The Federal Trade Commission's Expansion of the

By Benita A. Kahn and Heather J. Enlow

Data breaches are receiving increasing exposure and media attention as the list of those affected, the amount of information compromised, and the costs to the compromised company rapidly increase. In January, TJX announced the largest data breach to date, with over 45 million credit cards compromised. Additionally, according to the Privacy Rights Clearinghouse, over 159 million records containing the sensitive personal information of U.S. residents have been involved in data breaches since January 2005. As this problem has continued to grow, the FTC has stepped in to "protect" consumers. This article explores the evolution of the FTC's use of its jurisdiction to address these data breaches and questions whether the FTC has expanded its jurisdiction beyond its authority under the FTC Act.

Data breaches exposing thousands and even millions of consumers' personal financial information collected by large U.S. retailers, agencies, and universities seem to grace the headlines daily.[1] You may have even received a letter in the mail stating that your credit card or debit card number and/or other personal information—such as your driver's license number—had been compromised. In January 2007, TJX Companies Inc. announced the largest data breach to date: a breach that involved more than 45 million credit cards and debit cards used at the company's stores.[2]

Many lawsuits have been filed against TJX as a result of this breach, and the Federal Trade Commission (FTC) has announced that it is investigating TJX as well.[3] This article will explore how the FTC has used its § 5 authority in the wake of several high-profile data breaches. First, this article will discuss § 5 authority generally and then look at the FTC's authority under the Gramm-Leach-Bliley Act (GLBA), its resulting Safeguards Rule, and the FTC's expansion of the Safeguards Rule in actions against nonfinancial institutions involved in data compromises. Finally, the article will compare the FTC consent orders entered into with the retailers in the data breach context to litigation involving those data breaches. The discussion will conclude by questioning whether the FTC has indeed met its requirements for jurisdiction in these types of cases.

FTC Jurisdiction

The FTC's ∫ 5 Authority

The Federal Trade Commission Act, 15 U.S.C. §§ 41, *et seq*. (2007), prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1) (2007). The FTC Act was initially enacted to prohibit unfair methods of competition in commerce and to supplement and bolster the Sherman and Clayton Acts.[4] The act was also intended to condemn existing violations of the Sherman and Clayton Acts as unfair methods of competition.[5] Since it was enacted, the FTC Act has been amended to outlaw unfair or deceptive acts or practices in commerce, so that the Federal Trade Commission can take steps to directly protect consumers, not just business competitors.[6]

The FTC is one of the primary federal regulators of retail merchants. Section 5 of the FTC Act invests the FTC with broad investigative powers to determine unfair and deceptive trade practices that affect consumers. The FTC is also empowered to initiate federal court actions in order to enforce violations of § 5 and to seek appropriate equitable relief. 15 U.S.C. § 53(a)-(b), 57(b) (2007). Under this general enforcement authority, the FTC can investigate and pursue actions against businesses whose activities qualify as practices that "cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n) (2007).

FTC Jurisdiction Under the Gramm-Leach-Bliley Act

Under the Gramm-Leach-Bliley Act, "financial institutions" have an affirmative and continuing obligation to address the privacy of their customers and to protect the security and confidentiality of those customers' nonpublic personal information. 15 U.S.C § 6801(a) (2007). With respect to the security requirements under GLBA, the act requires financial institutions to: (1) establish appropriate standards for administrative, technical, and physical safeguards that will ensure the security and confidentiality of customer information; (2) protect the security of these records against any anticipated threats; and (3) protect customers against unauthorized access or use of this information, which could result in substantial harm or inconvenience to customers. 15 U.S.C. § 6801(b) (2007).

The term "financial institutions" is broadly defined under GLBA and includes institutions that are significantly engaged in financial activities. Examples of financial institutions other than the obvious banks and savings and loan institutions include mortgage brokers, check cashing businesses, and car dealers that arrange for the financing or leasing of a personal car. 16 C.F.R. § 313.3(K)(2) (2007). Because of the breadth of the definition of financial institutions, many of the "financial institutions" covered by GLBA do not have a specified regulator such as the Office of the Comptroller of the Currency or the Federal Deposit Insurance Corporation. As a result, the FTC is granted specific jurisdiction to regulate these entities and is responsible for enforcing the safeguard provisions included in the act. As required by GLBA, the FTC implemented the Safeguards Rule to set forth the standards for the protection of customer records and information that are to be followed by the financial institutions that the FTC regulates.

