Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of The TJX Companies, Inc., File No. 072-3055

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

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 appropriate action or make final the agreement's proposed order.

According to the Commission's complaint, TJX is an off-price retailer selling apparel and home fashions in over 2,500 stores worldwide. Consumers may pay for purchases at these stores with credit and debit cards (collectively, "payment cards"), cash, or personal checks. In selling its products, TJX 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 or 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.

The Commission's proposed complaint alleges that since at least July 2005, TJX engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks. Among other things, TJX: (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.

The complaint alleges that the breach compromised tens of millions of payment cards as well as the personal information of approximately 455,000 consumers who had made unreceipted returns. The complaint further alleges that issuing banks have claimed tens of millions of dollars in fraudulent charges on some of these payment card accounts. Issuing banks also have cancelled and re-issued millions of payment cards, and according to the complaint,

consumers holding these cards were unable to use them to access their credit and bank accounts until they received the replacement cards. Additionally, the complaint alleges that some consumers have obtained or will have to obtain new personal ID numbers, such as new drivers' licenses.

The proposed order applies to personal information TJX collects from or about consumers. It contains provisions designed to prevent TJX from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order requires TJX 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 collected from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to TJX's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. Specifically, the order requires TJX 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 personal information that could result in the 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.

- Develop and use reasonable steps to retain service providers capable of appropriately safeguarding personal information they receive from respondents, require service providers by contract to implement and maintain appropriate safeguards, and monitor their safeguarding of personal information.

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

Part II of the proposed order requires that TJX obtain, covering the first 180 days after the order is served, and on a biennial basis thereafter for twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that (1) it 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) its security program is operating

with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information is protected.

Parts III through VII of the proposed order are reporting and compliance provisions. Part III requires TJX to retain documents relating to its compliance with the order. For most records, the order requires that the documents be retained for a five-year period. For the third-party assessments and supporting documents, TJX must retain the documents for a period of three years after the date that each assessment is prepared. Part IV requires dissemination of the order now and in the future to principals, officers, directors, and managers having responsibilities relating to the subject matter of the order. Part V ensures notification to the FTC of changes in corporate status. Part VI mandates that TJX submit an initial compliance report to the FTC, and make available to the FTC subsequent reports. Part VII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

This is the Commission's twentieth case to challenge the failure by a company to implement reasonable information security practices. Each of the Commission's cases to date has alleged that a number of security practices, taken together, failed to provide reasonable and appropriate security to prevent unauthorized access to consumers' information. The practices challenged in the cases have included, but are not limited to: (1) creating unnecessary risks to sensitive information by storing it on computer networks without a business need to do so; (2) storing sensitive information on networks in a vulnerable format; (3) failing to use readily available security measures to limit access to a computer network through wireless access points on the network; (4) failing to adequately assess the vulnerability of a web application and computer network to commonly known or reasonably foreseeable attacks; (5) failing to implement simple, low-cost, and readily available defenses to such attacks; (6) failing to use readily available security measures to limit access between computers on a network and between such computers and the internet, and (7) failing to use strong passwords to authenticate (or authorize) users to access programs and databases on computer networks or online.

The purpose of the analysis is to aid 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.