JOURNAL OF INTERNET LAW
VOLUME 15
NUMBER 7
ASPEN PUBLISHERS
JANUARY 2012
EDITED BY DLA PIPER

Two Recent Federal Court Decisions May Signal New Approach to Data Breach Class Action Litigation

By Gary Zhao

Network data breaches and theft of electronically stored personal information have dramatically increased in recent years, giving rise to a litany of class action lawsuits against businesses and organizations that hold and/or transact personal information. In April 2011, Sony Corporation of America became part of a class action lawsuit that was filed in the Northern District of California, on behalf of potentially 12.3 million users who had their credit card numbers stolen off of their PlayStation® network. In October 2011, a veteran and a military family filed a class-action lawsuit in the District of Columbia against the US Department of Defense and its contractor, TRICARE, seeking $4.9 billion dollars in potential damages from the theft of a computer tape containing personal information of 4.9 million beneficiaries of TRICARE.

Historically, common law claims based on negligence and contractual theories in these data breach suits fail to survive the pleading stage, due to lack of actual damages when the only injury to the consumer is emotional harm, increased risk of identity theft, and/or future credit monitoring costs.[1] Absent evidence that a data breach resulted

Continued on page 10

Gary Zhao *is a partner at SmithAmundsen LLC, a law firm headquartered in Chicago, Illinois. Gary focuses his practice on business litigation and counseling.*

Wolters Kluwer
Law & Business

Two Recent Federal Court
Continued from page 1

in actual injury, the courts have generally found the potential risk of future identity theft, or the mitigation of that risk, does not satisfy the "injury in fact" requirement imposed by Article III of the US Constitution. Two recent federal court decisions have bucked the general trend by finding "risk of future harm" type of injuries recoverable at the pleadings stage.

In *Claridge v. RockYou*,[2] a federal district court in California allowed contract and negligence claims to survive a motion to dismiss. In doing so, the district court also recognized an ascertainable "value" inherent in a consumer's personally identifiable information (PII). The defendant in the California case, RockYou, is a company that develops and publishes online applications for social networking sites. Customers sign up by providing a valid email address and registration password, which RockYou then stores in its database. Many customers are also required to provide their Facebook or MySpace usernames and passwords in order to use RockYou's applications. Although RockYou promised on its Web site that it used "commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your personal information,"[3] the company did not use encryption to prevent hackers from "easily" accessing users' PII.[4] The failure to encrypt this information had led to the publication of the contents of RockYou's database on underground hacker forums.[5]

The plaintiff filed a putative class action suit against RockYou, alleging a plethora of statutory and common law claims. The first amended complaint also alleged that plaintiffs' user information has inherent value. The so-called "value" is created when advertisers are attracted to RockYou's platform because it has access to user's personal information.

The attorneys for RockYou brought a motion seeking to dismiss all of the class plaintiffs' claims, particularly, the common law contract and negligence claims, based on the plaintiffs' alleged failure to plead actual damages required to maintain a claim. The motion called the plaintiffs' theory of recovery "speculative" and "an incomprehensible theory."[6]

In opposition to the motion to dismiss, the plaintiffs' mainly argued that the class "paid" RockYou for products and services that they "buy" from the defendant by providing their personally identifiable information—in this instance, email accounts and social network logins.[7] Thus, the plaintiffs argued that their PII represented "valuable property" that was exchanged "not only for defendant's products and services, but also in exchange for defendant's promise to employ commercially reasonable methods to safeguard the PII that is exchanged."[8] The named plaintiff further argued that he has, in fact, already suffered an injury because of RockYou's failure to secure his PII, which, itself, is his personal property. The plaintiff's counsel conceded in his brief that their theory on damages is a novel one and supporting authority for it is scarce.

Though the court dismissed most of the plaintiffs' statutory claims and some its state law claims,[9] it denied RockYou's motion to dismiss with respect to the common law contract and the negligence claims. The court noted, "At the present pleading stage, plaintiff has sufficiently alleged a general basis for harm by alleging that the breach of his PII has caused him to lose some ascertainable but unidentified 'value' and/or property right inherent in the PII."[10] The court emphasized that it "has doubts about the plaintiff's ultimate ability to prove his damages theory in this case"[11] (emphasis added).

Most recently, in *Anderson v. Hannaford Bros. Co.*,[12] the First Circuit Court of Appeals reversed a district court's dismissal of the plaintiff's negligence and implied contract claims after finding that mitigation damages in the forms of identity theft insurance and credit card replacement were recoverable.

The defendant in *Anderson* is a national grocery chain whose electronic payment processing system was breached by hackers in December 2007. The hackers stole up to 4.2 million credit and debit card numbers, expiration dates, and security codes belonging to customers who had made purchases at the defendant's stores.[13] Twenty-six separate lawsuits were filed and subsequently consolidated into one case before the US District Court of Maine.[14] The plaintiffs claim that they had experienced approximately 1,800 unauthorized charges on their credit cards after the breach.[15] In the consolidated suit, the plaintiffs alleged seven claims, including breach of implied contract, negligence, and violation of the Unfair Trade Practices Act.[16] The plaintiffs also alleged that they sustained the following damages, including

but not limited to, cost of card replacement fees, fee for overdrawn accounts, loss of accumulated reward points, emotional distress, and purchase of identify theft insurance and credit monitoring services.[17]

The district court had found that although the plaintiffs had adequately alleged breach of implied contract, negligence, and violation of Unfair Trade Practices Act, the alleged injuries were too unforeseeable and speculative to be recoverable. Therefore, the court dismissed those claims along with the four other claims.[18]

In addressing whether the mitigation damages are cognizable, the First Circuit found instructive cases where courts awarded mitigation costs, even when it is not certain at the time that these costs are needed (see *Toledo Peoria & W. Ry. v. Metro Waste Sys., Inc.*).[19] The question, according to the *Anderson* court, "becomes whether plaintiffs' mitigation steps were reasonable."[20] The court found that it was both reasonable and foreseeable for a customer to replace his credit card after learning that his card had been compromised and fraudulent charges had resulted therefrom.[21] It was also foreseeable for a customer to pay a fee to replace the card and purchase insurance to further protect against misuse of the card. The court concluded that these forms of damages are applicable to the plaintiffs' negligence and implied contract-claims.[22] Thus, the district court's dismissal of those claims was reversed.

Because the American courts have been quick to dismiss data breach suits based on lack of actual damages or standing, there has been little or no incentive, at least from the court system, for businesses holding personal information and/or data to adopt stronger security safeguards to protect personal information. The *Anderson* and *RockYou* decisions could signal an evolving judicial approach to data-breach lawsuits. By allowing data-breach claims to survive at the motion-to-dismiss stage, the *Anderson* and *RockYou* courts have increased the chance of a defendant business being held liable for damages due to a data breach. There are also additional legal fees and costs associated with written and oral discovery and preparation of dispositive motions. Even if a defendant business' liability insurer pays the legal fees, coverage premium for future data breaches could increase as a result of these rulings. These recent decisions should incentivize and encourage relevant businesses to further invest in stronger and tougher security measures to reduce security breaches.

NOTES

1. *Hammond v. The Bank of New York Mellon Corp.*, 2010 U.S. Dist. LEXIS 71996, 2–6 (S.D. N.Y. 2010).
2. 2011 U.D. Dist. LEXIS 39145 (N.D. Cal. 2011).
3. 2011 U.S. Dist. LEXIS 39145 at 3.
4. *Id.* at 3–4.
5. *Id.* at 5.
6. 2009 U.S. Dist. Ct. Motions 6032.
7. 2011 U.S. Dist. LEXIS 39145 at 10.
8. *Id.* at 10–11.
9. Id. at 19, 21.
10. *Id.* at 23.
11. *Id.* at 12.
12. 2011 U.S. App. LEXIS 21239 (1st Cir. 2011).
13. 2011 U.S. App. LEXIS 21239, 3.
14. *Id.* at 5.
15. *Id.*
16. *Id.*
17. *Id.* at 6.
18. *Id.* at 7–8.
19. 59 F.3d 637 (7th Cir. 1995) (applying Illinois law).
20. *Id.* at 33.
21. *Id.* at 35.
22. *Id.* at 42–43.