The Safeguards Rule requires financial institutions to develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards that are appropriate to the institution's size and complexity, the nature and scope of activities, and the sensitivity of any customer information at issue. *See* 16 C.F.R. § 314 (2007). These requirements include the following:

- designating someone to coordinate the information security program;
- performing a risk assessment that considers personnel training, information systems, and the detection, prevention, and response to attacks, intrusions, and other systems failures;
- designing and implementing safeguards to control risks and regularly testing safeguards to monitor effectiveness;
- overseeing service providers by ensuring that they are able to take appropriate security precautions and in fact do so; and
- updating the security program as necessary in response to frequent monitoring and material changes in the business.

According to an FTC official, "An actual breach of security is not a prerequisite for enforcement under § 5; however, evidence of such a breach may indicate that the company's existing policies and procedures were not adequate."[7]

The Expansion of FTC Actions Against Nonfinancial Institutions

GLBA defines financial institution broadly, but the act generally does not cover retail merchants that do not issue their own credit. However, over the past several years the FTC has embarked on an aggressive strategy of investigations and has threatened enforcement actions against companies that had their customers' nonpublic personal information stolen through asserted data compromises. These investigations have resulted in companies not subject to GLBA to effectively agree to implement the Safeguards Rule and to submit to independent security audits for a set period of time—usually 20 years.

In early enforcement actions against these nonfinancial institutions, the FTC relied on the deception aspect of § 5 of the FTC Act. The FTC asserted that the privacy statements of companies contained false and misleading information in light of subsequent security breaches. One such case was that of Petco Animal Supplies Inc. Petco's online privacy policy stated that Petco encrypted consumers' personal information both in transit and in storage. After the online theft of customers' credit card information, however, it was determined that Petco did not encrypt customers' credit card information when stored.

Petco settled the FTC's charges that a security flaw in its Web site allowed hackers to access consumer records,

including credit card numbers. The FTC alleged that had Petco actually encrypted the data as promised, the credit card information would not have been accessed. The FTC stated that the false promises Petco had made to consumers were deceptive and therefore violated § 5 of the FTC Act. As part of the settlement, Petco agreed to establish and maintain a comprehensive security program that mirrors the requirements of the Safeguards Rule. The settlement also required biennial audits of the company's security program by an independent third party for the next 20 years, and required Petco to maintain records so that the FTC may monitor compliance.[8]

Subsequent data compromises occurred in stores, rather than on Web sites, and the FTC could not rely on deceptive privacy policies as a basis for enforcement actions. Therefore, the FTC turned to the FTC Act's unfairness doctrine to pursue enforcement. Unfairness under the FTC Act has three specific elements: (1) the violation causes substantial injury to consumers; (2) consumers are unable to reasonably avoid the injury; and (3) the substantial injury is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n) (2007). By using the unfairness doctrine, the FTC has expanded the reach of the Safeguards Rule beyond financial institutions, extending it to nonfinancial institutions that experience security breaches, by asserting that these entities did not have reasonable information security policies and procedures in place. The question that is raised, however, is whether the FTC can meet all these standards in a case that is litigated.

The first instance of the FTC's expansion of the Safeguards Rule occurred in the consent order entered into with BJ's Wholesale Club. Between July 2003 and February 2004, unauthorized persons accessed BJ's computer systems as well as the credit card and debit card numbers of thousands of customers. Visa discovered this security breach and notified BJ's and the banks within the Visa network. In the investigation and enforcement action against BJ's, the FTC pursued the broader strategy of alleging that the failure to ensure adequate security measures constituted an unfair practice. The commission did not claim that BJ's had made misrepresentations to its customers, as the FTC did in the Petco action. Rather, the FTC alleged that the failure of BJ's to provide adequate security measures constituted an unfair practice that violated federal law. The unreasonable security measures asserted by the FTC included the following actions by BJ's:

- failure to encrypt personal data while in transit or when stored on the computer networks of their stores;
- creation of unnecessary risks by storing information longer than necessary in violation of bank rules;
- storage of personal data in easily accessible files;
- failure to take adequate steps to prevent unauthorized wireless connections; and
- failure to take reasonable measures to detect unauthorized network access and failure to conduct security audits.

