ARNOLD & PORTER LLP

CLIENT ADVISORY

FTC Continues Enforcement Efforts to Protect Personal Information

MARCH 2006

Washington, DC
+1 202.942.5000

New York
+1 212.715.1000

London
+44 (0)20 7786 6100

Brussels
+32 (0)2 517 6600

Los Angeles
+1 213.243.4000

San Francisco
+1 415.356.3099

Northern Virginia
+1 703.720.7000

Denver
+1 303.863.1000

In March, the Federal Trade Commission ("FTC") gave final approval to the consent order in its investigation of DSW Inc., an Ohio-based national retailer of shoes. In December 2005, DSW agreed to settle FTC charges that it failed to take reasonable measures to safeguard sensitive consumer data.[1] This case comes on the heels of a similar security breach investigation, *BJ Wholesale*,[2] settled in June 2005. The *DSW* case confirms that the FTC will take enforcement action for security breaches involving consumers' personal information even when the situation does not involve a company's failure to comply with its own privacy policies. It also reinforces past FTC statements that "privacy and information security continues to be a top priority in the FTC's consumer protection program."[3] In a comment on its decision, the FTC has made clear that it may use its enforcement discretion to protect personal information of consumers even in cases where the information is public.[4]

FTC COMPLAINT

The FTC complaint against DSW alleged that DSW failed to take reasonable steps to secure sensitive personal data of customers collected at the point-of-sale and stored on DSW's computer network.[5] Like the FTC complaint in *BJ Wholesale*,[6] the FTC did not base its claim on DSW's failure to comply with its privacy statements, such as claims about the security it provided for personal information of consumers.[7] Instead, the FTC based its suit solely on the fact that DSW possessed sensitive consumer data and failed reasonably to protect it. The agency alleged that this failure constituted an unfair practice under § 5 of the Federal Trade Commission Act ("FTC Act").[8]

In March and April of 2005, DSW notified the public that security breaches had occurred in 108 store locations.[9] 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.[10]

To settle the matter, the FTC required DSW to implement the following security measures to protect personal information of its customers:[11]

- 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.

The agency required the same measures to be implemented in the *BJ Wholesale* case.[12]

FTC Approach in Protecting Personal Consumer Information

DSW confirms that the FTC's approach in *BJ Wholesale* was not an anomaly. Recent cases, including *DSW*, demonstrate that the FTC requires "companies holding sensitive data to have in place procedures to secure it[.]"[13] 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.[14] 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*, the FTC has challenged the company's information security practices as a direct violation of § 5.[15]

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'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 the 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."[16]

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.[17] 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.

In responding to another comment related to the DSW proposed order, the FTC clarified that a failure to encrypt does not in and of itself establish that a company lacked reasonable procedures to safeguard personal information of customers. The FTC will review security procedures overall to determine whether they were reasonable under the circumstances.[18]

CONCLUSION

In short, the FTC requires that companies with personal information of consumers: (1) conduct a risk analysis, (2) develop a program to address any identified risks, (3) designate a person or group to be responsible for the security program, (4) include compliance and monitoring procedures to ensure the program's effectiveness, and (5) update the program and security measures as needed.[19]

ENDNOTES

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

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

3 Remarks of Lydia Parnes, FTC Acting Director Bureau of Consumer Protection, at 2 (Oct. 28, 2004), *available at* www.ftc.gov/speeches/parnes/041028conprivparnes.pdf; *see* Remarks of Howard Beales, FTC Director Bureau of Consumer Protection (Dec. 1, 2005) (stating that consumer concerns about the security of private information were the FTC's "first priority."), *available at* www.ftc.gov/speeches/other/bealesconsumprotectagenda.htm.

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

5 *In the Matter of DSW Inc.*, File No. 052-3096 Complaint at 2-3.

6 *In the Matter of BJ Wholesale Club, Inc.*, File No. 042-3160 Complaint at 2-3, available at www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf.

7 *In the Matter of DSW Inc.*, File No. 052-3096 Complaint at 2-3.

8 *Id.*

9 DSW Mar. 8, 2005 Customer Alert, *available at* www.dswshoe.com/ccpressrelease/pr/CCAprilUpdate.html; DSW Apr. 18, 2005 Customer Alert, *available at* www.dswshoe.com/pressRelease.jsp.

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

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

12 *In the Matter of BJ Wholesale Club, Inc.*, File No. 042-3160 FTC Decision and Order at 3.

13 Testimony of Chairman Deborah Majoras Before the Senate Committee on Commerce, Science and Transportation at 9 (June 16, 2005), *available at* www.ftc.gov/os/2005/06/050616databreaches.pdf.

14 *In the Matter of Microsoft Passport*, File No. 012-3240 (Aug. 2002) (FTC investigation involving claims about alleged online security vulnerabilities), *available at* www.ftc.gov/os/2002/08/microsoftcmp.pdf; *In the Matter of Guess? Inc.*, File No. 022-3260 (June 2002) (same), *available at* www.ftc.gov/os/2003/06/guesscmp.htm; *In the matter of BJ Wholesale Club* (June 2005) (FTC investigation involving alleged point-of-sale vulnerabilities); *In the Matter of DSW Inc.*, File No. 052-3096 FTC (Dec. 2005) (same).

15 *In the Matter of DSW Inc.*, File No. 052-3096 FTC (Dec. 2005); *In the matter of BJ Wholesale Club* (June 2005) (FTC did not allege companies violated their own express privacy statements and policy).

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

17 The FTC's information security approach is discussed in more detail in Arnold & Porter LLP's June 2005 Client Advisory, *Recent FTC Enforcement Activity and Congressional Testimony Highlight Importance of Integrated Information Security Programs* (June 2005), *available at* www.arnoldporter.com/pubs/files/Arnold&PorterAdvisory-RecentFTCEnforcementActivityandCongressionalTestimony.pdf.

18 Letter to Visa, Inc. in *In the Matter of DSW Inc.*, File No. 052-3096 FTC (Mar. 7, 2005) *available at* www.ftc.gov/os/caselist/0523096/0523096DSWLettertoCommenterVisa.pdf.

19 *See* FTC Analysis of Proposed DSW Consent Order, File No. 052-3096; FTC Analysis of Proposed *BJ Wholesale* Consent Order, File No. 042-3160; *In the Matter of DSW* Decision and Order, File No. 052-3096; *In the Matter of BJ 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* www.ftc.gov/bcp/conline/pubs/buspubs/security.htm.

If you would like additional information, please contact:

Ronald Lee
202.942.5380
Ronald.Lee@aporter.com

Amy Mudge
202.942.5485
Amy.Mudge@aporter.com