Reasonable Security: The FTC's Focus on Personal Privacy Initiatives Highlights the Importance of Integrated Information Security Programs

RONALD D. LEE AND AMY RALPH MUDGE

The Federal Trade Commission has declared that it considers privacy to be a "central element" of its consumer protection mission. As technological advances have made it possible for detailed personal information to be compiled and shared more easily, the FTC has escalated its efforts to ensure that such information is protected adequately. This article discusses recent cases which demonstrate the FTC's commitment to achieving its objective.

In March 2006, the Federal Trade Commission (FTC or the Commission) gave final approval to the consent order in its investigation of DSW Inc., an Ohio-based national retailer of shoes, settling FTC charges that DSW failed to take reasonable measures to safeguard sensitive consumer data.[1] This case comes on the heels of a similar security breach investigation, *BJ's Wholesale*,[2] settled last summer. On the

Ronald D. Lee is a partner in Arnold & Porter LLP's Washington, D.C. office and heads the firm's Information Security, Computer Crime and Electronic Surveillance practice. Amy Mudge is a senior associate in the Antitrust and Trade Regulation practice group also practicing in the firm's Washington, D.C. office. Mr. Lee and Ms. Mudge can be contacted at ronald.lee@aporter.com and amy.mudge@aporter.com, respectively. The authors wish to thank their colleague Nancy Perkins and former colleagues Matthew Meisner and Nadine Jones for their contributions to this article.

This article appeared in Vol. 1, No. 7, of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006,

same day the BJ's Wholesale consent was announced, FTC Chairperson Deborah Platt Majoras testified before the Senate Commerce Committee on the topic of data breaches and identity theft. In her testimony, Chairperson Majoras stated the FTC's view that Section 5 of the FTC Act requires all companies "holding sensitive data to have in place procedures to secure it if its failure to do so is likely to cause substantial consumer injury."[3] Chairperson Majoras also urged Congress to consider legislation effectively extending the Commission's Safeguards Rule (which currently requires only "financial institutions" to implement safeguards to protect customer information) to all companies with access to sensitive customer data. There has been some legislative movement in recent months, including recent bills approved by congressional committees. The *DSW* and *BJ's Wholesale* cases confirm that the FTC will take enforcement action for security breaches involving consumers' personal information even when a company has not failed to comply with its own privacy policies. They also reinforce FTC statements that "privacy and information security continues to be a top priority in the FTC's consumer protection program."[4] In a comment on its *DSW* decision, moreover, the FTC has made clear that it may use its enforcement discretion to go beyond the substantive requirements of the Safeguards Rule and protect personal information of consumers even in cases where the information is public.[5] Thus, it is important for all companies, not just financial institutions, that collect or have access to customer data-whether or not it would always be considered confidential-to evaluate whether they have adequate information security programs in place. Finally, even those companies whose business models do not involve any collection or use of customer information should study the FTC's position as potentially indicative of the emerging standards for reasonable information security that Boards of Directors, regulators, potential plaintiffs, and the public may seek to impose on such companies.

BACKGROUND ON FTC PRIVACY INITIATIVES

The FTC has declared repeatedly that it considers privacy to be a "central element" of its consumer protection mission. As technological

advances have made it possible for detailed personal information to be compiled and shared more easily, the FTC has escalated its efforts to ensure that such information is protected adequately. Relying on its authority under Section 5 of the FTC Act,[6] the Commission has brought several cases to enforce the promises in privacy statements, including promises by firms about how they will collect, use, and secure consumers' personal information. Before the *BJ's Wholesale Club* and *DSW* cases, the Commission pursued its privacy enforcement efforts under Section 5 of the FTC Act exclusively under the "deceptive acts or practices" prong. Since 2002, the FTC has brought six such cases against companies that made allegedly deceptive claims about information security in their privacy statements.[7] These cases "alleged that the companies made explicit or implicit promises to take reasonable steps to protect sensitive consumer information but because they allegedly failed to take such steps, their claims were deceptive."[8]

