



ROPES & GRAY LLP  
ONE INTERNATIONAL PLACE  
BOSTON, MA 02110-2624  
WWW.ROPESGRAY.COM

June 22, 2009

Kevin V. Jones  
617-951-7345  
617-235-0857 fax  
kevin.jones@ropesgray.com

**BY HAND DELIVERY**

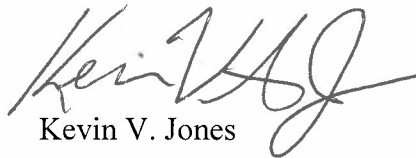
John M. Stephan, Esq.  
Assistant Attorney General  
Consumer Protection Division  
Office of the Attorney General  
One Ashburton Place  
Boston, MA 02108

RE: The TJX Companies, Inc.

Dear Mr. Stephan:

As you know, The TJX Companies, Inc. ("TJX") has entered into an Assurance dated June 22, 2009, with a multi-state group of Attorneys General acting on behalf of the states listed in the first paragraph of the Assurance. Further to the agreement, please find enclosed a final copy of the Assurance executed by and between TJX and the Attorney General of Massachusetts.

Sincerely,



Kevin V. Jones

KVJ:mw  
Enclosure

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT  
DEPARTMENT OF THE TRIAL COURT

In re:

The TJX Companies, Inc.

ASSURANCE

This Assurance (the "Assurance") is between The TJX Companies, Inc., a Delaware corporation ("TJX"), and the Attorneys General of Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Hawaii,<sup>1</sup> Idaho, Illinois, Iowa, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Vermont, Washington, West Virginia, Wisconsin, and the District of Columbia (referred to collectively as the "Attorneys General"), acting pursuant to their respective consumer protection statutes on behalf of their respective states (the "States").<sup>2</sup>

<sup>1</sup> Hawaii is represented by its Office of Consumer Protection, an agency which is not part of its Attorney General's office, but which is statutorily authorized to represent the State of Hawaii in consumer protection actions. For purposes of simplicity, the designation "Attorney General" as it pertains to Hawaii shall refer to the Executive Director of the State of Hawaii's Office of Consumer Protection.

<sup>2</sup> ALABAMA – Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19-1 *et seq.*; ARIZONA – Arizona Consumer Fraud Act, Ariz. Rev. Stat. §§ 44-152[1] *et seq.*; ARKANSAS – Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-101 *et seq.*; CALIFORNIA – Cal. Bus. & Prof. Code §§ 17200 *et seq.*; COLORADO – Colorado Consumer Protection Act, Colo. Rev. Stat. §§ 6-1-101 *et seq.*; CONNECTICUT – Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. §§ 42-110a *et seq.*; DELAWARE – Delaware Consumer Fraud Act, Del. Code Ann. tit. 6, §§ 2511-27 *et seq.*; FLORIDA – Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. §§ 501.201 *et seq.*; HAWAII – Haw. Rev. Stat. §§ 480-1 *et seq.*; IDAHO – Idaho Consumer Protection Act, Idaho Code §§ 48.601 *et seq.*; ILLINOIS – Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. §§ 505/1 *et seq.*; IOWA – Iowa Consumer Fraud Act, Iowa Code § 714.16; LOUISIANA – Louisiana Unfair Trade Practices and Consumer Protection Act, LSA-R.S. 51:1401, *et seq.*; MAINE – Maine Unfair Trade Practices Act, Me. Rev. Stat. Ann. tit. 5, §§ 210 *et seq.*; MARYLAND – Maryland Consumer Protection Act, Md. Code Ann. Com. Law §§ 13-101 *et seq.*; MASSACHUSETTS – Massachusetts Consumer Protection Act, Mass. Gen. Laws ch. 93A, §§ 1 *et seq.*; MICHIGAN – Michigan Consumer Protection Act, Mich. Comp. Laws Ann. §§ 445.901 *et seq.*

