Developments in Data Breach Liability

ALAN CHARLES RAUL, EDWARD McNICHOLAS, DAVID E. TEITELBAUM, AND BLAYNE V. SCOFIELD

As data breaches continue apace, so do enforcement action and litigation. This article describes a recent data breach settlement under the consumer protection statutes of 41 jurisdictions, as well as recent federal and state court judicial opinions addressing liability for data breaches under Maine and District of Columbia law.

In the *Hannaford* decision discussed herein, Judge Hornby succinctly and fairly characterized the growing body of data breach litigation as follows:

> "[T]he cases…are almost uniform in not allowing recovery where there is only a risk of injury and no actual misuse of the stolen electronic data. * * * [And] are almost unanimous: no mandatory credit monitoring, certainly where there is no demonstrated risk."

The jurisprudence of data breaches continues to evolve, however, with courts and regulators becoming increasingly sensitive to whether a business has adequately and "fairly" protected its customers' financial information. The *TJX* discussion below provides useful guidance on what security practices are considered adequate by the bulk of the nation's attorneys general. The discussion of the *Randolph* and *Hannaford* decisions

Alan Charles Raul, Edward McNicholas, and David E. Teitelbaum are partners and Blayne V. Scofield is an associate in the Washington D.C. office of Sidley Austin LLP. They may be contacted at araul@sidley.com, emcnicholas@sidley.com, dteitelbaum@sidley.com, and bscofield@sidley.com, respectively.

Published in the September 2009 issue of Privacy & Data Security Law Journal.

outlines the various legal theories that have been advanced in data breach litigation, and addresses which theories have been rejected out of hand, and which have survived summary disposition.

TJX SETTLES DATA BREACH CLAIMS WITH ATTORNEYS GENERAL

TJX Companies, Inc. ("TJX") and a multi-jurisdictional[1] group of 41 attorneys general ("the Attorneys General") recently agreed to settle claims stemming from a series of data breaches that occurred at TJX in 2005 and 2006. This action is the latest in the flurry of investigation and litigation that followed the TJX data breaches. Under the Assurance of Discontinuance ("the Assurance"), TJX agreed to pay $9.75 million to the jurisdictions and to implement and maintain a comprehensive information security program, and the Attorneys General agreed to conclude their respective investigations and settle and release their civil claims against TJX.

TJX operates over 2,600 retail apparel and home fashion stores in the U.S. and worldwide. In January 2007, TJX disclosed that during periods in 2005 and 2006 unauthorized intruders accessed computer systems at TJX that process and store information from payment card and other transactions. The breaches allowed the intruders to access and seize customer information, including cardholder data. Following disclosure of the breaches, the Attorneys General initiated investigations that paralleled private litigation brought on behalf of consumers and banks allegedly affected by the breaches.

Pursuant to the Assurance, TJX will implement and maintain a comprehensive information security program ("the Program"). TJX will report regularly to the Attorneys General on the efficacy of the Program after obtaining a third party assessment of its systems. For the most part, the Program reiterates standards set forth in the Federal Trade Commission's "safeguarding" regulation and in the Payment Card Industry's Data Security Standard ("PCI DSS"). As part of the Program, TJX must, among other things:

- Designate an employee to coordinate and be accountable for the Program;