In addition to enforcing the FTC Act, the FTC also enforces the financial privacy provisions of the Gramm-Leach-Bliley Act (GLB Act), which applies only to personal confidential financial information held by "financial institutions." (Financial institutions include those engaged in banking, lending, and insurance activities as well as loan brokering, credit reporting, and real estate settlement services.) To implement the GLB Act, the FTC has issued the Financial Privacy Rule,[9] which governs the collection and disclosure of customers' personal financial information by financial institutions. It has also issued the GLB Safeguards Rule,[10] which requires financial institutions under the FTC's jurisdiction to develop and implement appropriate physical, technical, and procedural safeguards to protect the security and integrity of their customer information.[11] The FTC also relies on the Fair Credit Reporting Act (FCRA) (which prohibits the distribution of consumer reports by consumer reporting agencies except for specified permissible purposes) to protect consumer privacy and settled a recent case with the largest ever civil penalty in a consumer protection case, $10 million (plus another $5 million for consumer redress), in part for inadequate security measures to protect sensitive consumer data.[12]

THE *BJ'S WHOLESALE* CASE

On June 16, 2005, the FTC announced that BJ's agreed to settle FTC charges "that its failure to take appropriate security measures to protect sensitive information of thousands of its customers was an unfair practice that violated federal law." The BJ's case is the first privacy enforcement action brought by the FTC pursuant to the "unfair practices" prong of the FTC Act. Unlike prior cases brought under the FTC's "deception" authority, which focus on misrepresentations, the FTC used its broader "unfairness" authority to prohibit practices that cause (or are likely to cause) substantial injury to consumers that they cannot reasonably avoid and where such harm is not offset by countervailing benefits to consumers or competition.

BJ's operates approximately 150 "Wholesale clubs" that sell a wide variety of products to its member-customers, who typically use credit cards or debit cards to make such purchases. Hackers were able to access more than 40,000 customer names along with associated credit or debit card information and other personal data that had been stored on BJ's computer system following the authorization of credit and debit card transactions. As a result of this security breach, several million dollars in fraudulent purchases were made using counterfeit copies of credit and debit cards members had used at BJ's stores.

The Commission alleged that BJ's "did not employ reasonable and appropriate measures to secure personal information collected at its stores."[13] In particular, the Commission found that BJ's "(1) did not encrypt the information while in transit or when stored on the in-store computer networks; (2) stored the information in files that could be accessed anonymously—that is, using a commonly known default user id and password; (3) did not use readily available security measures to limit access to its computer networks through wireless access points on the networks; (4) failed to employ sufficient measures to detect unauthorized access or conduct security investigations; and (5) created unnecessary risks to the information by storing it for up to 30 days when it no longer had a business need to keep the information, in violation of bank rules."[14] The FTC alleged that this failure was an "unfair practice" because it

This article appeared in Vol. 1, No. 7, of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006,

caused or was likely to cause substantial injury that was not reasonably avoidable and was not outweighed by countervailing benefits to consumers or competition.

The consent agreement has a term of at least 20 years and requires BJ's to "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."[15] The program must be fully documented in writing and must "contain administrative, technical, and physical safeguards appropriate to [BJ's] size and complexity, the nature and scope of [BJ's] activities, and the sensitivity of the personal information collected from or about consumers."[16]

The consent agreement further requires BJ's to obtain audits every other year for 20 years by a "qualified, objective, independent third-party professional" that "(A) set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period; (B) explain how such safeguards are appropriate to BJ's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers; (C) explain how the safeguards that have been implemented meet or exceed the protections required by the Order; and (D) certify that BJ's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected."[17]

In the press release accompanying this settlement, FTC Chairperson Majoras stated that "[c]onsumers must have the confidence that companies that possess their confidential information will handle it with due care and appropriately provide for its security. This case demonstrates our intention to challenge companies that fail to protect adequately consumers' sensitive information."

RECENT FTC TESTIMONY AND CONGRESSIONAL ACTIVITY ON PRIVACY ISSUES

On the same day the BJ's settlement was announced (June 16, 2005),

Chairperson Majoras testified before the Senate Committee on Commerce, Science and Transportation on the topic of data breaches and identity theft. Chairperson Majoras noted the FTC's "broad jurisdiction" under Section 5 to challenge deceptive practices relating to privacy and referenced the five cases recently brought against companies for deceptive security claims. While she did not mention the BJ's case, Chairperson Majoras made clear that the FTC "believe[s] that Section 5 already requires companies holding sensitive data to have in place procedures to secure it if the failure to do so is likely to cause substantial consumer injury . . ."[18] Chairperson Majoras also stated that "an actual breach of security is not a prerequisite for enforcement under Section 5; however evidence of such a breach may indicate that the company's existing policies and procedures were not adequate."[19]