## I. RECITALS

**WHEREAS**, as TJX publicly announced on January 17, 2007 and February 21, 2007, a person or persons (such intruder or intruders referred to collectively as the "Intruders") gained unauthorized access during periods in 2005 and 2006 to portions of TJX's computer system that centrally process and store information from payment card and other transactions at certain of TJX's retail stores (such intrusion or intrusions referred to collectively as the "Intrusion");

**WHEREAS**, on August 5, 2008, the United States Department of Justice and the United States Secret Service announced federal criminal charges against eleven individuals in connection with the Intrusion into portions of TJX's computer system;

**WHEREAS**, through the Intrusion, the Intruders are believed to have intercepted and stolen certain customer information, including cardholder data collected from the magnetic stripe on the back of payment cards, possibly while that data was in transit for bank authorization;

**WHEREAS**, a multi-state group of Attorneys General conducted an extensive review and inquiry of TJX's data security policies and procedures in place when the Intruders

---

MISSISSIPPI – Mississippi Consumer Protection Act, Miss. Code Ann. §§ 75-24-1 *et seq.*; MISSOURI – Missouri Merchandising Practices Act, Mo. Rev. Stat. §§ 407.010 *et seq.*; MONTANA – Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code Ann. §§ 30-14-101 *et seq.*; NEBRASKA – Nebraska Consumer Protection Act, Neb. Rev. Stat. §§ 59-1601 *et seq.*; NEVADA – Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. §§ 598.0903 *et seq.*; NEW HAMPSHIRE – New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. §§ 358-A:1 *et seq.*; NEW JERSEY – New Jersey Consumer Fraud Act, N.J. Stat. Ann. §§ 56:8-1 *et seq.*; NEW MEXICO – New Mexico Unfair Practices Act §§ 57-12-1 *et seq.*; NEW YORK – N.Y. Gen. Bus. Law §§ 349 & 350 and N.Y. Exec. Law § 63(12); NORTH CAROLINA – North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. §§ 75-1.1 *et seq.*; NORTH DAKOTA – North Dakota Consumer Fraud and Unlawful Credit Practices Act, N.D. Cent. Code §§ 51-15-01 *et seq.*; OHIO – Ohio Consumer Sales Practices Act, Ohio Rev. Code §§ 1345.01 *et seq.*; OKLAHOMA – Oklahoma Consumer Protection Act, Okla. Stat. tit. 15, §§ 751 *et seq.*; OREGON – Oregon Unlawful Trade Practices Act, Or. Rev. Stat. §§ 646.605 *et seq.*; PENNSYLVANIA – Pennsylvania Unfair Trade Practices and Consumer Protection Law, Pa. Stat. Ann. tit. 73, §§ 201-1 *et seq.*; RHODE ISLAND – Rhode Island Unfair Trade Practice and Consumer Protection Act, R.I. Gen. Laws §§ 6-13.1-1 *et seq.*; SOUTH DAKOTA – South Dakota Deceptive Trade Practices and Consumer Protection Act, S.D. Codified Laws §§ 37-24-1 *et seq.*; TENNESSEE – Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-101 *et seq.*; TEXAS – Texas Deceptive Trade Practices and Consumer Protection Act, Tex. Bus. & Com. Code Ann. §§ 17.41 *et seq.*; VERMONT – Vermont Consumer Fraud Act, Vt. Stat. Ann. tit. 9, §§ 2451 *et seq.*; WASHINGTON – Washington Consumer Protection Act, Wash. Rev. Code Ann. §§ 19.86.010 *et seq.*; WEST VIRGINIA – West Virginia Consumer Credit and Protection Act, W. Va. Code §§ 46A-1-101 *et seq.*; WISCONSIN – Wisconsin Statutes §§ 100.18 and 100.20; DISTRICT OF COLUMBIA – District of Columbia Consumer Protection Procedures Act, D.C. Code Ann. §§ 28-3901 *et seq.*

unlawfully gained access to consumer information and also reviewed TJX's policies and procedures after the discovery of the Intrusion (the "Investigation"). The inquiry considered, among other things: TJX's data encryption systems; data segmentation systems; data protection systems; and intrusion detection systems (the "Subject Matter");

