Federal Court of Appeals Dismisses Data Breach Class Action Following Hack of Bank's Marketing Web Site

ALAN CHARLES RAUL AND EDWARD McNICHOLAS

The authors discuss a decision by a federal court of appeals dismissing a purported class action against a bank that alleged failure to protect personal information on the bank's marketing Web site after a "sophisticated, intentional, and malicious" intrusion.

In a victory for a bank facing potential identity theft liability, a federal court of appeals has dismissed a purported class action that alleged failure to protect personal information on the bank's marketing Web site after a "sophisticated, intentional, and malicious" intrusion. The putative class action plaintiffs had claimed that they were injured by the negligent failure of Old National Bancorp (ONB) to protect their personal data. The plaintiffs further alleged breach of implied contract claims against ONB and breach of contract by NCR, the hosting facility that maintains ONB's marketing Web site.

The decision, *Pisciotta v. Old Nat'l Bancorp*[1] provides insight into how appellate courts will decide other "data breach" cases where there is no evidence of actual identity theft and the claimed harm is limited to the

Alan Charles Raul and Ed McNicholas are partners in the Washington, D.C., office of Sidley Austin LLP. The authors can be reached at araul@sidley.com and emcnicholas@sidley.com, respectively.

Published in the October 2007 Privacy & Data Security Law Journal.

costs associated with preventing malicious use of personal information. Perhaps significantly, the court disagreed with several district courts and considered the fear of future identity theft to be consequential enough to establish an injury-in-fact for Article III standing. Nevertheless, although primarily grounding its ruling in Indiana law, the court also emphasized that its holding is consonant with the consistent refusal of other federal courts to recognize credit monitoring costs as a compensable injury.

Significantly, the court of appeals analyzed the state data breach notification statute and concluded that if the state legislature had meant to create a private cause of action for data breaches per se, it would have done so in the very specific legislation dealing with such breaches. Because the legislature had not created a private right of action, and there was no analogous precedent in state case law, the federal court declined to create a data breach cause of action on its own initiative. Moreover, the court of appeals reviewed the existing data breach case law and found that all of the cases "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." Thus, the plaintiffs' data breach claims were dismissed as a matter of law.

FACTS OF *PISCIOTTA*

ONB is a bank that operates a marketing Web site on which potential customers can complete online applications for accounts, loans, and other ONB banking services. Some of these applications require the customer's or potential customer's name, address, social security number, driver's license number, date of birth, mother's maiden name, and credit card/financial account information. This information was stored on ONB's Web site and was maintained by NCR, a hosting facility. NCR, in 2005, informed ONB that a "sophisticated, intentional, and malicious" security breach of the ONB Web site had occurred. ONB then sent written notice of the breach to its customers.

Luciano Pisciotta and Daniel Mills, in 2002 and 2004 respectively, had accessed the ONB marketing site and entered personal information in connection with their applications for ONB banking services. On behalf

of themselves and similarly situated individuals, they brought a diversity suit in the United States District Court for the Southern District of Indiana. Plaintiffs claimed that ONB and NCR were negligent in the maintenance of personal information on the ONB marketing Web site, which caused them to suffer "substantial potential economic damages and emotional distress and worry" about an enhanced possibility of identity theft. On the question of damages, the court focused on the fact that plaintiffs alleged no "completed direct financial loss to their accounts as a result of the breach. Nor did they claim that they or any other member of the putative class already had been the victim of identity theft as a result of the breach." Rather, plaintiffs alleged that they "have incurred expenses in order to prevent their confidential personal information from being used and will continue to incur expenses in the future."

The district court had previously concluded that plaintiffs' claims failed as a matter of law "because they have not alleged that ONB's conduct caused them cognizable injury." Most significantly, the district court concluded that the credit monitoring and other costs incurred by the plaintiffs to prevent "a future injury" are not "damages." Without a concrete, cognizable damages claim, the district court was compelled to dismiss the negligence claims because, as a matter of Indiana law, plaintiffs could not state a claim for "potential damages." Absent an allegation of cognizable damages, plaintiffs also had no sustainable Indiana law claim for breach of contract. The Court of Appeals for the Seventh Circuit agreed and affirmed the district court.

COURT OF APPEALS ANALYSIS

The court of appeals began by holding that a threat of future harm is sufficient to give plaintiffs standing to bring their claims. The court noted that this conclusion was in conflict with the "no standing" decisions of a number of district courts such as *Randolph v. ING Life Ins. & Annuity Co.*[2] and *Bell v. Acxiom Corp.*[3] The court of appeals then turned to the merits of the plaintiffs' claims. Looking to the negligence standard under Indiana state law, the court of appeals concluded that one of the required elements includes "a compensable injury proximately caused by defen-

dant's breach of duty."[4] Thus the threshold question was whether Indiana "would consider that the harm caused by 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 or for breach of contract." The court of appeals held that the answer to that question is "no."

The court found no statute or case law precedent to support a cause of action for such alleged injuries. The court of appeals found the most relevant Indiana authority to be the state's data breach notification statute, passed in March 2006 and made effective as of July 2006. While the law came into effect after the date of the data breach in question, the court of appeals concluded that Indiana's state data breach notification statute demonstrated that the state would not consider monitoring expenses to constitute a compensable injury. The court emphasized that the breach notification statute requires only that a database owner disclose a security breach; there is no requirement that a database owner take other affirmative action upon discovering a breach. Moreover, the data breach notification provides that only the state's attorney general may bring suit in the event that statute is not followed. No cause of action exists for affected customers. Absent a much clearer statement of intent otherwise from the Indiana legislature, the court of appeals determined that consumers' monitoring costs associated with a data breach cannot alone be considered a compensable injury.

