A New Frontier: Litigation Over Data Breaches

John P. Hutchins, a partner with Troutman Sanders LLP, in Atlanta, represents businesses in various types of commercial disputes and transactions, with particular focus on information technology, intellectual property and privacy and data security. He leads the firm's Internet, E-Commerce & Information Technology Practice Team as well as the firm's Privacy & Data Security Practice Team. John regularly handles a variety of commercial disputes, but has substantial expertise in cases involving computer hardware and software development projects, government procurement, protection of trade secrets and proprietary business information, the Internet and e-commerce, privacy and data security, trademark and copyright infringement, and restrictive covenants. He has been lead counsel in numerous jury trials and bench trials in state and federal courts, as well as arbitration and mediation proceedings. He also regularly negotiates complex technology transactions and advises clients on corporate policy matters and regulatory compliance issues involving e-commerce, privacy and data security. John has been recognized as one of America's leading lawyers by *Best Lawyers in America.*

Renard C. Francois is an attorney for Caterpillar Inc. in Peoria, Illinois. He focuses on issues related to data privacy and data protection. This article is based on a paper the authors prepared for a seminar sponsored by the ABA's Section of Litigation

John P. Hutchins and Renard C. Francois

Corporate clients take notice: The FTC and individuals are ready to litigate when data security breaches occur.

2005 WAS CALLED "The Year of the Data Breach," as media outlets were flooded with stories of one data breach after another. 2006 and 2007 were worse, as the floodgates remained wide open. Estimates vary, but it is safe to say that the total number of reported data breaches from 2005 to 2007 combined topped 750. These breaches have involved more than 150 million records containing personal information. Reported data breaches in 2008 averaged around one per day!

A flood of plaintiffs' attorneys have attempted to take advantage of the misfortune of all associated with data breaches. Thus far, however, plaintiffs have enjoyed limited success on behalf of consumers, whether in class actions or on behalf of individuals. The second half of this article explores the reasons why data breaches are not necessarily the low-hanging fruit that plaintiffs' lawyers had hoped.

But those experiencing data breaches face another litigation threat. Claiming authority under the Federal Trade Commission Act, the Federal Trade Commission has brought several high-profile actions against organizations experiencing data breaches. *See, e.g., In the Matter of BJ's Wholesale Club, Inc., United States Federal Trade Commission,* File No. 042 3160 (Sept. 23, 2005) available at www.ftc.gov/os/

caselist/0423160/0423160.shtm; *United States of America v. ChoicePoint Inc.*, United States District Court for the Northern District of Georgia, Civil Action No. 1:06-CV-0198 (Jan. 30, 2006), available at www.ftc.gov/os/caselist/choicepoint/choicepoint.shtm; *In the Matter of DSW, Inc.*, United States Federal Trade Commission, File No. 052 3096 (March 14, 2006), available at www.ftc.gov/os/caselist/0523096/0523096.shtm; *In the Matter of CardSystems Solutions, Inc., and Solidus Networks, Inc., d/b/a/ Pay By Touch Solutions*, United States Federal Trade Commission, File No. 052 3148 (Sept. 8, 2006), available at www.ftc.gov/os/caselist/0523148/0523148.shtm. Betsy Broder, Assistant Director of the FTC's Division of Privacy and Identity Protection, made the following statements in the March 2006 edition of the ABA Journal: "Unless you're one of a few businesses that are exempt from our jurisdiction, like insurance companies, we will act against businesses that fail to protect their customer data…. At a basic level… businesses need to have a plan in writing describing how customer data is to be secured and an officer on staff responsible for implementing that plan." Jason Krause, *Stolen Lives*, 92 ABA Journal 36, 40, (Mar. 2006). Assistant Director Broder further stated that all businesses should look to Gramm-Leach-Bliley for guidance on how to protect consumer data. *Id.*

Many legal commentators have wondered aloud whether the Federal Trade Commission Act authorizes the FTC to police the data security practices of American businesses. The first part of this article examines the FTC's claimed authority under the Federal Trade Commission Act.

THE FEDERAL TRADE COMMISSION ACT • The Federal Trade Commission Act empowers the Federal Trade Commission to prevent persons, partnerships, or corporations from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce. 15 U.S.C. §45(a)(2). In its actions against companies experiencing data breaches, the FTC has generally alleged that the companies' lax data security practices constitute "unfair and deceptive trade practices."