**WHEREAS**, TJX has cooperated with the Attorneys General in their Investigation by, among other things, providing certain documents, making others available for inspection, and providing access to experts consulting with TJX;

**WHEREAS**, the Attorneys General have determined that it is in the public interest of their respective States and TJX's customers to enter into this Assurance at this time and conclude such review and inquiry; and,

**WHEREAS**, the parties wish to completely settle, release, and discharge all civil claims under the respective consumer protection laws of each of the States, and this Assurance constitutes a good faith settlement of any disputes and disagreements between TJX and the Attorneys General, as set forth in section IX.A of this Assurance;

**NOW, THEREFORE**, in consideration of their mutual agreements to the terms of this Assurance, and such other consideration as described herein, the sufficiency of which is hereby acknowledged, the parties hereby agree as follows:

## **II. DEFINITIONS**

A. **"Cardholder Information"** shall mean any electronic record of TJX containing sensitive payment card authentication data (as defined in subsection (3) of the definition of Personal Information in this Assurance) collected from the magnetic stripe of a credit or debit card in connection with a Transaction and transmitted through or stored on TJX's authorization network.

B. **"Confidential Information"** shall mean the confidential and proprietary information of TJX, including, but not limited to, financial and technical information; information regarding its computer network, systems, programs, capabilities, and security; costs and pricing; ideas, designs, specifications, techniques, models, programs, manuals, documentation, processes, and know-how; information regarding Consumers; marketing plans; information regarding contracts; information regarding litigation; audit results; investigations; discounts and rebates; databases; innovations and copyrighted materials; and trade secrets.

C. **"Consumer"** shall mean any person, natural person, or individual who has purchased merchandise from TJX and whose personal information has been obtained and/or collected by TJX.

D. **"Effective Date"** shall mean the date on which TJX receives a copy of this Assurance duly executed in full by TJX and by each of the Attorneys General.

E. **"Personal Information"** shall mean any TJX record, whether in paper, electronic, or other form, containing nonpublic personal information about a Consumer collected in connection with a Transaction, including, but not limited to, any (1) Consumer's name, address, or telephone number, in conjunction with the Consumer's Social Security number, driver's license number, financial account number, or credit or debit card number; (2) Consumer's user name and passphrase used to authorize Transactions over the Internet; or (3) sensitive payment card authentication data, which shall mean (a) Primary Account Number ("PAN"); (b) cardholder name, card expiration date, service code, Social Security number, date and place of birth, or mother's maiden name, in conjunction with PAN; or (c) full magnetic stripe data, CVC2/CVV2/CID, or PIN or PIN block; or (4) other information required to be protected by state or federal law.

- F. **"Subsidiaries"** shall mean the wholly owned United States subsidiaries of TJX.
- G. **"TJX"** shall mean The TJX Companies, Inc. and its successors and assigns.
- H. **"Transaction"** shall mean a retail transaction in which a Consumer has purchased merchandise from TJX.

### **III. APPLICATION OF ASSURANCE**

The duties, responsibilities, burdens, and obligations undertaken in connection with this Assurance shall apply to TJX, its successors and assigns, and its officers and employees.

### **IV. INFORMATION SECURITY PROGRAM**

A. **General Provisions.** TJX shall implement and maintain a comprehensive Information Security Program that is reasonably designed to protect the security, confidentiality, and integrity of Personal Information, by no later than one hundred twenty (120) days after the Effective Date of this Assurance. Such program's content and implementation shall be fully documented and shall contain administrative, technical, and physical safeguards appropriate to the size and complexity of TJX's operations, the nature and scope of TJX's activities, and the sensitivity of the Personal Information, including:

1. The designation of an employee or employees to coordinate and be accountable for the Information Security Program.
2. 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: (a) employee training and management; (b) information systems,

including network and software design, information processing, storage, transmission, and disposal; and (c) prevention, detection, and response to attacks, intrusions, or other systems failures.

