072-3055

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	)	
THE TJX COMPANIES, INC., a corporation.	)	**DOCKET NO. C-**

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

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