Lax Data Security: Is It "Unfair"?

In terms of what the Act means by "unfair," the FTC determined that enough cases had been decided to enable it to identify three criteria to use in determining whether a practice, which is neither anticompetitive nor deceptive, is nonetheless unfair to consumers:

"(1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; (3) whether it causes substantial injury to consumers (or competitors or other businessmen).

Appended to *International Harvester Co.*, 104 F.T.C. 949, 1072 n.8 (1984). *See* 15 U.S.C. §45(n).

In *FTC v. Sperry & Hutchinson*, 405 U.S. 233 (1972), the Supreme Court "put its stamp of approval on the Commission's evolving use of a consumer unfairness doctrine not moored in the traditional rationales of anticompetitiveness or deception." *American Financial Services Ass'n. v. FTC*, 767 F.2d 957, 971 (D.C. Cir. 1985), *cert. denied*, 475 U.S. 1011 (1986).

In 1980, the Commission issued its "Unfairness Statement." Most recently, in 1994, Congress amended the FTC Act by effectively codifying the Commission's modern definition of unfairness in Section 5(n):

"The Commission shall have no authority under this section or section 18 to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination."

15 U.S.C. §45(n).

To pursue a cause of action successfully under the FTC's current unfairness standard, the Commission must establish that:

- The respondent/defendant has engaged in an act or practice that caused, or is likely to cause, substantial injury to consumers;
- The injury is not reasonably avoidable by consumers; and
- The injury to consumers is not outweighed by countervailing benefits to consumers or to competition.

Id.

It may be questionable whether the data security practices of those the FTC has pursued are actionable under this standard. There is scant evidence that any consumer has, in fact, been substantially injured by the data breaches. Although the FTC alleged in its Complaint against ChoicePoint, for example, that ChoicePoint's data breach (involving approximately 163,000 personal records) led to "at least 800 incidences of identity theft," proving this allegation would have been extremely difficult for the FTC had ChoicePoint not settled. Establishing a causal link between a data breach and a specific instance of identity theft may be impossible. In ChoicePoint's case, the percentage of identity theft victims the FTC alleged—half of one percent—is less than the occurrence rate in the general population, which the FTC itself has stated is 4.6 percent per year. Federal Trade Commission, *Identity Theft Survey Report* (September 2003), available at www.ftc.gov/os/2003/09/synovatereport.pdf. In addition, there appears to be little evidence that data breaches are generally a source of identity theft. Survey results show that conventional methods such as lost or stolen wallets, misappropriation by family and friends, and theft of paper mail are by far the most common forms of identity theft. There is, to date, very little if any empirical survey evidence attributing any percentage of identity theft to large scale data breaches. Joris Evers, *Separating Myth from Reality in ID Theft*, CNET News.com October 24, 2005, http://news.cnet.com/Sparating-myth-from-reality-in-ID-theft/2100-1029_3-5907165.html. And, as even the FTC itself acknowledges, "Victims [of identity theft] are generally not liable for losses based on fraudulent action taken by identity thieves using their personal information." *Identity Theft Survey Report*, supra, at p.6 n.4. Thus, whether alleged "lax security practices" that lead to data breaches can be characterized as "a practice that caused, or is likely to cause, substantial injury to consumers" may be doubtful.

Also, it could be argued, in the wake of some 44 states (according to the National Conference of State Legislatures) having enacted data breach notification laws, that the injury to consumers is reasonably avoidable. If consumers act on the notifications and employ available precautions such as fraud alerts, identity theft may indeed be reasonably avoidable.

The FTC has settled the cases it has brought against high-profile entities that have experienced data breaches. No court has yet ruled on whether Section 5 of the FTC Act gives the FTC authority to police industry security practices as "unfair." It

has been said about the first data breach notification statute—SB 1386—that the law "uses fear and shame to make companies think more seriously about information security." Sarah Lourie, *The FAQs about SB-1386.* Available at http://searchcio.techtarget.com/news/article/0,289142,sid182_gci941077,00.html. In its actions under the FTC Act against entities experiencing data breaches, the FTC has likewise relied on fear and shame—the fear that large, high-profile business have of being "the test case" under Section 5, and the shame associated with a large-scale data breach, principally the desire for the story simply to go away. Thus far, all of the FTC's two dozen or so targets have similarly been persuaded into settling the FTC's charges, whether or not the FTC actually has statutory authority under Section 5 of the FTC Act.

