Serv. Corp., Inc.*, 2006 WL 288483 (D. Minn. Feb. 7, 2006).

Now, for the first time, a federal court of appeals has weighed in on the issue as well. On August 23, 2007, the U.S. Court of Appeals for the Seventh Circuit ("Seventh Circuit") concluded that present and future identity theft-monitoring costs are not compensable damages under Indiana's security breach notification statute, affirming the dismissal of a class action claim against a bank for allegedly failing to protect personal information collected on its online marketing Web site from a hacking incident (*Pisciotta v. Old Nat'l Bancorp.*, No. 06-3817, 2007 WL 2389770 (7th Cir. Aug. 23, 2007)).

The defendant operates a marketing Web site on which individuals seeking financial services can complete online applications for opening accounts and other financial services. Applications differ depending on the financial service requested, but some forms require a customer's name, address, Social Security number, driver's license number, date of birth, mother's maiden name, and certain financial account information. The plaintiffs accessed the defendant's Web site and entered personal information in connection with their applications for financial services.

A hosting facility that maintains the defendant's Web site notified the defendant of a security breach. The defendant subsequently sent written notice to its affected individuals. The plaintiffs brought suit on behalf of a putative class of users of the defendant's Web site alleging that the defendant failed to adequately protect their personal confidential information, which caused the plaintiffs and other past and present customers to suffer potential economic damages and caused concern that third parties would use the confidential personal information of the plaintiffs to cause them economic harm, or sell their confidential information to others who would in turn cause economic harm.

According to the plaintiffs, they incurred expenses in order to prevent their confidential personal information from being used and will continue to incur such expenses in the future. However, the plaintiffs did not allege any direct financial loss to their accounts as a result of the security breach, nor did they claim that they already had been the victim of identity theft as a result of the security breach. The plaintiffs requested compensation for all "economic and emotional damages suffered" as a result of the acts of the defendants which the plaintiffs claimed were negligent or in breach of contract, and any and "all other legal and/or equitable relief to which [p]laintiffs . . . are entitled, including establishing an economic monitoring procedure to insure [sic] prompt notice to [p]laintiffs . . . of any attempt to use their confidential personal information stolen from" the defendant.

The defendant filed a motion for judgment on the pleadings. The district court granted the motion, concluding that the plaintiffs' claims failed as matter of law because "they have not alleged that [the defendant's] conduct caused them cognizable injury." To support its conclusion, the district court noted that under Indiana law, damages must be more than speculative; therefore, the allegations of the plaintiffs that they suffered "substantial *potential* economic damages" did not state a claim.

On appeal, the Seventh Circuit was asked to determine whether Indiana law would consider “that the harm caused by the identity information exposure, coupled with the attendant costs to guard against identity theft, constitutes an existing *compensable injury and consequent damages* required to state a claim for negligence.”

The Seventh Circuit reviewed the Indiana breach notification statute, which creates certain duties when a database in which personal data, electronically stored by private entities or state agencies, potentially has been accessed by unauthorized third parties. The Indiana breach notification statute requires only that a database owner disclose a security breach to potentially affected consumers; the statute does not require the database owner to take any other affirmative action after a breach of security. Further, if the database owner fails to comply with the affirmative duty imposed by the Indiana breach notification statute, the statute provides for enforcement only by the Indiana Attorney General.

According to the Seventh Circuit, the Indiana breach notification statute does not create a private right of action against the database owner by an affected customer and does not impose a duty to compensate affected individuals for inconvenience or potential harm that may follow. The Seventh Circuit explained that, had the Indiana legislature intended that a cause of action be available against a database owner for failing to protect adequately personal information, the legislators would have made a more definite statement of that intent.

The Seventh Circuit concluded that the defined duties imposed by the Indiana breach notification statute, combined with state-enforced penalties as the exclusive remedy, suggest that Indiana law would not recognize the costs of credit file monitoring that the plaintiffs seek to recover as compensable damages. In addition, after consulting Indiana state court decisions, the Seventh Circuit found that the Indiana Supreme Court has suggested that compensable damage requires more than an exposure to a future potential harm. The Seventh Circuit also consulted other court decisions applying the law of other jurisdiction to the question posed in this case, and found that, although some cases involve different types of information loss, they rely on the same basic premise: “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.”