Significantly, Chairperson Majoras (on behalf of the FTC) recommended that Congress consider new legislation, in addition to the FTC's existing authority under Section 5, that would require companies "that hold sensitive consumer data" to "take reasonable measures to ensure its safety."[20] According to Chairperson Majoras, "[s]uch a requirement could extend the FTC's existing GLBA Safeguards Rule to companies that are not financial institutions."[21] The Commission further recommended that "Congress consider requiring companies to notify consumers when the security of this information has been breached in a manner that creates a significant risk of identity theft."[22]

Congress has taken Chairperson Majoras up on the Commission's suggestions, but progress has been slow due to a heavy legislative agenda and competing proposals. In March 2006, two House Committees-the Energy and Commerce Committee and the Financial Services Committee-each passed separate bills on the issue, with considerable overlap but notable distinctions. The Energy and Commerce Committee bill, the "Data Accountability and Trust Act" (H.R. 4127), would require companies to implement data security programs and notify consumers when their personal information has been compromised in a security breach and there is a "reasonable" risk of identity theft or fraud. The House Financial Services Committee bill, the "Financial Data Protection Act" (H.R. 3997), would require such notice in cases where the breach would cause "harm

or inconvenience." The precise trigger for such notifications is a major point of contention among interested parties, as are the bills' provisions for preemption of state law and mechanisms for enforcement. Both of the two reported House bills would preempt state law and give enforcement authority to the FTC, but the Energy and Commerce Committee bill would also permit state attorneys general to bring enforcement actions. In the Senate, two Committees also have passed similar bills: the Commerce, Science and Transportation Committee passed the "Identity Theft Protection Act" (S. 1408) in July 2005, and the Judiciary Committee approved the "Personal Data Privacy and Security Act" (S. 1789) in November 2005. The Senate Banking Committee also has a strong interest in the issue, and reaching a compromise acceptable to both Houses may prove difficult. While the lawmakers continue to consider these bills, the FTC continues its aggressive enforcement efforts.

THE *DSW* CASE

In March and April of 2005, DSW notified the public that security breaches had occurred in 108 store locations.[23] The security breaches compromised over 1.4 million credit and debit cards and exposed over 96,000 checking account and driver's license numbers. Upon investigation, the FTC alleged that DSW had failed to protect this information reasonably by: (1) not limiting access to its computer network; (2) not encrypting the data stored; and (3) failing to employ reasonable measures to detect unauthorized access.[24]

To settle the matter, the FTC required DSW to implement the same security measures to protect personal information of its customers as the FTC required in *BJ's Wholesale:*[25]

- Designate an employee to coordinate and be accountable for the information security program;
- Identify material internal and external risks to security, confidentiality, and the integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information;
- Design and implement reasonable safeguards to control the risks

identified through risk assessment; and

- Evaluate and adjust its information security program in light of the results of the required testing and monitoring.[26]

FTC APPROACH IN PROTECTING PERSONAL CONSUMER INFORMATION[27]

DSW confirms that the FTC's approach in *BJ's Wholesale* was not an anomaly. The FTC has instituted enforcement proceedings against security practices and vulnerabilities relating to personal consumer information collected both online and at the point of sale.[28] As noted, in some cases, the FTC has challenged information security practices by alleging that the company made false and misleading statements about its information security. In more recent instances, such as *DSW* and *BJ's Wholesale*, the FTC has challenged the company's information security practices as a direct violation of Section 5.[29]

Based on its recent actions, it appears that the Commission will consistently take the position that Section 5's prohibition of unfair acts or practices requires all companies to provide reasonable security for consumer information. Although the FTC's unfairness standard requires a showing of substantial consumer harm (that is not outweighed by benefits to consumers or to competition), as a practical matter, it is not likely to be difficult for the FTC to show substantial harm from the disclosure of personal information. It would also likely be very challenging for a firm to show that security measures that proved inadequate nonetheless had substantial consumer benefit. The FTC likely will continue investigating and bringing enforcement actions under Section 5 and will be involved actively in the continued congressional consideration of legislation that would extend the GLB Safeguards Rule to all companies that collect or have access to sensitive customer data.[30]

One other aspect of the DSW consent order deserves special note. In responding to a comment to the DSW proposed order, the FTC made clear that its use of the term "personal information" was not meant to be read as limited to confidential information. Instead, the consent order's

requirements apply to information collected about customers that may be available through public sources but that can be used to perpetrate identity theft, such as name, address, and phone number. As such, use of the term "personal information" in the order was not meant to track the definition of "customer information" used in the Gramm-Leach-Bliley Act applicable to financial institutions. The FTC explained that "the inclusion of publicly available information within the ambit of this particular consent order is warranted as fencing-in relief. Fencing-in remedies are designed to prevent future unlawful conduct. Such provisions are often broader in scope than the conduct that is declared unlawful in a particular case."[31] Looking forward, even where information is public (e.g., names and addresses), if the disclosure can be said to facilitate identity theft, fraud, or other adverse consumer effects, the FTC likely would demonstrate substantial harm.

IMPLEMENTATION OF THE LEGAL STANDARD OF REASONABLE SECURITY

A company must take reasonable steps to safeguard any consumer data it collects during the normal course of business. Because each business is unique, companies must tailor their security programs to the individual characteristics of their businesses and the information that those businesses collect. The more sensitive the data and the greater the risk of harm to customers if the information is disclosed, the more stringent the security procedures need to be. Stated differently, mechanical mitigation of the specific vulnerabilities or poor practices cited in prior FTC actions is inadequate. Businesses can be guided, however, by the core objectives announced in past FTC cases as well as by other materials published by the agency for purposes of helping businesses to develop reasonable information security programs.

Moreover, the FTC's approach and standards are relevant even for businesses that do not regard themselves as consumer-facing businesses. First, some companies, even if they are not retailers or purveyors of consumer goods, regularly or incidentally collect, process, and use consumer information for marketing, research, and other purposes. In addition, even

This article appeared in Vol. 1, No. 7, of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006,

those companies that never collect or access consumer information do collect and store similar information for employees, contractors, and consultants, as well as other sensitive information. Like all other companies, these companies are increasingly under scrutiny by their Boards of Directors, employees, regulators, potential plaintiffs, the media, and the public who expect or demand that these companies provide reasonable protection for this information. Because the FTC's approach to and standards for information security are themselves based upon widely-accepted information security practices, and because the FTC's adoption of this approach and these requirements infuses them with additional weight and authority, even companies that believe they are not directly subject to FTC enforcement actions would be wise to establish and maintain information security programs that are consistent with FTC requirements.

In responding to another comment related to the DSW proposed order, the FTC clarified that a failure to encrypt personal information of consumers does not in and of itself establish that a company lacked reasonable procedures to safeguard that personal information. The FTC will review security procedures overall to determine whether they were reasonable under the circumstances.[32]

CONCLUSION

In short, the FTC requires that companies with personal information of consumers:

- conduct a risk analysis,
- develop a program to address any identified risks,
- designate a person or group to be responsible for the security program,
- include compliance and monitoring procedures to ensure the program's effectiveness, and
- update the program and security measures as needed.[33]

The FTC is likely to continue to use its enforcement authorities to promote the use of reasonable information security measures to protect customer information, and FTC actions will themselves contribute to the

emerging law of information security.

FTC REQUIREMENTS CHECKLIST

- ✔ Conduct a risk analysis.
- ✔ Develop a program to address any identified risks.
- ✔ Designate a person or group to be responsible for the security program.
- ✔ Include compliance and monitoring procedures to ensure the program's effectiveness.
- ✔ Update the program and security measures as needed.

NOTES

1 *In the Matter of DSW Inc.,* File No. 052-3096 Complaint at 2-3, *available at* http://www.ftc.gov/os/caselist/0523096/051201comp0523096.pdf.

2 *In the Matter of BJ's Wholesale Club, Inc.*, File No. 042-3160 (June 2005), *available at* http://www.ftc.gov/opa/2005/06/bjswholesale.htm.

3 Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science and Transportation, U.S. Senate, on Data Breaches and Identity Theft, June 16, 2005 (FTC Testimony), at 9-10, *available at* http://www.consumer.gov/idtheft/pd6/ftc_06.16.05.pdf. More recently Chairperson Majoras summarized the FTC's enforcement efforts of the past year saying, "The ultimate goal here is not to rack up more settlements and fines. . . . Rather, the goal here is to create a culture of security for sensitive information so that businesses prevent breaches and identity theft. . . . Just as we know that businesses keep their cash safe, we must insist that they keep consumers' sensitive information safe." Remarks of Deborah Platt Majoras, at 6 (Feb. 23, 2006) *available at* http://www.ftc.gov/speeches/majoras/060223californiaidtheft.pdf.