PRIVATE LITIGATION ARISING FROM DATA BREACHES • Lawsuits against companies for the loss of a customer's sensitive financial information are nothing new. In the past, the plaintiffs had difficulty surviving motions to dismiss primarily because of their inability to demonstrate that the mere loss of data caused them a legally cognizable injury. To a certain extent, the damages hurdle has not been lowered despite the recent creativity of plaintiffs. However, plaintiffs, typically financial institutions, have become increasingly creative in their causes of action, and courts have been relatively consistent with their approach to certain causes of action. For example, the cases discussed below demonstrate that courts have consistently applied the "economic loss" doctrine to dismiss a plaintiff's negligence claim. Additionally, courts have consistently dismissed breach of contract claims brought by financial institutions arguing that they are third party beneficiaries to contracts between a breached retailer and its merchant bank. Yet, the recent class actions against TJX show that industry-wide standards are playing an important role in establishing a cause of action for negligent representation.

Four cases highlight the difficulty private litigants, individuals, and financial institutions have when suing a company for a data breach. The first case demonstrates the challenges that individuals, or a class of individuals, face in proving injury as a result of the data breach. The second case shows how plaintiffs have attempted to circumnavigate that issue by arguing that a data breach has increased the possibility that their personal data might be exploited by an identity thief. Anticipated injury or fear of a future crime is insufficient to meet the injury requirement.

Guin v. Brazos Higher Education Services And Bell v. Acxiom Corporation

To date, the victims of data theft have been unsuccessful in pursuing claims against data handlers for failure to secure personal or company information. In *Guin v. Brazos Higher Education Services,* 2006 U.S. Dist. LEXIS 4846 (D. Minn. Feb. 7, 2006), a company negligently permitted one of its employees to store unencrypted private customer data on a laptop computer that was later stolen. The company sent a notification letter warning about the laptop theft to all of its approximately 550,000 customers. One of Brazos' customers filed suit based upon breach of contract, breach of fiduciary duty, and negligence. The aggrieved customer produced no evidence that a third party had accessed his personal information; much less that he was a victim of fraud, identity theft, or any other damages. The court granted the defendant's summary judgment motion because of the plaintiff's failure to trace cognizable damages arising from the defendant's breach of the standard of care. The court found that the plaintiff failed to demonstrate a present and actual injury that resulted from the allegedly negligent security practices.

In *Bell v. Acxiom Corporation,* 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006), a class action lawsuit was filed against Acxiom (a company that stores personal, financial and other company data for cor-

porate clients) because an Acxiom client exploited a vulnerability in Acxiom's security and accessed Acxiom's server, downloaded other clients' databases, and then sold some of the information to a direct-mail marketer. The complaint sought "relief on behalf of all residents of the United States whose personal information was unlawfully taken" from Acxiom's Internet-accessible computers subsequent to January 1, 2001. It further alleged that Acxiom protected this information with insufficient security measures, such as a username and password which was frequently the same name as the customer's name, and usernames and passwords that were not changed with sufficient frequency. According to the plaintiff, due to Axciom's practices she suffered an increased risk of both receiving unsolicited mailing advertisements and of identity theft.

The complaint sought a declaration that Acxiom's security measures were inadequate, notice to all class members of the times their private information was breached, how it was breached, by whom, and what remedial action Acxiom had taken. The plaintiff also sought an injunction requiring Acxiom to remove the private information from its computer system and preventing it from obtaining any such private information in the future, plus compensatory and punitive damages.

In dismissing the complaint for lack of standing and entering judgment in favor of Acxiom, the court held that assertions of future injury did not satisfy the requirement for injury. The court also added that a threatened injury "must be certainly impending" to constitute injury in fact. *Id.* at 2. With respect to plaintiff's asserted damages, the court found that receiving unsolicited mailing advertisements and an increased threat of identity theft was insufficient to serve as damages. "A plaintiff may recover damages for an increased risk of harm in the future [only] if such risk results from a present injury and indicates a reasonably certain future harm." *Forbes v. Wells Fargo Bank, N.A,* 420 F. Supp. 2d 1018, 1020 (D. Minn. 2006).

