test or monitor the effectiveness of the safeguards' key controls, systems, and procedures.

● Develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from the respondent, and require service providers by contract to implement and maintain appropriate safeguards.

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

Part II of the proposed order requires each respondent to obtain within 180 days, and on a biennial basis thereafter for a period of 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 has been protected.

Parts III through VII of the proposed order are reporting and compliance provisions. Part III requires respondents to retain documents relating to their 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, respondents 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 persons with 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 each respondent submit a compliance report to the FTC within 180 days, and periodically thereafter as requested. Part VII is a provision ''sunsetting'' the order after twenty (20) years, with certain exceptions.

This is the Commission's nineteenth 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; and (6) failing to use readily available security measures to limit access between computers on a network and between such computers and the Internet. This proposed action against REI and Seisint is the first to challenge alleged security failures involving the security of passwords. Passwords are a critical part of a reasonable and appropriate security program because passwords are typically the first (and are often the only) method used to authenticate (or authorize) users to access resources, such as programs and databases, available on a computer network or online.

The purpose of this analysis is to facilitate 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.

By direction of the Commission.

Donald S. Clark

Secretary

[FR Doc. E8–6952 Filed 4–2–08: 8:45 am]

[BILLING CODE 6750–01–S]

FEDERAL TRADE COMMISSION

[File No. 072 3055]

The TJX Companies, Inc.; Analysis of Proposed Consent Order to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed Consent Agreement.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices or unfair methods of competition. The attached Analysis to Aid Public Comment describes both the allegations in the draft complaint and the terms of the consent order—embodied in the consent agreement—that would settle these allegations.

DATES: Comments must be received on or before April 28, 2008.

ADDRESSES: Interested parties are invited to submit written comments. Comments should refer to ''TJX, File No. 072 3055,'' to facilitate the organization of comments. A comment filed in paper form should include this reference both in the text and on the envelope, and should be mailed or delivered to the following address: Federal Trade Commission/Office of the Secretary, Room 135–H, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. Comments containing confidential material must be filed in paper form, must be clearly labeled ''Confidential,'' and must comply with Commission Rule 4.9(c). 16 CFR 4.9(c) (2005).[1] The FTC is requesting that any comment filed in paper form be sent by courier or overnight service, if possible, because U.S. postal mail in the Washington area and at the Commission is subject to delay due to heightened security precautions. Comments that do not contain any nonpublic information may instead be filed in electronic form by following the instructions on the web-based form at *http://secure.commentworks.com/ftc-TJX*. To ensure that the Commission considers an electronic comment, you must file it on that web-based form.

The FTC Act and other laws the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. All timely and responsive public comments, whether filed in paper or electronic form, will be considered by the Commission, and will be available to the public on the FTC website, to the extent practicable, at *www.ftc.gov.* As a matter of discretion, the FTC makes every effort to remove home contact information for individuals from the public comments it receives before placing those comments on the FTC website. More information, including routine uses permitted by the Privacy Act, may be found in the FTC's privacy policy, at *http://www.ftc.gov/ftc/privacy.shtm*.

FOR FURTHER INFORMATION CONTACT: Alain Sheer or Molly Crawford, FTC Bureau of Consumer Protection, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, (202) 326–2252.

[1] The comment must be accompanied by an explicit request for confidential treatment, including the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. The request will be granted or denied by the Commission's General Counsel, consistent with applicable law and the public interest. *See* Commission Rule 4.9(c), 16 CFR 4.9(c).

SUPPLEMENTARY INFORMATION: Pursuant to section 6(f) of the Federal Trade Commission Act, 38 Stat. 721, 15 U.S.C. 46(f), and § 2.34 of the Commission Rules of Practice, 16 CFR 2.34, notice is hereby given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of thirty (30) days. The following Analysis to Aid Public Comment describes the terms of the consent agreement, and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained from the FTC Home Page (for March 27, 2008), on the World Wide Web, at *http://www.ftc.gov/os/2008/03/index.htm.* A paper copy can be obtained from the FTC Public Reference Room, Room 130–H, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, either in person or by calling (202) 326–2222.

