THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor: Kirk J. Nahra, CIPP

Data Breach Litigation on the Rise—Eleventh Circuit Allows Data Breach Putative Class Action to Proceed

November 8, 2012


By David M. Governo and Corey M. Dennis, CIPP/US

A recent decision from the U.S. Court of Appeals for the Eleventh Circuit may lead to an uptick in data breach litigation. In *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012), the Eleventh Circuit, addressing issues of first impression, held that the plaintiffs' allegations of injury and causation were sufficient to withstand a motion to dismiss where they suffered identity theft due to a data breach affecting their health insurer, AvMed.

Background

The plaintiffs in this putative class action brought claims for negligence, negligence per se, breach of contract, breach of implied contract, breach of the implied covenant of good faith and fair dealing, breach of fiduciary duty and unjust enrichment in Florida state court. They alleged that two unencrypted laptops containing their personal information—including protected health information, Social Security numbers, names, addresses and phone numbers—as well as the personal information of approximately 1.2 million other current and former AvMed members, was stolen from AvMed's corporate office in December 2009.

The plaintiffs also alleged that this information was readily accessible because AvMed did not properly secure the laptops, which were later sold to an individual with a history of dealing in stolen property. Ten and 14 months later, financial accounts were opened in the plaintiffs' names and used to make unauthorized purchases. The plaintiffs sought to represent the class of AvMed customers whose sensitive information was stored on the

stolen laptops and a subclass of individuals whose identities had been stolen since the thefts.

AvMed removed the case to federal court and filed a motion to dismiss for failure to state a claim. The plaintiffs amended their complaint twice, and AvMed again moved to dismiss the complaint. The United States District Court for the Southern District of Florida granted the motion, concluding, among its "other deficiencies," the amended complaint failed to allege any cognizable injury.

Standing and injury

On appeal, the Eleventh Circuit began by addressing the issue of standing, acknowledging that whether a party "claiming actual identity theft resulting from a data breach has standing to bring suit" was an issue of first impression in the Eleventh Circuit. To demonstrate proper standing, the court explained, the plaintiffs were required to show that they suffered an "injury in fact" that was "fairly traceable" to the defendant's actions and redressable.

The court concluded that the plaintiffs' allegations, which indicated that they became the victims of identity theft after the unencrypted laptops containing their sensitive information were stolen, easily met this standard. The court also held that the plaintiffs' monetary loss was a cognizable injury under Florida law, rejecting AvMed's arguments to the contrary.

Causation

The court then analyzed whether the plaintiffs' allegations of causation were sufficient to support their claims of negligence, negligence per se, breach of fiduciary duty, breach of contract, breach of implied contract and breach of the implied covenant of good faith and fair dealing. The plaintiffs' complaint alleged that the unencrypted stolen laptop contained their sensitive information, that their identities were stolen and that the stolen identities were used to open unauthorized accounts.

The court held that the plaintiffs' claims adequately demonstrated a "nexus" between the data breach and identity theft because the allegations indicated that the compromised information was the same information used to steal the plaintiffs' identities and that the plaintiffs had taken "substantial precautions" to protect their personal information. The court reversed the district court's dismissal of these claims, concluding that these allegations showed "more than a coincidence of time and sequence."

Other claims

The court also held that the plaintiffs' unjust enrichment claim was sufficient because it alleged that they conferred a monetary benefit on AvMed in the form of monthly premiums, which AvMed used to pay for the administrative costs of data security, and that AvMed failed to implement adequate data security measures in accordance with industry standards.

However, the court found that the plaintiffs' negligence per se claim failed because it was based upon a Florida statute that did not apply to AvMed. The breach of the covenant of

good faith and fair dealing claim also failed, given that it did not allege a "conscious and deliberate act" that frustrated "the common purpose" of AvMed's agreement with the plaintiffs, as required under Florida law.

Implications

The case law is evolving in the area of data breach litigation. The *Resnick* decision is significant, given that it addressed both standing and causation in data breach cases, issues of first impression in the Eleventh Circuit. In particular, *Resnick* provides guidance on the causation requirement in data breach cases, which has been addressed by few courts thus far. The *Resnick* court held that a showing of "proximate cause" requires a logical relationship between the data breach and identity theft "beyond allegations of time and sequence," concluding that 10- and 14-month time intervals were not too temporally distant, given the circumstances.

The existing case law diverges on the allegations necessary to establish standing in data breach cases. Some courts have held that the mere threat of identity theft is sufficient to confer standing. *See* *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (holding, on issue of first impression, that class action plaintiffs had standing where they alleged threat of identity theft); *Pisciotta v. Old Nat. Bancorp,* 499 F.3d 629, 634 (7th Cir. 2007) (same); *Ruiz v. Gap*, Inc., 380 F. App'x 689, 691 (9th Cir. 2010) (same).

Others have reached a contrary conclusion, holding that the plaintiff has no standing in these circumstances. *See* *Reilly v. Ceridian Corp.,* 664 F.3d 38, 43 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2395 (2012) (affirming dismissal of case for lack of standing where risk of future harm was alleged); *Katz v. Pershing, LLC*, 672 F.3d 64, 78 (1st Cir. 2012) (same). In *Reilly*, the Third Circuit distinguished *Pisciotta* and *Krottner*, reasoning that the threatened harms were significantly more "imminent" and "certainly impending" in both cases because they involved intentional and malicious breaches. Similarly, in *Katz*, the First Circuit explained that the plaintiff's decision to purchase identity theft insurance and credit monitoring services must be "premised on a reasonably impending threat" of "actual or imminent" harm to confer proper standing.

Courts have also reached inconsistent conclusions on the injury requirement in data breach cases, with some holding that "mitigation damages"—such as fees for replacement credit/debit cards, identity theft insurance and credit monitoring—or the lost "value" of personal information by a provider of paid services, constitute a cognizable injury. *See* *Anderson v. Hannaford Bros. Co.,* 659 F.3d 151, 162-67 (1st Cir. 2011) (holding class action plaintiffs' negligence and implied contract claims were cognizable where plaintiffs alleged mitigation damages arising from the theft of millions of credit and debit card numbers); *Claridge v. RockYou, Inc.,* 785 F. Supp. 2d 855, 864-66 (N.D. Cal. 2011) (holding class action plaintiff's breach-of-contract and negligence claims were sufficient where they alleged lost unidentified "value" and/or a "property right" inherent in plaintiff's personal information following data breach affecting developer of social media applications); *Kuhn v. Capital One Fin. Corp.,* 67 Mass. App. Ct. 1111, 2006 WL 3007931 (2006) (slip op.) (holding that "the value of the time spent" by the plaintiff to prevent further identity theft was compensable injury, even though she did not have to pay charges on fraudulent accounts).

Other courts have held that a showing of actual identity theft is necessary to establish the injury requirement. *See* *Krottner v. Starbucks Corp.*, 406 F. App'x 129, 131 (9th Cir. 2010) (affirming dismissal of plaintiffs' negligence claims based on conclusion that the "mere danger of future harm" is not a cognizable injury); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, MDL No. 11MD2258, 2012 WL 4849054, at *12 (S.D. Cal. Oct. 11, 2012) (same).

The *Resnick* decision makes clear that an allegation of actual financial loss is sufficient to establish both adequate standing and a cognizable injury in data breach cases. The decision also underscores the importance of maintaining adequate security measures, including encryption of laptops and mobile devices, to reduce the risk of a data breach.

David M. Governo *is the founding partner of Governo Law Firm LLC, an 18-attorney law firm in Boston, MA. For over three decades, he has advised companies on a range of risk management and compliance issues and defended companies in complex litigation. He has attained Martindale-Hubbell's highest "AV" rating, is an active member of the Federation of Defense and Corporate Counsel and has been voted a New England Super Lawyer for many years.*

Corey M. Dennis*, CIPP/US, defends companies in complex litigation and advises companies on risk management and compliance issues at Governo Law Firm LLC. He has counseled businesses on compliance with data privacy laws, is a Certified Information Privacy Professional (CIPP/US) and has published numerous legal articles in the areas of data privacy, civil litigation, social media, product liability and employment law.*