Banknorth, N.A. v. BJ's Wholesale Club, Inc. and *Sovereign Bank v. BJ's Wholesale Club, Inc.*

The third and fourth cases involve companies suing other companies over data security breaches that exposed customer financial information. These cases arise out of the breach incurred by BJ's Wholesale and were brought by two banks against BJ's Wholesale. These two cases were just as unsuccessful as those cases previously discussed. BJ's Wholesale cases demonstrate the challenges that these companies face when trying to recover costs related to the issuance of new payment cards. In *Banknorth, N.A. v. BJ's Wholesale Club, Inc.*, 442 F. Supp. 2d 206 (M.D. Pa. 2006), the court rejected Banknorth's tort and contract claims. In *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 427 F. Supp. 2d 526 (M.D. Pa. 2006), *aff'd in part, rev'd in part,* 533 F.3d 162 (3d Cir. 2008), the court dismissed the tort claims against BJ's and BJ's merchant bank.

Banknorth filed breach of contract, negligence, and equitable subrogation claims against BJ's. On the contract claim, Banknorth asserted that it was a third-party beneficiary of a contact between BJ's and its own bank, which had obligated BJ's to follow certain security practices and standards to protect customer financial information. However, the court rejected the third-party beneficiary claim because the contract contained a provision stating that there was to be no third-party beneficiary of the contract. Regarding the negligence claim, the court reasoned that Banknorth's claim was solely for economic damages due to card losses and the costs of issuing new cards. Consequently, the court used the "economic loss" rule to dismiss the negligence claim but did not offer an opinion on whether negligence claims in data breach cases were in fact barred by the economic loss doctrine under Maine law.

Finally, the court also rejected an "equitable subrogation" claim, because Banknorth has no ability to "stand in the shoes" of its cardholders in making a claim against BJ's, because Banknorth's agreement with its customers gave them no liability for fraudulent transactions. Accordingly, because Banknorth covered these losses for its customers, the customers had not lost anything, and there was no claim for Banknorth to pursue against BJ's on the customers' behalf.

Sovereign Bank sued defendants, BJ's Wholesale Club, Inc., and Fifth Third Bank, after Sovereign incurred losses when its customers' Visa card numbers were stolen from a computer file maintained by BJ's. The losses were mainly for the cost of issuing new credit cards to replace the ones that had been compromised by the theft and for the cost of reimbursing those cardholders who had suffered unauthorized charges to their accounts. Sovereign sued BJ's for negligence, breach of fiduciary duty, and promissory estoppel, and against Fifth Third Bank for breach of contract and promissory estoppel. The court previously resolved the defendants' motions to dismiss the original complaint. *See Sovereign Bank v. BJ's Wholesale Club, Inc.,* 395 F. Supp. 2d 183 (M.D. Pa. 2005). But Sovereign filed an Amended Complaint. Furthermore, the court rejected the negligence claim based on the "economic loss" doctrine in the same manner discussed in *Banknorth.*

The plaintiff alleged that Fifth Third Bank promised to ensure that BJ's would comply with the Operating Regulations, a promise that Fifth Third should have reasonably expected the plaintiff to rely on. Relying on that promise, Sovereign provided BJ's with its customers' cardholder information, thinking Fifth Third would comply with the regulations by ensuring that BJ's would not store or retain the information. The plaintiff also alleged that Fifth Third failed to comply with its promise to abide by the Operating Regulations, failed to ensure that BJ's would not store and retain the cardholder information, and harmed Sovereign. The court dismissed the plaintiff's claim for promissory estoppel because the court did not believe that Sovereign's decision to provide BJ's with its cardholders' information was made in reliance on Fifth Third's promise to insure that BJ's would not store or retain the information.

In dismissing the promissory estoppel claim against BJ's, the court found that BJ's expressly excluded third-party beneficiaries from its merchant agreements with Fifth Third Bank. Additionally, the court reasoned that BJ's could not have reasonably expected that Sovereign, a third party to those agreements, would have relied on the promise BJ's made in the agreements to abide by the Operating Regulations, nor could Sovereign have reasonably relied on the promise in those agreements

With respect to the remaining claims against BJ's, the court dismissed the negligence and the breach of fiduciary duty claims. In dismissing the negligence claim, the court applied the economic loss doctrine. The court dismissed the breach of fiduciary claim because Sovereign had not turned over substantial control of its affairs to BJ's. Only cardholder information was disclosed, which did not rise to the level necessary to create a fiduciary relationship between Sovereign and BJ's.

In December of 2006, the TJX Companies, Inc. ("TJX"), which is the parent company to T.J. Maxx and Marshall's, suffered an unauthorized intrusion or intrusions into its computer systems that process and store customer transactions information, including the computer system that handled its credit card, debit card, check, and merchandise return transactions for most of its stores in the United States, Puerto Rico, and Canada. The breach resulted in an estimated 45 to 97 million credit card records being compromised.

In addition to being investigated by more than 30 state attorneys general and the United States Federal Trade Commission, TJX faced numerous class action lawsuits relating to the security breach.

See, e.g., In re TJX Companies Retail Security Breach Litigation, Consumer Track Actions, and Financial Institutions Track, Consolidated Class Action Complaints, Master Docket No. 07-10162-WGY (D. Mass.). In focusing on two of the class action lawsuits filed against TJX, one can see how that tactics of the plaintiffs have changed since *Banknorth* and *Sovereign*. In the first lawsuit to be addressed, the class action is brought by an individual who uses the widely acceptable industry standards to protect consumer financial data as a basis for the negligence claim. Additionally, this case shows that to date plaintiffs still have difficulty showing injury or loss merely because of a breach. In the second lawsuit, which was filed by a class of banking associations, the plaintiffs' claims of negligent misrepresentation and a violation of a state statute remained after the court dismissed the causes of action for negligence and breach of contract.

In *Mace v. TJX Companies, Inc.*, Docket No. 07-10162 WGY. (D. Mass 2007), the complaint alleged only that TJX was negligent in maintaining adequate security measures to protect consumer financial information. To support this cause of action, plaintiffs relied on three facts. First, the plaintiffs claimed that the length of time during which the intrusions into TJX's systems went undetected demonstrated that TJX's security measures were neither sufficient nor properly monitored. Second, TJX violated industry standards because it was keeping customer financial data for longer than it had a business purpose to do so. Finally, the plaintiffs also pointed to news reports that auditors had informed TJX that it was not following industry standards for the security of its wireless network, or other credit card industry regulations. The Payment Card Industry Data Security Standard ("PCI-DSS") was developed by the major credit card companies to help business that process card payments prevent credit card fraud, cracking, and various other security vulnerabilities and threats. *See* https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml. This standard is organized into 12 security requirements for protecting payment card information. A company processing, storing, or transmitting payment card data must be PCI-DSS compliant or risk losing their ability to process credit card payments and being audited and/or fined.

In order to prevail in this complaint, the plaintiff must prove:

- A duty of care owed by TJX to the consumer class of victims;
- TJX's computer security fell below the applicable standard of care that amounts to a breach of that duty;
- An injury or loss;
- Cause in fact; and
- Proximate, or legal, cause.

Although it would be clear that the data security standards that apply to retailers' protection of customer financial information would establish a duty of care that TJX owed to customers and the loss of consumer data would have been a breach of that duty, the complaint was not clear on how the plaintiffs would have demonstrated that the mere breach itself caused injury or loss for her or the other class members.

In *Massachusetts Banking Association, et al. v. TJX Companies, Inc.*, the complaint argued that TJX failed adequately to safeguard customers' personal financial information, failed to follow industry standards for data security, and failed to maintain adequate systems for detecting or preventing intrusions and were subject to liability for negligent misrepresentation, a violation of Massachusetts Unfair and Deceptive Practices under Massachusetts statutory law, negligence, and breach of contract. The unfair and deceptive trade practices cause of action is fairly straightforward, but each of the remaining causes of action are interesting and differ in the approaches of past data breach litigation.