3. The design and implementation of reasonable safeguards to control the risks identified through risk assessment and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

4. The implementation and evaluation of any modification to TJX's Information Security Program, in light of the results of the testing and monitoring of any material changes to TJX's operations or business arrangements, or any other change in circumstances that TJX knows or has reason to know may have a material impact on the effectiveness of its Information Security Program.

B. Specific Provisions. The Attorneys General and TJX recognize that technology relating to information security is constantly changing and that current security procedures, software, hardware, and other security infrastructures may become obsolete or inadequate in the future. Without either party admitting that the following provisions alone amount to reasonable actions to protect Cardholder or Personal Information in the future, TJX shall, to the extent it has not already done so:

1. Replace or upgrade all Wired Equivalent Privacy ("WEP") based wireless systems in TJX's retail stores with wired systems or with Wi-Fi Protected Access ("WPA") or wireless systems at least as secure as WPA.

2. Not store or otherwise maintain on its network subsequent to the authorization process the full contents of the magnetic stripe of a credit or debit card, or of any single track of such a stripe, or the CVC2/CVV2/CID of any such card, or the PIN or PIN block

of any such card. TJX may retain a portion of the contents of the magnetic stripe of a credit or debit card on its network subsequent to the authorization process for a period of time for legitimate business, legal, or regulatory purpose(s), but if TJX does so, any such Cardholder Information must be securely stored in encrypted form, be accessed by essential personnel only, and retained for no longer than necessary to achieve the business, legal, or regulatory purpose.

3. Segment appropriately from the rest of the TJX computer system those network-based portions of the TJX computer system that store, process, or transmit Personal Information, including Cardholder Information, by firewalls, access controls, or other appropriate measures.

4. Implement security password management for the portions of the TJX computer system that store, process, or transmit Personal Information, including Cardholder Information, such as, where appropriate, strong passwords and, with respect to remote access to the network, two-factor authentication.

5. Implement security patching protocol for the portions of the TJX computer system that store, process, or transmit Cardholder Information.

6. Use Virtual Private Networks ("VPNs") or, where appropriate, encrypted transmissions, or other methods at least as secure as VPNs for transmission of Personal Information, including Cardholder Information, across open, public networks.

7. Install and maintain appropriately configured antivirus software on the portions of the TJX computer system that store, process, or transmit Personal Information, including Cardholder Information, and that are commonly affected by viruses.

8. Implement and maintain security monitoring tools, such as intrusion detection systems or other devices to track and monitor unauthorized access to the portions of

TJX's computer system that store, process, and transmit Personal Information, including Cardholder Information. Conduct regular testing or monitoring of the key systems and procedures used to protect Personal Information, including Cardholder Information.

9. Implement access control measures for the portions of TJX's computer system that store, process, and transmit Personal Information, including Cardholder Information. Access control measures include: (a) limiting physical and electronic access to Cardholder Information on a need-to-know basis; (b) assigning unique user IDs to persons with access to Cardholder Information; and (c) generating logs or other inventories of the user accounts on the portions of TJX's computer system used to store, process, or transmit Cardholder Information.

