Analysis of Proposed Consent Order to Aid Public Comment

DSW Inc., File No. 052-3096

The Federal Trade Commission has accepted a consent agreement, subject to final approval, from DSW Inc. ("DSW").

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received and will decide whether it should withdraw from the agreement and take other appropriate action or make final the agreement's proposed order.

As described in the Commission's proposed complaint, DSW sells footwear for men and women at approximately 190 stores in 32 states. Consumers pay for their purchases with cash, credit cards, debit cards, and personal checks. In the course of seeking approval for credit and debit card purchases, DSW collects consumers' personal information, including name, card number and expiration date, and other information, from magnetic stripes on the cards. The information collected from the magnetic stripe is particularly sensitive because it contains a security code which can be used to create counterfeit cards that appear genuine in the authorization process. In the course of seeking approval for personal check purchases, DSW also collects consumers' personal information, including routing number, account number, check number, and the consumer's driver's license number and state, from the check using Magnetic Ink Character Recognition ("MICR") technology.

The Commission's proposed complaint alleges that DSW stored consumers' personal information on computers on networks located at both the store and corporate levels and failed to employ reasonable and appropriate security measures to protect the information. The complaint alleges that this failure was an unfair practice because it caused or was likely to cause substantial consumer injury that was not reasonably avoidable and was not outweighed by countervailing benefits to consumers or competition. In particular, the complaint alleges that until at least March 2005, DSW engaged in a number of practices which, taken together, failed to provide reasonable security for sensitive personal information, including: (1) creating unnecessary risks to personal information collected at its stores by storing it in multiple files when it no longer had a business need to keep the information; (2) failing to use readily available security measures to limit access to its computer networks through wireless access points on the networks; (3) storing the information in unencrypted files that could be accessed easily by using a commonly known user ID and password; (4) failing to sufficiently limit the ability of computers on one in-store computer network to connect to computers on other in-store and corporate networks; and (5) failing to employ sufficient measures to detect unauthorized access.

The complaint further alleges that there have been fraudulent charges on accounts that consumers had used at DSW's stores. Additionally, some consumers whose checking account information was compromised were advised to close their accounts, thereby losing access to those accounts, and incurred out-of-pocket expenses such as the cost of ordering new checks.

The proposed order applies to personal information from or about consumers that DSW collects in connection with its business. It contains provisions designed to prevent DSW from engaging in the future in practices similar to those alleged in the complaint.

Specifically, Part I of the proposed order requires DSW to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information it collects from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to DSW's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected. Specifically, the order requires DSW to:

- Designate an employee or employees to coordinate and be accountable for the information security program.

- Identify material internal and external risks to the security, confidentiality, and integrity of consumer information that could result in unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

- Design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures.

- Evaluate and adjust its information security program in light of the results of testing and monitoring, any material changes to its operation or business arrangements, or any other circumstances that DSW knows or has reason to know may have a material impact on the effectiveness of its information security program.

Part II of the proposed order requires that DSW obtain within 180 days, and on a biennial basis thereafter, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) DSW has in place a security program that provides protections that meet or exceed the protections required by Part I of the proposed order, and (2) DSW's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information has been protected. This provision is substantially similar to comparable provisions obtained in prior Commission orders under Section 5 of the FTC Act. *See, e.g.*, *BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005).

Parts III through VII of the proposed order are reporting and compliance provisions. Part III requires DSW to retain documents relating to compliance. For the assessments and supporting documents, DSW must retain the documents for three (3) years after the date that each assessment is prepared. Part IV requires dissemination of the order now and for the next ten (10) years to persons with supervisory responsibilities. Part V ensures notification to the FTC of changes in corporate status. Part VI mandates that DSW submit compliance reports to the FTC. Part VII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed order or to modify its terms in any way.