With respect to its negligence cause of action, TJX, similar to Banknorth, tried to dismiss the cause of action by arguing that the negligence claim was barred by the economic loss doctrine. (In Massachusetts, "purely economic losses are unrecoverable in tort and strict liability actions in the absence of personal injury or property damage." *See Aldrich v. ADD Inc.,* 770 N.E.2d 447, 454 (Mass. 2002).) The Banking Associations argued that the economic loss doctrine did not apply to the facts of this particular case. In this case, according to the plaintiffs, the breach caused damage to property because the compromised cards could no longer be used and that card verification codes were lost. The court dismissed this claim and held that the alleged "physical" destruction of the credit cards, debit cards, and security codes should instead be considered economic losses.

In support of its negligent misrepresentation claim, the Banking Associations alleged that TJX represented that it participated in VISA and MasterCard's programs to protect consumer data and that such a representation implied a certain level of protection that a retailer will provide to consumer financial data. According to the complaint, the breach meant that TJX did not have security measures that were consistent with the VISA and MasterCard programs and TJX falsely implied compliance with those programs. Additionally, the plaintiffs alleged that TJX's use of the issuing bank's credit or debit cards was tantamount to a negligent misrepresentation. According to the Banking Associations, as part of the approval process of each card, TJX communicates with the issuing bank that it is part of the payment card system; that it has been presented with the issuing bank's payment card; that it wants to use that card to effect a transaction; and that it will effect the transaction as part of the necessary rules. The Banking Associations alleged that the security breach meant that TJX's communications with the issuing banks were false. The court did not dismiss this cause of action.

Finally, the Banking Associations argued that TJX breached their contract to its merchant bank, Fifth Third Bank, and that the Banking Associations were third-party beneficiaries entitled to recover from TJX. According to the complaint, the plaintiffs alleged that the merchant agreements between TJX and Fifth Third Bank incorporated the MasterCard and Visa Operating Regulations. However, the court dismissed the breach of contract claims because the Operating Regulations, which were incorporated into the contracts between Fifth Third and Visa and MasterCard, appeared to deny third parties the ability to bring suit against either TJX or Fifth Third Bank.

Although it is still difficult for plaintiffs to prevail on many claims against companies that have incurred a data breach, recent cases shed some light on causes of action that have survived a motion to dismiss. The above cases illustrate those claims and provide several lessons:

- First, individual consumers, or a class of individual consumers, still have difficulty showing that a breach, and nothing more, causes injury;
- Second, defendants in breach cases can use the economic loss doctrine to dismiss negligence claims. This doctrine was used successfully in *Sovereign* and by TJX to dismiss the Banking Associations claim of negligence;
- Third, it is extremely difficult for financial institutions to succeed on a breach of contract claim if the financial institution is alleging that it is a third-party beneficiary to the contract between the defendant company and the company's merchant bank;

- Fourth, the new class actions show the emergence and importance of the PCI-DSS and how those standards can be used to establish a standard of care in negligence claims. In the earlier cases, plaintiffs argued that companies had a fiduciary duty to protect and to preserve information. In the more recent cases, plaintiffs, both individual and business plaintiffs, have claimed that PCI-DSS is an industry standard for the protection of customer financial information that imposes a duty on all businesses that use credit or debit card numbers;
- Fifth, the payment card companies have heavily fined companies for incurring a breach when the company is not PCI-compliant. For example, as a result of the TJX data breach, VISA USA assessed Fifth Third Bank $880,000 in penalties for failing to maintain adequate computer security.

Ross Kerber, *Visa Fines Bank After Losses in TJX Breach,* Boston Globe (October 29, 2007), available at www.boston.com/business/globe/articles/2007/10/29visa_fines_bank_after_lossses_in_tjx_breach.

CONCLUSION • Data breaches are "actionable" by consumers—who vote with their feet. Ponemon's National Survey on Data Security Breach Notifications, which surveyed more than 1,000 people who had received notice of personal data security breaches, found that 20 percent had already terminated their relationships with companies that maintained their data. Another 40 percent said they might do so, and nearly five percent said they had hired lawyers to seek legal recourse after their data was put at risk. Clearly, market forces will have a significant say in whether American businesses employ better data security practices. The U.S. media and population, as well as the FTC and State Attorneys General, are on hyper-alert about all things related to privacy. Corporate management should take note, especially as it relates to employee and customer information.