This article appeared in Vol. 1, No. 7, of The PRIVACY & DATA SECURITY LAW JOURNAL, published monthly by Sheshunoff Information Services, Inc., 1725 K St., NW., Suite 700, Washington, D.C. 20006,

4 Remarks of Lydia Parnes, FTC Director Bureau of Consumer Protection, at 2 (Oct. 28, 2004), *available at* http://www.ftc.gov/speeches/parnes/041028conprivparnes.pdf; *see also* Remarks of Howard Beales, former Director Bureau of Consumer Protection FTC (Dec. 1, 2005) (stating that consumer concerns about the security of private information were the FTC's "first priority"), *available at* http://www.ftc.gov/speeches/other/bealesconsumprotectagenda.htm; Remarks of Pamela Jones Harbour, Commissioner, at 4 (Mar. 10, 2006) ("Commission recently launched its new Division of Privacy and Identity Protection in the Bureau of Consumer Protection, in order to more fully dedicate critical resources to this important area.") *available at* http://www.ftc.gov/speeches/harbour/6309iapp.pdf (Harbour Speech).

5 Letter to Bank of America Corporation in *In the Matter of DSW Inc.*, File No. 052-3096 FTC (Mar. 7, 2005) *available at* http://www.ftc.gov/os/caselist/0523096/0523096DSWLettertoCommenterBankofAmerica.pdf.

6 Section 5(a) provides that "unfair or deceptive acts or practices in or affecting commerce are declared unlawful." 15 U.S.C. § 45(a)(1). "Unfair" practices are defined to mean those that "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n).

7 *Nations Title Agency, Inc. et al.,* (FTC File No. 052 3117) (May 10, 2006); *Petco Animal Supplies, Inc*. (FTC Docket No. C-4133) (Mar. 4, 2005); *MTS Inc., d/b/a Tower Records/Books/Video* (FTC Docket No. C-4110) (May 28, 2004); *Guess?, Inc.* (FTC Docket No. C-4091) (July 30, 2003); *Microsoft Corp.* (FTC Docket No. C-4069) (Dec. 20, 2002); *Eli Lilly & Co.* (FTC Docket No. C-4047) (May 8, 2002).

8 FTC Testimony at 5.

9 *See* 16 C.F.R. § 313, *available at* http://www.ftc.gov/os/2000/05/65fr33645.pdf.

10 *See* 16 C.F.R. § 314, *available at* http://www.ftc.gov/os/2002/05/67fr36585.pdf.

11 The FTC has brought several cases for security breaches under GLB and the Safeguards Rule. *See Nations Title Agency Inc. et al.,* (FTC File No. 052 31177) (May 10, 2006)*;Superior Mortgage Corp*., FTC Docket No. C-4153 (Dec. 14, 2005); *Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (Apr. 12, 2005); *In the Matter of Sunbelt Lending Serv.*, FC Docket No. C-4129) (Jan. 3, 2005).

12 *United States v. ChoicePoint, Inc.*, No. 106-CV-0198, Proposed Stipulated Final Judgment and Order for Civil Penalties (N.D. Ga. filed Jan. 30, 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf.

13 *In the Matter of BJ Wholesale, Inc.,* File No. 042-3160 Complaint at 72-3, *available at* http://www.ftc.gov/os/caselist/0423160/09230comp0423160.pdf.

14 *Id.*

15 *In the Matter of BJ's Wholesale, Inc.,* File No. 042-3160 Order at 3, *available at* http://www.ftc.gov/os/caselist/0423160/09230do0423160.pdf.

16 *Id.*

17 *Id.* at 4.

18 FTC Testimony at 9-10.

19 FTC Testimony at 6.

20 FTC Testimony at 7.

21 *Id.*

22 *Id.*

23 DSW Mar. 8, 2005 Customer Alert, *available at* http://www.dsw-shoe.com/ccpressrelease/pr/; DSW Apr. 18, 2005 Customer Alert, *available at* http://www.dswshoe.com/pressRelease.jsp.

24 *In the Matter of DSW Inc*., File No. 052-3096 FTC Complaint at 2.

25 *In the Matter of DSW Inc*., File No. 052-3096 Decision and Order at 3-4, *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWDecisionandOrder.pdf.