- Identify material internal and external risks to the security, confidentiality, and integrity of personal information that could result in unauthorized disclosure, and assess the sufficiency of safeguards in place to control these risks;
- Design and implement reasonable safeguards to control the risks identified through the risk assessment process and regularly test or monitor the effectiveness of the safeguards' key controls, systems and procedures;
- Implement and evaluate modifications to the Program in light of the results of the testing and monitoring, any material changes to TJX's operations or business arrangements, or any other change in circumstances that TJX knows or has reason to know may have a material impact on the effectiveness of the Program;
- Replace or upgrade all Wired Equivalency Privacy-based wireless systems in its retail stores to wired systems or Wi-Fi Protected Access ("WPA") or wireless systems at least as secure as WPA;
- Not store or otherwise maintain certain credit card or debit card data on its network subsequent to the authorization process; provided that TJX may retain a portion of the contents of the magnetic stripe of a credit or debit card on its network subsequent to the authorization process for legitimate business, legal, or regulatory purpose(s), but any such cardholder information must be securely stored in encrypted form, accessed only by essential personnel, and retained for no longer than necessary to achieve the business, legal, or regulatory purpose;
- Use Virtual Private Networks ("VPNs") or, where appropriate, encrypted transmissions, or other methods at least as secure as VPNs for transmission of personal information, including cardholder information, across open, public networks; and
- For portions of the TJX computer system that store, process or transmit personal information, including cardholder information, TJX must:

  (1) Segment such portions of its computer system appropriately from the rest of its system using firewalls, access controls, or other appropriate measures;

(2) Implement security password management;

(3) Implement security patching protocols;

(4) Install and maintain appropriately configured antivirus software;

(5) Implement and maintain security monitoring tools, such as intrusion detection systems or other devices to track and monitor unauthorized access; and

(6) Implement access control measures.

Although TJX is given 120 days to certify its compliance with these security requirements, it generally is provided flexibility to use "alternative measure(s) that alone or in the aggregate provide for substantially equivalent security." Moreover, "compliance" of its in-store point-of-sale terminals with respect to several security conditions is satisfied by the development of "a reasonable and appropriate plan to evaluate the technological and operational feasibility of such provisions." In other words, given the challenges of implementing many security measures at the point-of-sale, the Attorneys' General have given TJX substantial leeway to make its own commercially reasonable judgments, subject to card association requirements, as to the appropriate means of securing cardholder data at the point-of-sale.

In addition to the Program, TJX agreed to notify Visa, MasterCard and its acquiring banks in the U.S. that it desires to participate in pilot programs to test new security-related payment card technology. If invited, TJX will generally participate in any such pilot program during the next two years provided that TJX determines, in good faith, that the security related payment card technology and the terms and conditions of its participation are feasible and reasonable. TJX will also take steps to encourage the development of new technologies within the payment card industry for "end-to-end" encryption cardholder information during the bank authorization process.

As with the settlements of the other pieces of litigation stemming from the TJX data breaches, retailers and others that come into possession of nonpublic personal information, should re-evaluate their own data security programs in light of the standards established in the Assurance.

D.C. COURT OF APPEALS AFFIRMS DISMISSAL IN DATA BREACH LITIGATION

On June 18, the District of Columbia Court of Appeals affirmed the dismissal of a suit against ING Life Insurance and Annuity Company over the loss of a laptop that contained unencrypted personal financial data, including social security numbers, of participants in an employee deferred compensation plan. The laptop was stolen from an ING representative's home in June 2006. The purported class action, originally filed in D.C. Superior Court, was removed to the U.S. District Court for the District of Columbia. The district court found that the plaintiffs' alleged injury was only speculative, and thus insufficient to establish the legal "standing" required for federal jurisdiction. Upon dismissal, the federal court remanded the complaint to the D.C. Superior Court, which likewise dismissed the action for lack of standing and concrete injury. The D.C. court concluded that, in the absence of any allegation that the data in the computer was used or accessed for the purpose of committing identity theft, the plaintiffs' allegations of fear of future identity theft were simply too speculative and remote to support the litigation.[2] Plaintiffs then appealed the dismissal from the D.C. Superior Court to the Court of Appeals, which affirmed as described below.