Since Indiana's data breach notification law was not directly on point, the court of appeals also examined the reasoning of other federal courts and concluded that "a series of cases has rejected information security claims on the merits."[5] The court of appeals found that all of these cases "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." Accordingly, the plaintiffs' claims failed as a matter of law. This is only the second case where a federal court has dismissed a complaint solely on the pleadings as a matter of law.[6]

IMPLICATIONS

The *Pisciotta* case suggests that, despite the steady stream of high-profile identity theft incidents and the resulting public outcry, courts will likely continue to hold plaintiffs in identity theft cases to traditional standards for proving harm and damages before these individuals will be permitted to recover monetary damages for any alleged injuries.[7] *Pisciotta*, therefore, provides yet another disincentive for these type of class action suits because district courts now have substantial, precedential support for disposing of "prospective harm" data breach complaints as a matter of law without the need to allow discovery.

The court of appeals' approach in *Pisciotta* also accords with the perspective of another federal court of appeals, which recently held that the disclosure of social security numbers is "not sensitive enough" to constitute a 42 U.S.C. § 1983 injury to a constitutional right to privacy.[8] The Court of Appeals for the Sixth Circuit addressed a situation where a state department of corrections released the social security numbers and birth dates of several corrections officers to prisoners held at a state corrections facility. The information was released in the context of a prison investigation into claimed abuse, and the officers feared that the release of this information would jeopardize their lives along with the lives of their families. Nevertheless, the court rejected the federal constitutional privacy claim because "[t]he plaintiffs do not allege that this information allowed the prisoners to discover information that they would have been unable to otherwise."

Like the *Pisciotta* court, the *Barber* court recognized that a compensable injury exists only insofar as the personal information is actually used to some pernicious end. Under these cases, heightened concern stemming from the release of personal information would not itself be enough to claim a compensable injury.

Nonetheless, warning signs of the unsettled nature of this area of law persist. One such indication is the *Pisciotta* court conclusion that the plaintiffs had standing to bring, and thus the court had jurisdiction to entertain, this "prospective harm" case despite the developing body of case law to the contrary. The court of appeals' standing determination

deprives defendants in these actions of a significant basis upon which to bring a motion to dismiss on the pleadings while at the same time leaving defendants subject to the vagaries of state law definitions of their own tort duties. Consequently, should any state recognize a statutory or common law tort cause of action on these facts, the associated litigation costs for a nationwide data security breach will substantially increase the potential downside risk of such a breach. Similarly, the court of appeals' decision on the merits may increase the pressure on state attorney generals to bring more enforcement actions and on state and federal legislators to enact tougher legislation. As always, given the rapidly evolving state of the law in this area, companies would be well advised to adhere to appropriate security practices in storing, handling, and disposing of personal data, in order to minimize reputational damage and avoid exposure to lawsuits. Companies are also well advised to monitor and comply carefully with applicable data breach notification laws, as well as any legal requirements and best practices.

NOTES

[1] No. 06-3817 (7th Cir. Aug. 23, 2007).

[2] 486 F. Supp. 2d 1 (D.D.C. 2007).

[3] 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006) (unpublished).

[4] *Bader v. Johnson*, 732 N.E.2d 1212, 1216-17 (Ind. 2000).

[5] *Citing Kahle v. Litton Loan Servicing, LP*, 486 F. Supp. 2d 705, 712-713 (S.D. Ohio 2007); *Guin v. Brazos Higher Education Service Corp.*, 2006 WL 288483 (D. Ariz. Sept. 6, 2005) (unpublished); *Stollenwerk v. Tri-West Healthcare Alliance*, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005) (unpublished).

[6] *See Hendricks v. DSW Shoe Warehouse, Inc.*, 444 F. Supp. 2d 775, 778 (W.D. Mich. 2006) (dismissing complaint on the pleadings "as a matter of law" where "[t]here is no existing Michigan statutory or case law authority to support plaintiff's position that the purchase of credit monitoring constitutes either actual damages or cognizable loss"). In *Randolph v. ING Life Ins. & Annuity Co.*, No. 06-4932, at *5 (D.C. Sup. Ct. June 13, 2007), the Superior Court of the District of Columbia, on remand, echoed the federal district court in dismissing the complaint for lack of standing. Significantly, however, the

Superior Court also noted that, in these types of cases, dismissal for lack of standing and dismissal for failure to state a claim "are first cousins." The court concluded this is so because "[w]ithout a cognizable injury-in-fact, Plaintiffs lack standing to sue and, for the same reason, have arguably not stated a claim for relief under any of the various [alleged] tort theories." *Id.* (The defendant in that action, ING Life Insurance & Annuity Company, was represented in the federal district court and D.C. Superior Court by the authors' firm.)

[7] Indeed, a few days after *Pisciotta* was decided, a state court, in *Kulpa v. Ohio University*, No. 06-4202 (Ohio Ct. of Claims August 29, 2007), similarly dismissed a class action lawsuit brought on behalf of thousands of individuals whose Social Security numbers and other personal information were exposed to hackers who broke into Ohio University's computer network in 2006. The plaintiffs in that case claimed that Ohio University should be ordered to provide credit-monitoring services to the affected individuals, but the Ohio court of claims held that — absent evidence of actual identity theft — the mere fear of potential damages due to the release of personal information is not among the type of compensable damages recognized by Ohio's tort laws.

[8] *See Barber v. Orton*, No. 05-2014 (6th Cir. August 2, 2007).