PRACTICE CHECKLIST FOR
A New Frontier: Litigation Over Data Breaches

Although actions based on data security breaches have not yet met with wide success, there is little doubt that more breaches will occur, and more actions will be pursued. So it makes sense for the litigator to know how these matters are handled both by the FTC and as private actions.

- Claiming authority under the Federal Trade Commission Act, the Federal Trade Commission has brought several high-profile actions against organizations experiencing data breaches on the theory that lax data security practices constitute "unfair and deceptive trade practices." To pursue a cause of action successfully under the FTC's current unfairness standard, the Commission must establish that:

__ The respondent/defendant has engaged in an act or practice that caused, or is likely to cause, substantial injury to consumers;
__ The injury is not reasonably avoidable by consumers; and
__ The injury to consumers is not outweighed by countervailing benefits to consumers or to competition.

- Cases brought by the FTC include:

__ *In the Matter of BJ's Wholesale Club, Inc., United States Federal Trade Commission,* File No. 042 3160 (Sept. 23, 2005) available at www.ftc.gov/os/caselist/0423160/0423160.shtm;
__ *United States of America v. ChoicePoint Inc.,* United States District Court for the Northern District of Georgia, Civil Action No. 1:06-CV-0198 (Jan. 30, 2006), available at www.ftc.gov/os/caselist/choicepoint/choicepoint.shtm;
__ *In the Matter of DSW, Inc.,* United States Federal Trade Commission, File No. 052 3096 (March 14, 2006), available at www.ftc.gov/os/caselist/0523096/0523096.shtm;
__ *In the Matter of CardSystems Solutions, Inc., and Solidus Networks, Inc., d/b/a/ Pay By Touch Solutions,* United States Federal Trade Commission, File No. 052 3148 (Sept. 8, 2006), available at www.ftc.gov/os/caselist/0523148/0523148.shtm.

- The FTC has settled the cases it has brought against high-profile entities and no court has yet ruled on whether Section 5 gives the FTC authority to police industry security practices as "unfair."

- Four cases highlight the difficulty private litigants, individuals, and financial institutions face when suing a company for a data breach:

__ *Guin v. Brazos Higher Education Services,* 2006 U.S. Dist. LEXIS 4846 (D. Minn. Feb. 7, 2006), demonstrates the challenges that individuals, or a class of individuals, face in proving injury as a result of the data breach. (The court granted the defendant's summary judgment motion because of the plaintiff's failure to trace cognizable damages arising from the defendant's breach of the standard of care. The court found that the plaintiff failed to demonstrate a present and actual injury that resulted from the allegedly negligent security practices);
__ *Bell v. Acxiom Corporation,* 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006), shows how plaintiffs have attempted to argue that a data breach has increased the possibility that their personal data might be exploited by an identity thief. (The court held that anticipated injury or fear of a future crime is insufficient to meet the injury requirement);
__ In *Banknorth, N.A. v. BJ's Wholesale Club, Inc.,* 442 F. Supp. 2d 206 (M.D. Pa. 2006), the court rejected the tort and contract claims. (Regarding the negligence claim, the court reasoned that Banknorth's claim was solely for economic damages due to card losses and the costs of issuing new cards. Consequently, the court used the "economic loss" rule to dismiss the negligence claim but did not an opinion on whether negligence claims in data breach cases were in fact barred by the economic loss doctrine);
__ In *Sovereign Bank v. BJ's Wholesale Club, Inc.,* 427 F. Supp. 2d 526 (M.D. Pa. 2006), *aff'd in part, rev'd in part,* 533 F.3d 162 (3d Cir. 2008), the court dismissed the tort claims against BJ's and BJ's merchant bank. (The court rejected the negligence claim based on the "economic loss" doctrine in the same manner discussed in *Banknorth*).

- The December 2006 security breach affecting the TJX Companies, Inc. ("TJX") resulted in investigations by more than 30 state attorneys general and the United States Federal Trade Commission, as well as numerous class action lawsuits. To prevail in these cases, the plaintiffs would have to prove:

__ A duty of care owed by TJX to the consumer class of victims;
__ TJX's computer security fell below the applicable standard of care that amounts to a breach of that duty;
__ An injury or loss;
__ Cause in fact; and
__ Proximate, or legal, cause.