26 Neither *BJ's Wholesale* nor *DSW* were required to pay civil penalties

or consumer redress because there were no violations of any of the FTC's trade regulations rules or any statutes specifically authorizing civil penalties. If Congress extends the GLB Safeguards Rule to companies other than financial institutions as the FTC has urged, one can expect future security breach cases to include monetary payments in addition to the injunctive relief of requiring a comprehensive information security program and independent audits by third parties every other year for 20 years. *See* Harbour Speech at 15.

27 Some of the regulations promulgated under the GLB Act and the guidance in the BJ's and DSW cases relating to safeguarding the security of customer information are broadly consistent with those in the European Union Data Protection Directive (95/46/EC). The Directive, which came into force in 1995, sets out the broad data protection principles that EU Member States are required to implement as part of the EU harmonization of data privacy law. (However, national implementation within the 25 Member States will inevitably differ from country to country, and the general principles of data privacy and security will also be supplemented by sector-specific regulations.) The Directive requires the implementation of "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access." The Directive does not prescribe how compliance is to be achieved, but does provide that firms must ensure a level of security appropriate to the type of data. Other principles of the Directive lay down guidance as to the handling and dissemination of data, as well as provisions relating to the use and misuse of data. Companies that are subject to both the EU Directive and the information security requirements discussed in this Advisory (as a result of being either a "financial institution" or subject to the FTC's jurisdiction) need to coordinate their US-based and EU-based information security programs and oversight, with particular attention to the flow of personal information between the EU and the United States.

28 *In the Matter of Microsoft Passport*, File No. 012-3240 (Aug. 2002) (FTC investigation involving claims about alleged online security

vulnerabilities), *available at* http://www.ftc.gov/os/2002/08/microsoftcmp.pdf; *In the Matter of Guess? Inc.,* File No. 022-3260 (June 2002) (same), *available at* http://www.ftc.gov/os/2003/06/guesscmp.htm.

29 *In the Matter of DSW Inc.,* File No. 052-3096 FTC (Dec. 2005); *In the Matter of BJ's Wholesale Club* (June 2005) (FTC did not allege companies violated their own express privacy statements and policy). More recently, the FTC settled with a processor of credit and debit card purchases in the largest known compromise of personal financial data to date. *In the Matter of Card Systems Solutions Inc. and Solidus Networks Inc., d/b/a/ Pay by Touch Solutions,* File No. 052-3148 (proposed settlement posted for public comment on Feb. 23, 2006), *available at* http://www.ftc.gov/os/caseList/0523148/0523148consent.pdf.

30 It is important to understand the relationship between Section 5 and other information security rules such as the GLB Safeguards Rule and the Security Rule under the Health Insurance Portability and Accounting Act (HIPAA). These various rules are not mutually exclusive. Rather, enforcement under Section 5 may be pursued either in conjunction with or as an alternative to other privacy rules. A breach of the GLB Safeguards Rule would likely be considered by the Commission to be a violation of Section 5 as well. Notably the FTC lacks jurisdiction over financial institutions that are regulated by the federal banking agencies (e.g., banks and credit unions) and thus will not pursue Section 5 enforcement actions against such entities. Rather, the banking agencies themselves may initiate enforcement actions against financial institutions subject to their jurisdiction. However, entities subject to HIPAA that maintain electronic personal health information could be subject to potential exposure to FTC actions under Section 5 in addition to their obligation to comply with the HIPAA Security Rule.

31 Letter to Bank of America Corporation in *In the Matter of DSW Inc.,* File No. 052-3096 FTC (Mar. 7, 2005).

32 Letter to Visa, Inc. in *In the Matter of DSW Inc.,* File No. 052-3096 FTC (Mar. 7, 2005), *available at*

http://www.ftc.gov/os/caselist/0523096/0523096DSWLettertoCommenterVisa.pdf.

33 *See* FTC Analysis of Proposed DSW Consent Order, File No. 052-3096, *available at* http://www.ftc.gov/os/caseList/0523096/051201analysis0523096.pdf; FTC Analysis of *BJ's Wholesale* Consent Order, File No. 042-3160; *In the Matter of DSW* Decision and Order, File No. 052-3096, *available at* http://www.ftc.gov/os/caseList/0423160/050616anal0423160.pdf; *In the Matter of BJ's Wholesale Club, Inc.,* File No. 042-3160 FTC Decision and Order at 3; *see also* FTC's *Security Check: Reducing Risks to your Computer Systems* (June 2003), *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm.