

**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

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