052 3096

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **Deborah Platt Majoras, Chairman**
Pamela Jones Harbour
Jon Leibowitz
William E. Kovacic
J. Thomas Rosch

In the Matter of	)	
DSW Inc.,	)	
a corporation.	)	**DOCKET NO. C-4157**

COMPLAINT

The Federal Trade Commission, having reason to believe that DSW Inc. ("respondent") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent DSW Inc. is an Ohio corporation with its principal office or place of business at 4150 East 5th Avenue, Columbus, Ohio 43219.

2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

3. Respondent 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.

4. For credit card, debit card, and check purchases at its stores, respondent uses computer networks to request and obtain authorization for the purchase. To obtain card authorization, respondent collects information from consumers, including name, card number and expiration date, and certain other information. To obtain approval for payments by check, respondent collects the routing number, account number, check number, and the consumer's driver's license number and state (collectively, "personal information").

5. For a credit or debit card purchase, respondent typically collects the information from the magnetic stripe of the credit or debit card. The information collected from the magnetic stripe includes, among other things, a security code used to verify electronically that the card is genuine. This code is particularly sensitive because it can be used to create counterfeit credit and debit cards that appear genuine in the authorization process. For purchases using a check, respondent typically collects information from the check using Magnetic Ink Character Recognition ("MICR") technology. In each case, respondent collects the information at the cash register and wirelessly transmits the information, formatted as an authorization request, to a computer network located in the store ("in-store computer network"). The authorization request is then transmitted to the appropriate bank or check processor, which sends a response back to respondent through the same networks. Until at least March 2005, respondent stored personal information used to obtain credit card, debit card, and check authorizations, including magnetic stripe data, on in-store and corporate computer networks.

6. Respondent operates wireless access points through which the cash registers connect to the in-store computer networks. Other wireless access points are used to transmit information about respondent's inventory from in-store scanners to the in-store computer networks.

7. Until at least March 2005, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information collected at its stores. Among other things, respondent (1) created unnecessary risks to the information by storing it in multiple files when it no longer had a business need to keep the information; (2) did not use readily available security measures to limit access to its computer networks through wireless access points on the networks; (3) stored the information in unencrypted files that could be accessed easily by using a commonly known user ID and password; (4) did not limit sufficiently the ability of computers on one in-store network to connect to computers on other in-store and corporate networks; and (5) failed to employ sufficient measures to detect unauthorized access. As a result, a hacker could use the wireless access points on one in-store computer network to connect to, and access personal information on, the other in-store and corporate networks.

8. In March 2005, respondent issued a press release stating that credit card and other purchase information stored on its computer networks had been stolen. In April 2005, respondent issued another press release listing the locations of 108 stores that were affected by the breach, and stating that checking account and driver's license numbers also had been subject to the breach. In April 2005, respondent also began sending notification letters to customers for whom it had or obtained addresses.

9. The breach compromised a total of approximately 1,438,281 credit and debit cards (but not the personal identification numbers associated with the debit cards), along with 96,385 checking accounts and driver's license numbers. To date, there have been fraudulent charges on some of these accounts. Further, some customers whose checking

account information was compromised were advised to close their accounts, thereby losing access to those accounts, and have incurred out-of-pocket expenses such as the cost of ordering new checks. Some of these checking account customers have contacted DSW requesting reimbursement for their out-of-pocket expenses, and DSW has provided some amount of reimbursement to these customers.

10. As described in Paragraph 7 above, respondent's failure to employ reasonable and appropriate security measures to protect personal information and files caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was and is an unfair act or practice.

11. The acts and practices of respondent as alleged in this complaint constitute unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this seventh day of March, 2006, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary

SEAL