

DATA BREACH CASELOAD: ABOUT TO BLOW?

By Henry R. Chalmers, Litigation News Associate Editor

In a departure from litigation trends in other circuits, the U.S. Court of Appeals for the Eleventh Circuit recently lowered the bar for data breach plaintiffs to allege sufficient causation to survive a motion to dismiss. At the same time, it adopted a broad scope of recoverable unjust enrichment damages in data breach lawsuits. *Resnick v. AvMed, Inc.* As a result, data breach class actions may be a step closer to the sizable payoffs they have threatened for the past several years.

The plaintiffs in *Resnick* did not allege facts directly tying the data breach to subsequent identity thefts. Yet, the appellate court found the allegations satisfied the *Twombly/Iqbal* pleading standards because the plaintiffs alleged they had adequately safeguarded their personally identifiable information (PII), and that the information accessed in the data breach was the same kind of information used to steal their identities nearly a year later.

The appellate court also allowed the plaintiffs to proceed with their allegation that AvMed, a health plan provider, was unjustly enriched by premium payments, because those premiums were used ostensibly for data management and security that allegedly failed to safeguard the putative plaintiff class's PII.

DATA BREACH EXPLOSION

The last decade brought with it a world-wide explosion of data breaches involving PII. A recent study by Verizon found that in 2011, more than 850 security breaches were reported, involving more than 170 million confidential records. These breaches sometimes lead to actual identity thefts in which the PII is used to open financial accounts and make fraudulent purchases in the victims' names. Other times, the threat of identity theft exists but may not come to fruition for months, if ever.

"Most data breaches occur because a company that possesses its customers' or employees' PII—such as names, dates of birth, social security numbers, and sometimes even credit card numbers and passwords—fails to adequately protect it from outside access," says W. David Hubbard, Basking Ridge, NJ, cochair of the Internet/Privacy Subcommittee of the ABA Section of Litigation's Intellectual Property Litigation Committee. "Then, when hackers gain access to

the company's computer system, or the company loses a laptop containing unencrypted PII, that information can be used to create phony credit card accounts and perform other financial transactions," he explains.

Data breaches are growing in scope and sophistication, according to Scott F. Bertschi, Atlanta, cochair of the Section of Litigation's Professional Liability Litigation Committee. "Carriers offering data breach insurance policies are trying to keep pace," he observes, "but it's a challenge with the nature of the threat and the relevant case law evolving so quickly."

Another recent study by NetDiligence, a cyber risk assessment firm, concludes that, among companies reporting breaches to their insurance carriers, the average cost per breach is \$3.7 million, the average cost of litigation defense is over \$500,000, and the average cost of settlement with the putative plaintiff class is \$2.1 million. Against this backdrop, attorneys and courts are scrambling to define the claims that can grow out of such a breach and what must be alleged to satisfy the demanding *Twombly* and *Iqbal* pleading standards.

IS IDENTITY THEFT NEEDED TO CONFER STANDING?

"Not all data breaches result in actual identity thefts," says Vanessa J. Soman, New York, cochair of the Internet/Privacy Subcommittee of the Section's Intellectual Property Litigation Committee. "Sometimes a laptop with PII is lost and that's the last we hear of it," she notes, "and sometimes a hacker accesses PII, but no identity theft results."

Most courts find that a data breach without subsequent identity theft is not a sufficient injury to confer standing. For example, in *Reilly v. Ceridian Corp.*, a hacker accessed computers containing PII for more than 25,000 of the defendant's employees. Because there were no allegations of resulting misuse of the data, however, the Third Circuit affirmed the plaintiffs' lack of standing. "Allegations of 'possible future injury' are not sufficient to satisfy Article III [of the U.S. Constitution]," the appellate court found.

Other courts reach similar conclusions where storage media containing PII has been lost or misplaced, e.g., *Whitaker v. Health Net of California*; *Hammond v. Bank of New York Mellon Corp.* But this is not always the case.

In *Pisciotta v. Old National Bancorp*, the U.S. Court of Appeals for the Seventh Circuit found standing even though the plaintiffs did not allege identity theft injury due to the data breach. The Seventh Circuit observed that the breach was “sophisticated, intentional, and malicious,” which apparently prompted the court to conclude that the increased risk of identity theft attributable to the breach was sufficient to confer standing.

The U.S. Court of Appeals for the Ninth Circuit reached a similar conclusion in *Krottner v. Starbucks Corp.* Two months after laptops containing employee PII were stolen from Starbucks, someone tried to open a new bank account using the social security number of one of the plaintiffs. The attempt failed, but the appellate court found the threat of future identity theft sufficient nonetheless to satisfy Article III’s standing requirements.