In the consent order, BJ's essentially agreed to implement the requirements of the FTC's Safeguards Rule and to perform biennial security audits for the next 20 years.[9]

Relying on the unfairness doctrine, these same Safeguards Rule standards and audit requirements have been imposed in a subsequent settlement by a merchant with the FTC stemming from the theft of credit card information.[10] These merchant settlements have resulted in the expansion by the FTC of the Safeguards Rule beyond the financial institutions the FTC regulates under GLBA to nonfinancial institutions such as retail merchants. The standard has required the retail merchants to implement a comprehensive information security program and biennial audits by an independent third-party security professional for 20 years. However, financial institutions that have violated GLBA receive lesser terms.[11] Because these FTC investigations resulted in settlements rather than litigated enforcement, no court has made a determination of whether the FTC can meet all the requirements of the unfairness standard when a retail merchant is involved in a data compromise of customer information. The decisions in ongoing civil litigation against these merchants, however, may shed some light on the FTC's ability to meet all the elements of the unfairness doctrine.

Data Breach Litigation

To date, courts have rarely adjudicated favorably the claims of plaintiffs whose nonpublic personal information has been lost or stolen. In fact, in the data breach context, courts have frequently held that plaintiffs have not suffered injuries-in-fact, reasoning that an increased risk of identity theft is insufficient to support the injury-in-fact requirement of Article III standing.[12] Moreover, this alleged injury of an increased risk of future harm has been judged insufficient to support the damages requirements of tort actions and contract claims.[13] Courts have noted the danger in awarding damages to buy "peace of mind" as well as the possibility that plaintiffs could conceivably be awarded damages not only in the present for a perceived increased risk of harm but also in the future, if and when actual harm occurs.[14]

Specifically, in cases against merchants, the courts have ruled against the plaintiffs for lack of injury. In *Key v. DSW Inc.*, the plaintiff alleged that because of DSW's data breach, she had been subjected to a substantially increased risk of identity theft or other financial crimes. In dismissing all claims, the court held that the plaintiff lacked Article III standing. "To satisfy the case or controversy requirement a plaintiff must establish three elements: '(1) an injury-in-fact that is concrete and particularized; (2) a connection between the injury and the conduct at issue—the injury must be fairly traceable to the defendant's action; and (3) likelihood that the injury would be redressed by a favorable decision by the Court.'"[15] Under this standard, a plaintiff's injury must be "actual or imminent," and not "conjectural or hypothetical."[16]

The court held that a substantial increased risk of identity theft or other related financial crimes was insufficient to confer standing to sue. Reasoning that, in the identity theft context, courts have held an alleged increase in risk of future injury is not an actual or imminent injury, the court

held the plaintiff's injury was not actual or imminent.

> At the present time, Plaintiff has not alleged evidence that a third party intends to make unauthorized use of her financial information or of her identity. The mere inquiry as to who would cause harm to Plaintiff, when it would occur, and how much illustrated the indefinite, and speculative nature of Plaintiff's alleged injury. In sum, Plaintiff's claims are based on nothing more than a speculation that she will be a victim of wrongdoing at some unidentified point in the indefinite future. Because Plaintiff has failed to allege that she suffered injury-in-fact that was either 'actual or imminent,' this Court is precluded from finding that she has standing under Article III.[17]

Even when there is evidence of fraudulent use of an individual's credit cards and debit cards, that individual is not held responsible for those purchases under many banks' Zero Liability Policies.[18] Courts, therefore, have been reluctant to state that fraudulent use of a credit or debit card constitutes an injury when there was no actual injury. Plaintiffs have also run into causation problems. For example, in *Stollenwerk v. Tri-West Healthcare Alliance*, No. Civ. 03-0185PHXSRB, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005), one plaintiff's identity was actually stolen, costing that person thousands of dollars. However, the plaintiff could not prove that the defendant's data breach was the proximate cause of his identity theft, and the court granted judgment to defendant. Thus, courts have been reluctant to rule favorably for plaintiffs in the data breach context, because they are unable to identify cognizable damages.[19]

Conclusion

In conducting its investigations of data breaches, the FTC has claimed a violation of the unfairness doctrine. In the consent orders imposed on retailers involved in data compromises, the FTC stated that it had jurisdiction, because the "failure to secure customers' sensitive information was an unfair practice because it caused substantial injury that was not reasonably avoidable by consumers and not outweighed by offsetting benefits to consumers or competition."[20]

It is interesting that, given the same set of facts, courts have failed to recognize asserted claims or the existence of injuries to allow banks or consumers to recover against an entity that has suffered a data breach. The courts found that an alleged increase in risk of future injury is not an actual or imminent injury—much less a substantial injury. Along with court rulings, the implementation of the Zero Liability Policy issued by credit card associations to protect consumers against all liability resulting from fraudulent transactions on their credit or debit cards addresses the issue of consumers' ability to reasonably avoid any potential injury when credit card information is compromised. Moreover, findings in a report released by the Government Accountability Office in June 2007 raise further questions as to whether the unfairness test can be met.[21] The report stated that research through interviews and data "indicated that most breaches have not resulted in detected incidents of identity theft" and that there is great difficulty in determining the source of the data used to commit identity theft.[22]

If the anticipation or perceived risk of future harm is insufficient to meet the requirements of injury-in-fact for standing, can this same perceived risk from a data compromise of credit card information, for which consumers can avoid injury through reporting, be sufficient to meet the requirements of the unfairness doctrine? One must wonder if § 5 of the FTC Act was meant to be used in this way. **TFL**

Benita A. Kahn, a partner with Vorys, Sater, Seymour and Pease LLP in its Columbus, Ohio, office, specializes in privacy, data security, and consumer protection laws and represents numerous national retail clients. Heather J. Enlow, an associate with Vorys, Sater, Seymour and Pease LLP in the same office, provided significant assistance in preparing this article.

Endnotes

[1]For a complete list of security breaches since 2005, see Privacy Rights Clearinghouse, *Chronology of Data Breaches*, April 22, 2007, available at www.privacyrights.org/ar/ChronDataBreaches.htm.

[2]*See TJX Companies Inc.*, 10-K, March 28, 2007, available at ir.10kwizard.com/files.php?source=487.

[3]As of March 2007, 16 lawsuits have been filed against TJX as a result of the data breach announced in January. *See id.* More recent reports indicate that to date 19 lawsuits have been filed.

[4]*See generally FTC v. Beech-Nut Packing Co.*, 257 U.S. 441 (1992); *Luria Bros. & Co. v. FTC*, 389 F.2d 847 (3d Cir. 1968).

[5]*See generally FTC v. Brown Shoe Co.*, 384 U.S. 316 (1966).

[6]*See FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233 (1972); *FTC v. A.P.W. Paper Co.*, 328 U.S. 193 (1946). In spite of this broad jurisdiction to protect consumers, the FTC Act excludes some industries from its jurisdiction, such as banks, savings and loan institutions, common carriers, air carriers, and others. 15 U.S.C. § 45(a)(1) (2007).

[7]Deborah Platt Majoras, FTC chair, "Data Breaches and Identity Theft," Testimony before the Senate Committee on Commerce, Science, and Transportation, 109th Cong. 6 (June 16, 2005), available at commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Testimony&Hearing_ID=1536&Witness_ID=3484.

[8]FTC, Press Release, "Petco Settles FTC Charges: Security Flaws Allowed Hackers to Access Consumers' Credit Card Information" (Nov. 17, 2004), available at www.ftc.gov/opa/2004/11/petco.htm.

[9]FTC, Press Release, "BJ's Wholesale Club Settles FTC Charges: Agency Says Lax Security Compromised Thousands of Credit and Debit Cards" (June 16, 2005), available at www.ftc.gov/opa/2005/06/bjswholesale.shtm.

[10]FTC, Press Release, "DSW Inc. Settles FTC Charges: Agency Says Company Failed to Protect Sensitive Customer Data" (Dec. 1, 2005), available at www.ftc.gov/

opa/2005/12/dsw.shtm.

[11]*See In the Matter of Nationwide Mortgage Group Inc. and John D. Eubank*, File No. 042-3104, Agreement Containing Consent Order (March 4, 2005), available at www.ftc.gov/os/adjpro/d9319/index.shtm; *see also In the Matter of Sunbelt Lending Services Inc.*, File No. 042-3153, Agreement Containing Consent Order (Nov. 16, 2004), available at www.ftc.gov/os/caselist/0423153/04231513.shtm. Both Nationwide Mortgage Group and Sunbelt Lending Services were required to implement biennial auditing for only 10 years.