DISCUSSION

The Court of Appeals affirmed the dismissal of all data breach claims. However, the appellate court largely side-stepped the standing issue, essentially assuming that the plaintiffs had sufficient injury to establish standing. The Court of Appeals did not adopt the Superior Court's reasoning on lack of standing because it drew an (perhaps inapposite) analogy to the Supreme Court's recent federal Privacy Act decision in *Doe* v. *Chao*. The Court of Appeals cited *Chao* to support the perspective that standing is a relatively easy standard to meet. The lack of concrete injury, however, was ultimately fatal to the plaintiffs' claims. When the court turned to the elements of the specific causes of action at issue, it concluded that the defendant could not be found liable for negligence in connection with the

Published in the September 2009 issue of Privacy & Data Security Law Journal.

data breach because no actual identity theft had been alleged. In other words, there was sufficient injury to establish standing, but insufficient injury to state a claim for negligence, because while the plaintiffs feared identity theft, they had not actually suffered it.

The court also dismissed the invasion of privacy count. The court held that invasion of privacy is an "intentional tort," and the complaint failed to allege that the defendant's actions were intentional. Even if the actions were intentional, however, the court held that the complaint failed to allege another required element of the tort — namely, public disclosure of, or unauthorized access to, the private data. In other words, the complaint did not allege that any personal information on the stolen laptop had actually been viewed by any unauthorized person.

The court surmised that the plaintiffs had no basis to allege actual exposure of their data because the data on the stolen laptop may have been deleted or ignored by criminals only interested in the value of the hardware. Finally, the court also dismissed the plaintiffs' statutory claims under D.C. pension fund laws. The court found that the funds in question were not covered by those laws and, in any event, there was no private right of action.

Perhaps significant for future litigation, the Court of Appeals stated that it had no doubt that, if all the required elements were alleged (intentional actions and public disclosure or actual unauthorized access, *etc*.), a data breach involving personal financial information would constitute an intrusion of privacy sufficiently highly offensive to a reasonable person to sustain a claim for invasion of privacy. However, the court also suggested in a footnote that liability for invasion of privacy would not be found where a plaintiff's injury resulted from the intervening actions of a third party wrongdoer that were not foreseeable to the defendant.

Finally, the court also confirmed, unsurprisingly, that it was entirely appropriate for the personal financial information in question to be shared among the defendant's employees and agents for business purposes. The court declined to decide (as unnecessary to the resolution of the issues at hand) whether the defendant financial institution had "a special, confidential relationship" with the account holders whose information was contained on the laptop.

In sum, the *Randolph* litigation continues the prevailing trend in fed-

eral and state courts of recognizing that data breach liability should turn on whether the alleged victims suffered actual harm. The court's rejection of the defendant's "standing" argument, and its hypothetical support for invasion of privacy liability in certain data breach cases, indicate that litigation in this area will continue to evolve.

HANNAFORD WINS PARTIAL DISMISSAL IN MULTI-DISTRICT DATA BREACH LITIGATION

The U.S. District Court for the District of Maine recently issued an order granting in part Hannaford Bros. Co.'s motion to dismiss in *In Re Hannaford Bros.Co. Customer Data Security Breach Litigation*. The purported class action of grocery customers alleged that Hannaford, which operates stores across New England and the east coast, had allowed 4.2 million debit and credit card numbers to be stolen by hackers. The plaintiffs sued in several different jurisdictions, which were consolidated in a multi-district litigation. The amended complaint asserted seven different bases for relief: breach of implied contract, breach of implied warranty, breach of duty of a confidential relationship, failure to advise customers of the theft of their data, strict liability, negligence, and violation of Maine's Unfair Trade Practices Act ("UTPA"). The court stated the issue as follows:

> A customer uses a credit card or debit card to buy groceries. A third party steals the electronic payment data from the grocer. Can the customer then recover from the grocer any loss resulting from the third-party data theft? That is the question this case poses.
>
> Judge Hornby answered his own question this way:
>
> For those wanting a definitive answer to this question of who should bear the risk of data theft in electronic payment systems, my ruling will be unsatisfactory. In this case, the answer depends wholly on state law, and the state law is still undeveloped...
>
> My answer to the liability question between customer and grocer is this: Under Maine law as I understand it, when a merchant is negligent

Published in the September 2009 issue of Privacy & Data Security Law Journal.

in handling a customer's electronic payment data and that negligence causes an unreimbursed fraudulent charge or debit against a customer's account, the merchant is liable for that loss. In the circumstances of this case, there may also be liability under Maine's Unfair Trade Practices Act for an unfair or deceptive trade practice. But if the merchant is not negligent, or if the negligence does not produce that completed direct financial loss and instead causes only collateral consequences — for example, the customer's fear that a fraudulent transaction might happen in the future, the consumer's expenditure of time and effort to protect the account, lost opportunities to earn reward points, or incidental expenses that the customer suffers in restoring the integrity of the previous account relationships — then the merchant is not liable.