ANOTHER HURDLE FOR PLAINTIFFS

Even where standing is found, other hurdles remain. To avoid dismissal, a court also must find that the plaintiffs have stated a claim upon which relief can be granted. Under Rule 12(b)(6), courts uniformly require that the data breach lead to actual identity theft before they will find a cognizable injury.

In *Holmes v. Countrywide Fin. Corp.*, a Countrywide employee stole, and then sold, PII of 2.4 million Countrywide loan customers. Countrywide offered each affected customer two years of free credit monitoring, but the heightened risk of future identity theft prompted some affected loan customers to purchase their own credit monitoring services. The district court, however, found that “scant evidence exists demonstrating that [the thieves] misused the customers’ information or engaged in any kind of financial fraud.” Thus, while the district court recognized the plaintiffs’ standing, it dismissed their claims for failure to allege a cognizable injury.

As another court explained, “An increased risk of [future] identity theft, even accompanied by credit-monitoring costs, does not constitute present injury.” *Worix v. MedAssets, Inc.* Thus, even in *Pisciotta* and *Krottner*, where the plaintiffs were found to have standing, the claims ultimately were dismissed for lack of a cognizable injury.

MEETING THE TWOMBLY/IQBAL STANDARD

What must a data breach plaintiff allege to survive a motion to dismiss? A recent decision of the U.S. Court of Appeals for the First Circuit is instructive. In *Anderson v. Hannaford Bros. Co.*, hackers stole 4.2 million credit and debit card numbers and security codes from a Maine grocery chain. The defendant acknowledged that more than 1,800 incidents of identity theft resulted from the breach. Many victims had to pay to cancel their cards or purchase credit monitoring services. Others were hit with unauthorized charges.

The First Circuit found this set of facts sufficient to allege cognizable damages and reversed the trial court’s dismissal. “The court’s ruling in *Anderson* may be explained by the abnormally large number of identity thefts and the fact that the defendant appears to have essentially agreed that they resulted from the data breach,” says Hubbard. “In most cases,” he adds, the defendant “does not admit causation, and the actual source of the data used in the identity theft remains unclear.”

With defendants understandably hesitant to admit causation, how can plaintiffs survive a *Twombly/Iqbal* challenge? “When a data breach is followed in time by identity thefts, the challenge is determining whether the thieves got the PII from the data breach at issue or from some other source that didn’t involve the defendant,” explains Soman. The question of liability can hang in the balance. “Obviously, if a plaintiff class can survive a motion to dismiss based solely on supposition that the theft ‘must have’ resulted from the breach, then the specter of liability increases significantly,” Soman observes.

“Thus far, though, cases with tenuous connections between the breach and

the alleged identity theft haven’t fared well against motions to dismiss,” she notes. That may change with the Eleventh Circuit’s recent decision in *Resnick v. AvMed, Inc.*

ELEVENTH CIRCUIT LOWERS THE BAR

In *Resnick*, thieves stole two laptops from an AvMed office containing the names, addresses, phone numbers, and social security numbers of 1.2 million AvMed customers. They then sold the laptops to a known trafficker in stolen property.

Ten months after the breach, a bank account was opened and credit cards were issued in the name of one AvMed customer. Four months later, an E*Trade account was opened in the name of another AvMed customer. Unauthorized purchases were made from both accounts. The two customers sued AvMed on behalf of a putative class of customers whose PII was on the stolen laptops and a subclass of those customers whose identities were later stolen.

The U.S. District Court for the Northern District of Florida granted AvMed’s motion to dismiss, finding that the plaintiffs failed to allege a cognizable injury. The U.S. Court of Appeals for the Eleventh Circuit reversed on six of eight counts.

As an initial matter, the appellate court easily found the plaintiffs had established the requisite standing because the plaintiffs alleged actual theft. The court then turned to the question of whether the complaint stated a claim upon which relief could be granted—specifically, whether the plaintiffs sufficiently alleged causation to satisfy the *Twombly/Iqbal* standard.

The court noted that, generally, “to prove that a data breach caused identity theft, the pleadings must include allegations of a nexus between the two instances beyond [mere] allegations of time and sequence.” Thus, the fact that the identity thefts occurred relatively close in time and after the data was allegedly misappropriated is not sufficient to state a claim.

In *Resnick*, however, the plaintiffs also alleged that they had never experienced identity theft prior to the data breach and

that they had taken “substantial precautions” to safeguard their PII. They further alleged that “the sensitive information on the stolen laptop was the same sensitive information used to steal Plaintiffs’ identity.”

This was enough to convince a two-judge majority of the appellate court that the plaintiffs had alleged a sufficient nexus to state a viable claim. The third judge dissented. “Although it is conceivable that the unknown identity thieves used the sensitive information stolen from AvMed to open the fraudulent accounts,” the dissent opined, “it is equally conceivable, in the light of the facts alleged in the complaint, that the unknown identity thieves obtained the information from third parties.” Thus, according to the dissent, the plaintiffs failed to nudge their claims “across the line from conceivable to plausible.”

“The sizeable gap in time between the data breach and the subsequent identity theft in *Resnick* is significant,” says Bertschi. “Many policies only cover data breach response costs for breaches that both occurred in and were discovered during the policy period,” Bertschi explains, “but the ruling in *Resnick* creates a need for response costs well after the event.” And those costs are not insubstantial. “A single data breach can impact tens or hundreds of thousands of accounts,” Soman notes, explaining that “response costs can run a couple hundred dollars per record.”


To understand the impact of this per-account expense, consider a data breach class action that was recently filed against the Department of Defense arising from theft of computer tapes. The tapes contained PII for almost 5 million active and retired military personnel, and the lawsuit seeks \$1,000 in damages for each affected individual. What may appear at first to be a fairly modest sum becomes considerable in the aggregate.

USING UNJUST ENRICHMENT TO AVOID DISMISSAL

Unjust enrichment claims may provide another vehicle for surviving motions to dismiss because causation is not an element of the claim. But how big a threat

can such a claim be? Pretty big, says the *Resnick* court.

The plaintiffs in *Resnick* allege that AvMed used their health care premium payments to pay for, among other things, “the administrative costs of data management and security.” And because AvMed allegedly “failed to implement or inadequately implemented policies to secure sensitive information, as can be seen from the data breach,” the plaintiffs contend that AvMed was unjustly enriched by the premium payments and “should not be permitted to retain” them. The appellate court’s majority agreed, adopting a fairly expansive definition of what might be recoverable through such a claim.

“If other circuits follow the Eleventh Circuit’s lead, we should expect to see more data breach class actions clear the initial motion to dismiss hurdle,” says Bertschi. Other challenges will remain, however, including class certification and motions for summary judgment, where plaintiffs will have to support their causation allegations with actual evidence. So, is the data breach volcano about to blow? Maybe not just yet—but the pressure continues to mount. 

RESOURCES

-  *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012).
-  *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3rd Cir. 2011), cert. denied, 132 S. Ct. 2395 (2012).
-  *Whitaker v. Health Net of California, Inc.*, No. 11-0910, 2012 U.S. Dist. LEXIS 6545 (E.D. Calif. January 19, 2012).
-  *Hammond v. Bank of New York Corp.*, No. 08-6060, 2010 U.S. Dist. LEXIS 71996 (S.D.N.Y. June 25, 2010).
-  *Pisciotta v. Old National Bancorp.*, 499 F.3d 629 (7th Cir. 2007).
-  *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010).
-  *Holmes v. Countrywide Fin. Corp.*, No. 08-00205, 2012 U.S. Dist. LEXIS 96587 (W.D. Ky. July 12, 2012).
-  *Worix v. MedAssets, Inc.*, 857 F. Supp. 2d 699 (N.D. Ill. 2012).
-  *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011).
-  Verizon, 2012 Data Breach Investigations

SIGNIFICANT DATA BREACHES IN 2012

Utah Department of Health

On March 30, 2012, personal information was stolen of approximately 780,000 Medicaid patients and recipients of the Children’s Health Insurance Plan in Utah when a hacker accessed a Utah Department of Technology Services server.

Zappos.com

On January 15, 2012, Zappos’ CEO sent a letter to 24 million customers, informing them that information was stolen from the company, perhaps including the last four digits of customers’ credit cards and encrypted passwords.

LinkedIn

In June 2012, LinkedIn confirmed that about 6.5 million LinkedIn passwords were compromised and posted online in a Russian hacker forum.

Yahoo!


In July 2012, Yahoo apologized for a network breach that exposed 400,000 Yahoo! usernames and passwords.

South Carolina Department of Revenue

On November 20, 2012, Governor Nikki Haley alerted South Carolina residents that the state’s Department of Revenue computer system had been hacked, resulting in the theft of 3.6 million social security numbers and 387,000 credit and debit card numbers.

Source: Identity Theft Resource Center, 2012 Breach List, <http://bit.ly/LN382-IDtheft>.

Report, <http://bit.ly/LN382-verizon>.

 NetDiligence White Paper, Cyber Liability & Data Breach Insurance Claims (October 2012), <http://bit.ly/LN382-netdiligence>.