[12]*See Randolph v. ING Life Ins. and Annuity*, No. 06-1228 (CKK), 2007 WL 565872 (D. D.C. Feb. 20, 2007) (plaintiffs failed to allege a cognizable injury-in-fact where the laptop computer of the defendant was stolen containing plaintiffs' personal information but there was no evidence the information had been accessed or improperly used); *Bell v. Acxiom Corp.*, No. 4:06CV00485-WRW, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006) (plaintiff lacked standing because she failed to allege she had suffered concrete damages where defendant's computer files were improperly accessed; assertions of potential future injury do not satisfy injury-in-fact requirement); *Key v. DSW Inc.*, 454 F. Supp. 2d 684 (S.D. Ohio 2006) (plaintiff lacked standing because her alleged increase in risk of future harm was insufficient to show injury-in-fact where defendants' computer systems had been improperly accessed; court also found future risk was insufficient for cognizable damages for contract, negligence, conversion, and fiduciary duty claims); *Giordano v. Wachovia Securities LLC*, No. 06-476, 2006 WL 2177036 (D. N.J. July 31, 2006) (defendant lost a backup tape containing the plaintiff's personal information but the court concluded that the mere possibility of future harm fails to satisfy the standard of concrete and particularized harm).

[13]*See Kahle v. Litton Loan Servicing LP*, 486 F. Supp. 2d 705 (S.D. Ohio 2007) (plaintiff's choice to purchase credit monitoring services and an alleged increased risk of future harm was insufficient to support the damages element of her negligence claim where there was no evidence her information was accessed or used for identity fraud); *Hendricks v. DSW Shoe Warehouse Inc.*, 444 F. Supp. 2d 775 (W.D. Mich. 2006) (plaintiff failed to allege cognizable damages where she did not allege her personal information had been used or her credit damaged); *Forbes v. Wells Fargo Bank*, 420 F. Supp. 2d 1018 (N.A.D. Minn. 2006) (plaintiff's perceived risk of future harm was insufficient to satisfy the damages requirements where computers containing unencrypted personal information were stolen from the defendant's service provider); *Guin v. Brazos Higher Educ. Serv. Corp. Inc.*, No. Civ. 05-668 RHK/JSM, 2006 WL 288483 (D. Minn. Feb. 7, 2006) (plaintiff could not establish he suffered any injury to support his negligence claim against the defendant where a laptop computer belonging to the defendant was stolen from an employee's home).

[14]*Hendricks*, 444 F. Supp. 2d at 779–780.

[15]*Key*, 454 F. Supp. 2d at 686-687 (citing *Courtney v. Smith*, 297 F.3d 455, 459 (6th Cir. 2002)); *see Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992); *Allen v. Wright*, 468 U.S. 737, 751 (1984).

[16]*Key*, 454 F. Supp. 2d at 687 (quoting *Lujan*, 504 U.S. at 560).

[17]*Id.* at 690.

[18]*See, e.g., Banknorth v. BJ's Wholesale Club Inc.*, 442 F. Supp. 2d 206 (M.D. Pa. 2006) (noting that the plaintiff bank's equitable subrogation claim failed because, under its Zero Liability Policy, the customer is not held liable for fraudulent purchases).

[19]Note that, in the rare cases in which the courts have ruled in favor of plaintiffs, the plaintiffs had suffered actual financial harm and were able to prove who stole their identities. *See Bell v. Michigan Council 25 of the American Federation of State, County, and Municipal Employees, AFL-CIO, Local 1023*, No. 246684, 2005 WL 356306 (Mich. App. Feb. 15, 2005) (where the daughter of the union's treasurer had stolen the identities of several members, and the court upheld the jury award against the union, finding that the union had a duty to safeguard its members' nonpublic personal information); *Daly v. Metropolitan Life Ins. Co.*, 4 Misc.3d 887 (N.Y. 2004) (where two employees of the defendant had accessed the plaintiff's nonpublic personal information and used the information to establish and use numerous credit accounts; the court held that the defendant had a duty to protect the plaintiff's nonpublic personal information); *see also Jones v. Commerce Bankcorp. Inc.*, No. 05-5600 (D. N.J. July 16, 2007) (court certified settlement class and approved settlement where five employees stole customer information and sold it to a criminal; police had arrested the employees and the criminal, finding the confidential banking information of numerous Commerce customers in their possession).

[20]FTC, Press Release, "DSW Inc. Settles FTC Charges"; *see also* FTC, Press Release, "BJ's Wholesale Club Settles FTC Charges."

[21]U.S. Government Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, GAO-07-737 (June 4, 2007), available at www.gao.gov/docsearch/abstract.php?rptno=GAO-07-737.

[22]*Id.* at 5.