072-3055

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

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

In the Matter of	)	
THE TJX COMPANIES, INC., a corporation.	)	**DOCKET NO. C-4227**

COMPLAINT

The Federal Trade Commission, having reason to believe that The TJX Companies, 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 The TJX Companies, Inc. is a Delaware corporation with its principal office or place of business at 770 Cochituate Road, Framingham, Massachusetts, 01701.

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 is an off-price retailer selling apparel and home fashions in over 2,500 stores worldwide, including, but not limited to, T.J. Maxx, Marshalls, A.J. Wright, Bob's Stores, and HomeGoods stores in the United States; Winners and HomeSense in Canada; and T.K.Maxx stores in the United Kingdom, Ireland, and Germany. Consumers may pay for purchases at these stores with credit and debit cards (collectively, "payment cards"), cash, or personal checks.

4. Respondent operates corporate computer networks in the United States ("central corporate network") and internationally, as well as networks in each store ("in-store networks"). These networks link worldwide corporate headquarters in the United States with each store, and, among other things, are used to process sales transactions and provide wireless access to the networks for wireless devices, such as devices for marking down prices.

5. In selling its products, respondent routinely uses its computer networks to collect personal information from consumers to obtain authorization for payment card purchases,

verify personal checks, and process merchandise returned without receipts ("unreceipted returns"). Among other things, it collects: (1) account number, expiration date, and an electronic security code for payment card authorization; (2) bank routing, account, and check numbers and, in some instances, driver's license number and date of birth for personal check verification; and (3) name, address, and drivers' license, military, or state identification number ("personal ID numbers") for unreceipted returns (collectively, "personal information"). This information is particularly sensitive because it can be used to facilitate payment card fraud and other consumer harm.

6. To obtain payment card authorization, respondent formats personal information from the card into an authorization request. It typically transmits authorization requests from in-store networks to designated computers ("card authorization computers") on the central corporate network, and from there to the banks that issued the cards ("issuing banks"). Respondent receives responses authorizing or declining the purchase from issuing banks over the same networks.

7. Until December 2006, respondent stored authorization requests and personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks. At all relevant times, respondent transmitted authorization requests and responses in clear text between and within its in-store and corporate networks.

8. Since at least July 2005, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its networks. In particular, respondent:

   (a) created an unnecessary risk to personal information by storing it on, and transmitting it between and within, in-store and corporate networks in clear text;

   (b) did not use readily available security measures to limit wireless access to its networks, thereby allowing an intruder to connect wirelessly to in-store networks without authorization;

   (c) did not require network administrators and other users to use strong passwords or to use different passwords to access different programs, computers, and networks;

   (d) failed to use readily available security measures to limit access among computers and the internet, such as by using a firewall to isolate card authorization computers; and

   (e) failed to employ sufficient measures to detect and prevent unauthorized access to computer networks or to conduct security investigations, such as by patching or updating anti-virus software or following up on security warnings and intrusion alerts.

9. Between July 2005 and November 2005, an intruder connected to respondent's networks without authorization, installed hacker tools, found personal information stored in clear text, and downloaded it over the internet to remote computers. Further, between May and December 2006, an intruder periodically intercepted payment card authorization requests in transit from in-store networks to the central corporate network, stored the information in files on the network, and transmitted the files over the internet to remote computers. After learning of the breach, respondent took steps to prevent further unauthorized access and to notify law enforcement and affected consumers.

10. In January 2007, respondent issued a press release stating that payment card and other personal information had been stolen from its computer networks by an intruder. In February 2007, respondent issued another press release stating that additional personal information may have been stolen from stores located in the United States and Canada as early as July 2005.

11. The breach compromised tens of millions of unique payment cards used by consumers in the United States and Canada. To date, issuing banks have claimed tens of millions of dollars in fraudulent charges on some of these accounts. Issuing banks also have cancelled and re-issued millions of payment cards, and consumers holding these cards were unable to use them to access their credit and bank accounts until they received the replacement cards. In addition, the breach compromised the personal information of approximately 455,000 consumers who had made unreceipted merchandise returns. This personal information included personal ID numbers, which in some instances were also consumers' Social Security numbers. Further, some consumers have obtained or will have to obtain new personal ID numbers, such as new drivers' licenses.

12. As described in Paragraphs 8 through 11, respondent's failure to employ reasonable and appropriate security measures to protect personal information 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.

13. 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 twenty-ninth day of July, 2008, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary