SINCE 1854

Chicago Daily Law Bulletin®

Volume 157, No. 218 Monday, November 7, 2011

Decisions may show trend in data breach cases

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. Historically, common law claims based on negligence and contractual theories in these data breach suits fail to survive the pleading stage due to a 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. See e.g. *Hammond v. The Bank of New York Mello Corp.* However, two recent federal court decisions have bucked the general trend by finding "risk of future harm" type of injuries recoverable at the pleadings stage.

First, in *Claridge v. RockYou,* a federal district court in California allowed contract and negligence claims to survive a motion to dismiss. In doing so, the district court recognized an ascertainable "value" inherent in a consumer's personally identifiable information (PII). The defendant, RockYou, is a company that develops and publishes online applications for social networking sites. Customers sign up by providing a valid e-mail 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. RockYou's failure to encrypt this information led to the publication of the contents of RockYou's database on underground hacker forums. *Claridge v. RockYou.* 2011 U.D. Dist. LEXIS 39145 (N.D. Cal. 2011).

The plaintiffs filed a putative class-action suit against RockYou alleging a plethora of statutory and common law claims. The first amended complaint also alleged that the 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 users' personal information.

In opposition to the defendant's motion to dismiss the common law claims, the plaintiffs argued that they "paid" RockYou for products and services that they "bought" by providing their personally identifiable information. The named plaintiff further argued that he already suffered an injury in fact because of RockYou's failure to secure his PII, which itself is his personal property.

Though the court dismissed most of the plaintiffs' statutory claims it did not dismiss with respect to the common law contract and the negligence claims. The court noted, "At the present pleading stage, the 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." The court emphasized that it "has doubts about the plaintiff's ultimate ability to prove his damages theory in this case."

In another example of the new trend in data breach class actions, *Anderson v. Hannaford Bros. Co.,* the 1st U.S. 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 forms of identity theft insurance and credit card replacement were recoverable. *Anderson v. Hannaford Bros. Co.* 2011 U.S. App. LEXIS 21239(1st Cir. 2011).

Hannaford Bros. Co, the defendant, 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 their stores. Twenty-six separate lawsuits were filed and subsequently consolidated into one case before the U.S. District Court in the District of Maine. The plaintiffs claim that they had experienced approximately 1,800 unauthorized charges on their credit cards after the breach. In the consolidated suit, the plaintiffs alleged seven claims, including breach of implied contract and negligence. 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 purchasing identify theft insurance and credit monitoring services.

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

On appeal, the 1st Circuit found instructive cases like *Toledo Peoria & W. Ry. v. Metro Waste Sys., Inc.,* where courts awarded mitigation costs even when it was not certain at the time that these costs were needed. The question, according to the appellate court, "becomes whether the plaintiffs' mitigation steps were reasonable." 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. 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 and the district court's dismissal was reversed.

Since the U.S. 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 data breach. There are also additional legal fees and costs associated with written and oral discovery and preparation of dispositive motions. Even if the legal fees are paid by a defendant business' liability insurer, 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.

Gary Zhao is a commercial litigation attorney in SmithAmundsen LLC's Chicago office. He represents clients in complex business litigation matters, including breach of contract, breach of fiduciary duty, false advertising, construction, fraud and other deceptive trade practices and white-collar crime. He is also chairman of the firm's Chinese-American business services team helping Chinese businesses with legal needs in the U.S.