C. Confirmation of Compliance with Specific Provisions.

1. Within one hundred twenty (120) days following the Effective Date of this Assurance, TJX shall identify in writing the provision(s) in section IV.B of this Assurance with which it has achieved Compliance ("Compliance Certification") and/or shall submit a Compliance Plan (as defined below) with respect to any such provision(s) with which it has not achieved Compliance by that date. "Compliance" with such provisions shall mean (A) that TJX has taken the relevant measure(s) where technologically feasible and otherwise reasonable or has taken alternative measure(s) that alone or in the aggregate provide for substantially equivalent security, or (B) with respect to the application of subsections (4) and (9) of section IV.B to the point of sale terminals in TJX's retail stores, that TJX has developed a reasonable and appropriate plan to evaluate the technological and operational feasibility of such provisions. If TJX has not achieved Compliance with any such provisions by that date, it shall provide written notice to the Attorneys General identifying: (a) the provision(s) with which it has not yet achieved Compliance; (b) the reason(s) that Compliance has not yet been achieved or cannot be

achieved; and (c) a reasonable and appropriate plan and timetable for achieving Compliance with such provisions ("Compliance Plan"). After the submission by TJX of a Compliance Plan, and until such time as TJX submits a Compliance Certification with respect to each of the provision(s) identified in such Compliance Plan, TJX shall submit to the Attorneys General an updated Compliance Plan within the earlier of (i) thirty (30) business days after the expiration of the latest timetable specified in the most recent Compliance Plan that TJX provided to the Attorneys General (or at such later time as TJX and the Attorneys General may agree) or (ii) one hundred eighty (180) days after the date of the submission of the most recent Compliance Plan that TJX submitted to the Attorneys General (or at such later time as TJX and the Attorneys General may agree).

2. If the Attorneys General dispute that any Compliance Certification or any Compliance Plan satisfies TJX's obligations under section IV.B, the Attorneys General shall send TJX a written notice of the dispute within sixty (60) days following receipt of TJX's submission of the Compliance Certification or Compliance Plan in question, pursuant to the Meet and Confer provisions set forth in section VIII.H of this Assurance.

3. If TJX has submitted a Compliance Certification under section IV.C.1 and the Attorneys General have not disputed TJX's Compliance as set forth in section IV.C.2, then the provision(s) as to which TJX has certified Compliance in a Compliance Certification shall be fully and finally satisfied and TJX shall have no additional obligations with respect to such provision(s); however, TJX shall have the continuing responsibility, under section IV.A, to implement and maintain a comprehensive Information Security Program that is reasonably designed to protect the security, confidentiality, and integrity of Personal Information, as set forth therein.

4. Notwithstanding any other provision of this Assurance, TJX shall provide any documents under this section IV to the Attorney General for The Commonwealth of Massachusetts (the "Designated Representative Attorney General"), and the Designated Representative Attorney General shall treat such documents as exempt from disclosure under the relevant public records laws, pursuant to this Assurance or, as necessary, by employing other means to ensure confidentiality. These documents may contain sensitive information about the current state of TJX's security infrastructure and mechanisms, which could be harmful to TJX's ability to secure data if disclosed. The Designated Representative Attorney General may provide a copy of documents received under this section IV to any other of the Attorneys General upon request, so long as the laws of the State represented by each such requesting Attorney General treat such documents as exempt from disclosure under the relevant public records laws and such requesting Attorney General agrees to so treat such documents.

D. Security Breach Notification. TJX shall notify the Attorneys General, within ten (10) business days, or earlier if required by applicable law, after mailing notice or providing substitute notice to resident Consumers pursuant to the requirements of any of the States' security breach notification laws, that TJX or any of its Subsidiaries provided such Consumer notice and shall in such notice to the Attorneys General include the following information to the extent then available: (a) the type of personal information accessed or acquired as a result of the breach; (b) the approximate date(s) on which the breach occurred; (c) a brief description of the nature of the breach; (d) a brief description of the steps TJX has taken or is planning to take to protect Consumers, if any, affected by the breach; (e) whether other law enforcement agencies have been notified and, if so, the contact information for such agencies; (f) TJX's plan to address any Consumer injuries arising from the breach; and (g) a copy or representative example of the

notice provided to Consumers. This provision shall expire three (3) years after the Effective Date of this Assurance. Nothing in this provision alters any obligation under any state statute or regulation governing security breach notification.

#### **V. PAYMENT CARD SYSTEM PILOT PROGRAMS AND ENHANCEMENTS**

The Attorneys General and TJX believe that the security of Cardholder Information collected in connection with retail transactions is an important priority. Protecting Cardholder Information is a dynamic challenge, because as security technologies available to retailers evolve, criminals attempt to develop more sophisticated ways of trying to circumvent such technologies. The Attorneys General and TJX therefore agree that possible improvements within the payment card system could aid the protection of consumers. To further that goal, TJX agrees as follows:

A. Pilot Programs. TJX will notify Visa and MasterCard in the United States and its acquiring bank(s) in the United States, simultaneous with the execution of this Assurance, that TJX desires to participate in pilot programs for testing new security-related payment card technology, such as the chip-and-PIN technology that is used in many other countries. TJX will participate in such program(s), if invited to do so, within two (2) years following the Effective Date of this Assurance, provided that any new security-related payment card technology and the terms and conditions of such participation are considered in good faith by TJX to be feasible and reasonable.

B. New Encryption Technologies. TJX will take steps over the one hundred eighty (180) days following the Effective Date of this Assurance, to encourage the development of new technologies within the Payment Card Industry to encrypt Cardholder Information during some or all of the bank authorization process with a goal of achieving "end-to-end" encryption of

Cardholder Information (i.e, from PIN pad to acquiring bank). Such methods may include but are not limited to encouraging the development of new technologies and seeking the cooperation of TJX's acquiring bank(s) in the United States and other appropriate third parties. TJX will provide the Attorneys General, within one hundred eighty (180) days following the Effective Date, with a report specifying its progress in this effort.

## **VI. SETTLEMENT COMPLIANCE ASSESSMENT**

A. Report. TJX shall obtain an assessment and report from a third-party professional ("Third-Party Assessor"), using procedures and standards generally accepted in the profession ("Third-Party Assessment"), by no later than one hundred eighty (180) days after the Effective Date of this Assurance, and biennially thereafter during the term of this Assurance. The report shall:

1. Set forth the specific administrative, technical, and physical safeguards that TJX and its Subsidiaries have implemented and maintained during the reporting period.
2. Explain how such safeguards are appropriate in light of TJX's size and complexity, the nature and scope of TJX's activities, and the sensitivity of the Personal Information collected from or about Consumers.
3. Explain how the safeguards that have been implemented meet the protections required by this Assurance.
4. Certify that TJX's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of Personal Information is protected and, for biennial reports, has been so operated throughout the reporting period.

B. Third-Party Assessor Qualifications. The Third-Party Assessor shall be a person qualified as a Certified Information System Security Professional ("CISSP") or as a Certified Information Systems Auditor ("CISA"), or a similarly qualified person or organization with at least five (5) years of experience evaluating the effectiveness of computer systems or information system security.

C. Supporting Documentation. TJX shall provide to the Third-Party Assessor as part of the Third-Party Assessment the following materials that are within TJX's possession, custody, and control:

1. TJX's most recently completed annual Report of Compliance ("ROC") with the Payment Card Industry's Data Security Standard ("PCI DSS") (or such other standard as subsequently may be adopted by Visa and/or MasterCard as the standard to be used in preparing a ROC), as prepared by a Qualified Security Assessor or an Approved Scanning Vendor (or such other person as subsequently may be accepted by Visa and/or MasterCard as the person authorized to prepare a ROC).

2. Any final written assessment of information technology internal controls for the portions of TJX's computer system that store, process, or transmit Personal Information prepared by TJX's independent registered public accounting firm and submitted to TJX within the then preceding year as part of such firm's audit of TJX's financial statements.

D. Submission to Attorneys General.

1. A copy of the first Third-Party Assessment shall be provided, within one hundred eighty (180) days following the Effective Date of this Assurance, by TJX to the Designated Representative Attorney General, and the Designated Representative Attorney General shall treat such documents as exempt from disclosure under the relevant public records

laws, pursuant to this Assurance or, as necessary, by employing other means to ensure confidentiality.

2. All subsequent Third-Party Assessments shall be retained by TJX, and upon request of any of the Attorneys General, shall be provided to the Designated Representative Attorney General, as per the preceding subsection (1), within ten (10) business days following such request.

3. The Designated Representative Attorney General may provide a copy of any Third-Party Assessment received from TJX under the preceding two subsections (1) and (2) to any other of the Attorneys General upon request, so long as the laws of the State represented by each such requesting Attorney General treat such Third-Party Assessment as exempt from disclosure under the relevant public records laws and such requesting Attorney General agrees to so treat such Third-Party Assessment.

E. FTC Coordination. The Attorneys General acknowledge that TJX is subject to a Decision and Order issued by the United States Federal Trade Commission ("FTC"), FTC Docket No. C-4227 and File No. 072-3055, relating to the Intrusion (the "FTC Order"), under which TJX will obtain biennial assessments and reports from a third-party professional and provide to the FTC the initial report and, upon request, the subsequent reports. The Attorneys General agree that, notwithstanding any other provision herein, the same assessments and reports undertaken and prepared pursuant to section II of the FTC Order shall be sufficient to satisfy the requirements of the Third-Party Assessments contemplated under section VI.A of this Assurance and the other requirements of sections VI.A-C. To coordinate the timetables for the assessments and reports required under the respective documents, and notwithstanding any other provision of this Assurance, the Attorneys General agree that the first assessment and report obtained by TJX

pursuant to the FTC Order, whenever prepared (whether before or after the Effective Date of this Assurance) shall constitute the first Third-Party Assessment under this Assurance, and that the assessments conducted and reports prepared thereafter on a biennial basis under section II of the FTC Order shall constitute the Third-Party Assessments required under section VI.A of this Assurance on a biennial basis for twenty (20) years following entry of this Assurance. The requirements of sections VI.A-C of this Assurance shall expire upon the conclusion of the final assessment and report obtained by TJX under section II of the FTC Order, unless they have expired at an earlier date pursuant to the terms of this Assurance.

## **VII. MONETARY PAYMENTS**

A. Payment to the States. TJX shall pay to the States, collectively, a total amount of \$9.75 million, by electronic fund transfer to the Office of the Massachusetts Attorney General, to be distributed to the States in a manner agreed to by the States. This amount comprises:

1. Settlement Amount. \$5.5 million to be distributed as designated by and in the sole discretion of the Attorneys General as part of the resolution of their respective investigations under the state consumer protection laws regarding the Subject Matter of this Assurance. Said payment shall be used by the Attorneys General to fund or assist in funding, consumer education, outreach, prevention or monitoring programs, consumer protection enforcement, litigation, local consumer aid funds, consumer protection enforcement funds and public protection funds including without limitation, developing, implementing or enforcing data security protection programs and protecting consumers' personally identifiable information, or for other uses permitted by state law, at the sole discretion of each Attorney General;

2. Data Security Fund. \$2.5 million payable to the Massachusetts Office of the Attorney General, to be distributed as designated by and in the sole discretion of the

Attorneys General for the purposes of initiatives by the States to research the benefits of data security technology and develop best practices, protocols, policies or model legislation or regulations concerning data security or data security technology; and develop and implement programs, education and outreach for consumers with respect to data security; for other efforts to examine data security matters and to protect consumer privacy; and for other uses permitted by state law. This payment (\$2.5 million) to the Data Security Fund shall be held in trust by the Massachusetts Office of the Attorney General for the benefit of the Attorneys General of the States consistent with this paragraph VII.A.2. Distributions from the Data Security Fund may come from interest or principal and shall be made only pursuant to instructions from a majority of the five State Attorneys General that comprise the Data Security Fund Committee, namely, the Attorneys General of California, Florida, Massachusetts, Pennsylvania and Tennessee; and,

3. Attorney Fees and Costs. \$1.75 million in fees and costs associated with the States' investigation. Said payment shall be used by the States for attorneys' fees and other costs of investigation and litigation, or to be placed in, or applied to, the consumer protection enforcement fund, including future consumer protection enforcement, consumer education, litigation or local consumer aid fund or revolving fund, used to defray the costs of the inquiry leading hereto or for other uses permitted by state law.

B. No Tax Characterization. Nothing in this Assurance constitutes an agreement by the Attorneys General concerning the characterization of the amounts paid hereunder for purposes of any proceeding under the Internal Revenue Code or any state tax laws.

### **VIII. ENFORCEMENT**

A. Enforceable Under State Law. TJX and the Attorneys General agree that this Assurance constitutes a legally enforceable agreement. This Assurance and the rights and

obligations of the parties hereunder shall be governed within each of the respective States by the laws of such States in which any enforcement of this Assurance or any action to determine the rights and obligations hereunder is attempted.

B. Enforceable By Parties Only. This Assurance may be enforced only by the parties hereto. Nothing in this Assurance shall provide any rights to or permit any person or entity not a party hereto, including any state or attorney general not a party hereto, to enforce any provision of this Assurance. No person or entity not a signatory hereto is a third-party beneficiary of this Assurance. Nothing in this Assurance shall be construed to affect, limit, alter, or assist any private right of action that a consumer or other third party may hold against TJX.

C. Application. This Assurance shall be binding on TJX, its successors and assigns, and its officers and employees. Notwithstanding any other provision in this Assurance, the obligations herein undertaken by TJX shall not apply to any act or omission by TJX within any state that has not signed this Assurance.

D. Duration. The obligations and other provisions of this Assurance shall expire at the conclusion of the twenty (20) year period after the Effective Date of this Assurance, unless they have expired at an earlier date pursuant to their specific terms.

E. Modifications or Amendments. This Assurance may be modified or amended solely in writing by TJX and the Attorneys General for the States to be bound by the amendment or modification in question. If TJX believes that modification or amendment of this Assurance becomes warranted or appropriate for any reason, including, but not limited to, changes in the risks to the security, confidentiality, and integrity of Personal Information or to the relevant security procedures, practices, or tools used to protect against those risks, TJX may submit to the Attorneys General the proposed written modification or amendment and, if TJX considers it

appropriate, a statement from an independent expert supporting the proposed modification or amendment. Should the Attorneys General object to the modification or amendment, they shall, within sixty (60) days after delivery of TJX's written modification or amendment notice, initiate the Meet and Confer process as set forth in section VIII.H below. If the objection is not resolved through the Meet and Confer process, then (i) the Attorney General reserves the right to seek to enforce the terms of this Assurance notwithstanding the modification requested by TJX; and (ii) TJX reserves the right to modify or amend the terms of this Assurance in the appropriate state court with jurisdiction.

F. Monitoring. Upon the written request of the Attorneys General, TJX agrees to provide responsive, non-privileged information, books, records, documents, or testimony (formal or informal) to the Attorneys General for the purpose of monitoring TJX's compliance with this Assurance. TJX shall make the requested information available, within sixty (60) calendar days of the request, at the office of the Designated Representative Attorney General, or at such other time and/or place as is mutually agreed to in writing by TJX and the requesting Attorneys General. This section shall in no way limit (1) any right of the Attorneys General to obtain documents, records, testimony, or other information pursuant to any law, regulation, or rule, or (2) the effect of the provisions set forth in sections IV.C and VI.D of this Assurance. The parties agree that any dispute arising under this section shall be resolved through the Meet and Confer process set forth in section VIII.H below.

G. Conflicts. Nothing in this Assurance shall be construed as preventing or exempting TJX from complying with any law, rule, or regulation, nor shall any of the provisions of this Assurance be deemed to authorize or require TJX to engage in any acts or practices prohibited by such law, rule, or regulation.

