

Complaint

IN THE MATTER OF

THE TJX COMPANIES, INC.CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS
OF SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket C-4227; File No. 072 3055
Complaint, July 29, 2008 – Decision, July 29, 2008

This consent order addresses practices of The TJX Companies, Inc., that failed to provide reasonable and appropriate security for personal information on its computer networks. TJX sells apparel and home fashions in over 2,500 stores worldwide. A breach of its computer networks compromised tens of millions of unique payment cards used by consumers in the United States and Canada. The 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. The order requires that TJX obtain, on a biennial basis for 20 years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that TJX has in place a security program that provides protections that meet or exceed the protections required by the order, and that its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information is protected. TJX is required to retain documents relating to its compliance with the order; to disseminate the order to principals, officers, directors, and managers having responsibilities relating to the subject matter of the order; to notify the Commission of changes in corporate status; and to file compliance reports with the Commission.

Participants

For the *Commission*: *Molly Crawford, Jessica Rich, Alain Sheer, and Joel Winston.*

For the *Respondents*: *Lisa J. Sotto, Hunton & Williams, and Mit Spears, Ropes & Gray LLP.*

Complaint

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,

Complaint

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;

Complaint

(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.

Complaint

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 un-receipted 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.

Decision and Order

DECISION AND ORDER

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft of Complaint which the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued, would charge the Respondent with violation of the Federal Trade Commission Act; and

The Respondent and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of the agreement is for settlement purposes only and does not constitute an admission by the Respondent that the law has been violated as alleged in such complaint, or that any of the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the Respondent has violated the Federal Trade Commission Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, now in further conformity with the procedure prescribed in Section 2.34 of its Rules, 16 C.F.R. § 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following order:

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.

Decision and Order

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

For purposes of this Order, the following definitions shall apply:

1. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name, that reveals an individual’s email address; (d) a telephone number; (e) a Social Security number; (f) credit or debit card information, including card number, expiration date, and data stored on the magnetic strip of a credit or debit card; (g) checking account information, including the ABA routing number, account number, and check number; (h) a driver’s license, military, or state identification number; (i) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (j) any information that is combined with any of (a) through (i) above.
2. Unless otherwise specified, “respondent” shall mean The TJX Companies, Inc., and its successors and assigns, officers, agents, representatives, and employees.
3. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

Decision and Order

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program.
- B. the identification of 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 assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.
- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment and

Decision and Order

regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

- D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards.
- E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by sub-Part C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that, in connection with its compliance with Part I of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of

Decision and Order

respondent's activities, and the sensitivity of the personal information collected from or about consumers;

- C. explain how the safeguards that have been implemented meet or exceed the protections required by the Part I of this order; and
- D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

III.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy

Decision and Order

of each document relating to compliance, including but not limited to:

- A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and
- B. for a period of three (3) years after the date of preparation of each Assessment required under Part II of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts I and II of this order, for the compliance period covered by such Assessment.

IV.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

V.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices

Decision and Order

subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. *Provided, however,* that with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VI.

IT IS FURTHER ORDERED that respondent shall, within one hundred eighty (180) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VII.

This order will terminate on July 29, 2028, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however,* that the filing of such a complaint will not affect the duration of:

- A. any Part in this order that terminates in less than twenty (20) years;
- B. this order's application to any respondent that is not named as a defendant in such complaint; and
- C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Analysis to Aid Public Comment

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

**ANALYSIS OF 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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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,

Analysis to Aid Public Comment

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.

Complaint

IN THE MATTER OF

TALX CORPORATIONCONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS
OF SEC. 7 OF THE CLAYTON ACT AND SEC. 5 OF THE FEDERAL
TRADE COMMISSION ACT

Docket C-4228; File No. 061 0209
Complaint, August 6, 2008 – Decision, August 6, 2008

This consent order addresses TALX Corporation's consummated acquisitions of several of its competitors, which substantially reduced competition in the provision of unemployment compensation management services and verification of income and employment services nationwide. The order prohibits the respondent from enforcing certain restrictions on competition, solicitation, and trade secret disclosure against certain current and former employees who accept employment with its competitors. The order lists and categorizes such employees and limits the number of persons in each category subject to this provision. In addition, the provision will end two years after such person's receipt of the required notice from TALX. The order requires TALX to allow certain customers with long-term contracts to terminate their contracts if those customers outsource their services to a competitor of TALX, and it places an upper limit of \$10 million on the total value of terminated long-term contracts. TALX is also required to transfer certain specified customer file information to former customers, upon request. TALX is barred from entering into agreements that would prevent or discourage any entity from supplying goods or services to any of its competitors. The order requires TALX to notify current and former employees and long-term contract customers of their rights under the order, and to notify customers of their right to cancel contracts that would otherwise be renewed automatically, as well as to post information on websites concerning the rights of employees and customers. The order prohibits TALX from entering into certain agreements and requires that TALX notify the Commission before acquiring or entering into a management contract with a provider of unemployment compensation management services or verification of income and employment services. Additional provisions appoint a monitor/administrator to assist in monitoring the respondent's compliance with the order and require the respondent to comply with certain reporting requirements to the Commission.