Public comments are invited, and may be filed with the Commission in either paper or electronic form. All comments should be filed as prescribed in the **ADDRESSES** section above, and must be received on or before the date specified in the **DATES** section.

Analysis of Agreement Containing Consent Order to Aid Public Comment

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.

By direction of the Commission.

Donald S. Clark

Secretary

[FR Doc. E8–6950 Filed 4–2–08: 8:45 am]

[BILLING CODE 6750–01–S]

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Agency for Healthcare Research and Quality

Agency Information Collection Activities: Proposed Collection; Comment Request

AGENCY: Agency for Healthcare Research and Quality, HHS.

ACTION: Notice.

SUMMARY: This notice announces the intention of the Agency for Healthcare Research and Quality (AHRQ) to request that the Office of Management and Budget (OMB) approve the proposed information collection project: ''Assessment of the Emergency Severity Index (ESI).'' In accordance with the Paperwork Reduction Act of 1995, Public Law 104–13 (44 U.S.C. 3506(c)(2)(A)), AHRQ invites the public to comment on this proposed information collection.

This proposed information collection was previously published in the **Federal Register** on January 22nd, 2008 and allowed 60 days for public comment. No comments were received. The purpose of this notice is to allow an additional 30 days for public comment.

DATES: Comments on this notice must be received by May 5, 2008.

ADDRESSES: Written comments should be submitted to: AHRQ's OMB Desk Officer by fax at (202) 395–6974 (attention: AHRQ's desk officer) or by e-mail at *OIRA_submission@omb.eop.gov* (attention: AHRQ's desk officer). Copies of the proposed collection plans, data collection instruments, and specific details on the estimated burden can be obtained from the AHRQ Reports Clearance Officer.

FOR FURTHER INFORMATION CONTACT: Doris Lefkowitz, AHRQ Reports Clearance Officer, (301) 427–1477, or by e-mail at *doris.lefkowitz@ahrq.hhs.gov*.

SUPPLEMENTARY INFORMATION:

''Proposed Project—Assessment of the Emergency Severity Index (ESI)''

AHRQ is proposing to examine uptake and use of an emergency room triage tool, the Emergency Severity Index (ESI). The hospital emergency department (ED) represents a critical point in care delivery for patients across the United States. Over the past decade, however, the dramatic influx of patients into EDs has seriously challenged the ability of these departments to deliver timely, quality, and safe emergency healthcare services. Moreover, with most emergency departments operating at or over capacity it may prove difficult for them to respond to the surge in emergency room demand created by natural and man-made disasters. Development of increasingly refined and validated triage methods is one potential key to addressing overcrowding by speeding up the care delivery to the most acute ED patients while helping hospitals assess, carefully allocate and plan the amount of human and other resources needed to care for all patients.

In response to a need to standardize the triage process and improve the flow of patients, Richard C. Wuerz, MD, (Department of Emergency Medicine at the Brigham and Women's Hospital and the Harvard Medical School) and David R. Eitel, MD, (Department of Emergency Medicine, The York Hospital WellSpan Health System) initiated development of the Emergency Severity Index (ESI) in 1995. The ESI is unique in its focus on appropriate resource allocation and its consideration of necessary resource utilization in assigning acuity. To encourage adoption of the ESI, AHRQ developed an implementation handbook (Emergency Severity Index, Version 4) and companion DVDs. These materials are intended to provide hospitals and triage nurses with background on why they might want to implement the ESI as a triage tool, and offers recommendations on the implementation process and staff training.

This project will assess the product's acceptance by emergency departments and others involved in addressing medical surges to better understand the usefulness of the ESI compared to other similar tools. It will focus on the satisfaction with the product's presentation, content, and clarity; extent to which the product has improved emergency services and surge preparation; and the improvements users would like to see in the next version of this product. This will be accomplished through (1) developing and implementing an electronic and paper-based survey targeting emergency department professionals assessing the satisfaction with the ESI's content, clarity and actual use of the system in everyday emergency departments, and (2) convening focus groups of ED professionals to identify characteristics that might predict uptake and use of this