DISCUSSION

Ruling under Maine law, as agreed to by the parties, the district court found that only the breach of implied contract, negligence, and UTPA claims were cognizable. First, the court concluded that a jury could find that a promise to take reasonable measures to protect consumer information could be implied in the contract made when customers bought groceries from Hannaford; however, an unqualified guaranty of confidentiality could not be implied, since such a data security term would not be "absolutely essential" to a contract for the purchase of groceries. Next, the court noted that under Maine law, a judge must decide, as a matter of law, whether a defendant has a tort-based duty to a plaintiff; if so, a jury then decides if the defendant acted negligently. The court found that a jury could find that Hannaford was negligent, and held that Maine's doctrine of "economic loss" did not apply in this case. Finally, drawing on First Circuit precedent that interpreted a similar Massachusetts law, the court held that Maine's UTPA could support a claim of unfair or deceptive trade practices here. Specifically, the court found that plaintiffs could state a claim that the grocer's failure to disclose the data breach to customers promptly was an unfair trade practice. The court expressly noted that the standard for upholding a failure to disclose claim under Maine's UTPA was not as exacting as under the common law.

Conversely, the court found that the claims for breach of implied warranty, breach of duty of a confidential relationship, failure to advise customers about the data breach, and strict liability could not be maintained. Under Maine law, a warranty is implied only for the goods sold, not the payment mechanism, and no case from Maine could be found extending such a warranty to services, such as credit card processing, which were offered free and without obligation to the customer. The court also concluded that there was not a confidential relationship established between the parties, especially because the grocery purchase was not characterized by a disparity of bargaining power. Next, the court noted that Maine common law (in contrast to the UTPA, as discussed above) does not recognize a claim for breach of duty to advise on theft of data, particularly when no confidential relationship is established. The court noted that the plaintiffs had not alleged violation of the state's data breach notification law, which does not, in any event, grant a private right of action. Finally, the court declined to expand Maine strict liability law to cover secure payment transactions, despite the plaintiffs' argument that such an activity should be deemed "extra-hazardous" and thus meriting strict liability.

In the second part of its opinion, the court needed to determine which plaintiffs had alleged an injury sufficient to sustain recovery on their claims. The court rejected the claims of any plaintiff that had not suffered any actual fraudulent charges to their account, as well as any plaintiff whose fraudulent charges had been removed by their bank. Consequential losses, such as overdraft fees, new card fees, loss of accumulated reward points, and temporary lack of access to funds were insufficient injuries, since they were too remote, not reasonably foreseeable, and too speculative. For the one plaintiff whose card-issuing bank had not removed the fraudulent charges on her account, the court found she had suffered sufficient injury to proceed against Hannaford on the three claims that the court allowed to proceed.

In short, the court concluded that consumers whose payment data was stolen can recover against Hannaford only if its negligence caused a direct loss to the consumer's account. Those plaintiffs (here, only one named plaintiff) could pursue Hannaford under Maine law only on claims for breach of implied contract, negligence, and violations of Maine's UTPA.

Published in the September 2009 issue of Privacy & Data Security Law Journal.

NOTES

[1] The jurisdictions participating in the settlement are: Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, the District of Columbia, Florida, Hawaii, Idaho, Illinois, Iowa, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Vermont, Washington, West Virginia and Wisconsin.

[2] The authors' firm represented the defendant in this litigation in the U.S. district court and in D.C. superior court.