

1 as the “Attorneys General”), acting pursuant to their respective consumer protection statutes
2 on behalf of their respective states (the “States”).³

3
4 **I. RECITALS**

5 **WHEREAS**, as TJX publicly announced on January 17, 2007, and February 21, 2007,
6 a person or persons (such intruder or intruders referred to collectively as the “Intruders”)
7 gained unauthorized access during periods in 2005 and 2006 to portions of TJX's computer
8 system that centrally process and store information from payment card and other transactions

9
10 ³ ALABAMA – Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19-1 *et seq.*; ARIZONA –
11 Arizona Consumer Fraud Act, Ariz. Rev. Stat. §§ 44-152[1] *et seq.*; ARKANSAS – Arkansas Deceptive Trade
12 Practices Act, Ark. Code Ann. §§ 4-88-101 *et seq.*; CALIFORNIA – Cal. Bus. & Prof. Code §§ 17200 *et seq.*;
13 COLORADO – Colorado Consumer Protection Act, Colo. Rev. Stat. §§ 6-1-101 *et seq.*; CONNECTICUT –
14 Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. §§ 42-110a *et seq.*; DELAWARE – Delaware
15 Consumer Fraud Act, Del. Code Ann. tit. 6, §§ 2511-27 *et seq.*; FLORIDA – Florida Deceptive and Unfair Trade
16 Practices Act, Fla. Stat. Ann. §§ 501.201 *et seq.*; HAWAII – Haw. Rev. Stat. §§ 480-1 *et seq.*; IDAHO – Idaho
17 Consumer Protection Act, Idaho Code §§ 48.601 *et seq.*; ILLINOIS – Illinois Consumer Fraud and Deceptive
18 Business Practices Act, 815 Ill. Comp. Stat. §§ 505/1 *et seq.*; IOWA – Iowa Consumer Fraud Act, Iowa Code §
19 714.16; LOUISIANA – Louisiana Unfair Trade Practices and Consumer Protection Act, LSA-R.S. 51:1401, *et*
20 *seq.*; MAINE – Maine Unfair Trade Practices Act, Me. Rev. Stat. Ann. tit. 5, §§ 210 *et seq.*; MARYLAND –
21 Maryland Consumer Protection Act, Md. Code Ann. Com. Law §§ 13-101 *et seq.*; MASSACHUSETTS –
22 Massachusetts Consumer Protection Act, Mass. Gen. Laws ch. 93A, §§ 1 *et seq.*; MICHIGAN – Michigan
23 Consumer Protection Act, Mich. Comp. Laws Ann. §§ 445.901 *et seq.*; MISSISSIPPI – Mississippi Consumer
24 Protection Act, Miss. Code Ann. §§ 75-24-1 *et seq.*; MISSOURI – Missouri Merchandising Practices Act, Mo.
25 Rev. Stat. §§ 407.010 *et seq.*; MONTANA – Montana Unfair Trade Practices and Consumer Protection Act,
26 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.*

1 at certain of TJX's retail stores (such intrusion or intrusions referred to collectively as the
2 "Intrusion");

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

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

10 **WHEREAS**, a multi-state group of Attorneys General conducted an extensive review
11 and inquiry of TJX's data security policies and procedures in place when the Intruders
12 unlawfully gained access to consumer information and also reviewed TJX's policies and
13 procedures after the discovery of the Intrusion (the "Investigation"). The inquiry considered,
14 among other things: TJX's data encryption systems; data segmentation systems; data
15 protection systems; and intrusion detection systems (the "Subject Matter");

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

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

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

26 **NOW, THEREFORE**, in consideration of their mutual agreements to the terms of this

1 Assurance, and such other consideration as described herein, the sufficiency of which is hereby
2 acknowledged, the parties hereby agree as follows:

3 II. DEFINITIONS

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

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

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

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

21 E. **“Personal Information”** shall mean any TJX record, whether in paper,
22 electronic, or other form, containing nonpublic personal information about a Consumer
23 collected in connection with a Transaction, including, but not limited to, any (1) Consumer's
24 name, address, or telephone number, in conjunction with the Consumer's Social Security
25 number, driver's license number, financial account number, or credit or debit card number;
26 (2) Consumer's user name and passphrase used to authorize Transactions over the Internet; or

1 (3) sensitive payment card authentication data, which shall mean (a) Primary Account Number
2 (“PAN”); (b) cardholder name, card expiration date, service code, Social Security number, date
3 and place of birth, or mother's maiden name, in conjunction with PAN; or (c) full magnetic
4 stripe data, CVC2/CVV2/CID, or PIN or PIN block; or (4) other information required to be
5 protected by state or federal law.

6 F. “**Subsidiaries**” shall mean the wholly owned United States subsidiaries of TJX.

7 G. “**TJX**” shall mean The TJX Companies, Inc. and its successors and assigns.

8 H. “**Transaction**” shall mean a retail transaction in which a Consumer has
9 purchased merchandise from TJX.

10 III. APPLICATION OF ASSURANCE

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

13 IV. INFORMATION SECURITY PROGRAM

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

21 1. The designation of an employee or employees to coordinate and be
22 accountable for the Information Security Program.

23 2. The identification of material internal and external risks to the security,
24 confidentiality, and integrity of Personal Information that could result in the unauthorized
25 disclosure, misuse, loss, alteration, destruction, or other compromise of such information and
26 assessment of the sufficiency of any safeguards in place to control these risks. At a minimum,

1 this risk assessment should include consideration of risks in each area of relevant operation,
2 including, but not limited to: (a) employee training and management; (b) information systems,
3 including network and software design, information processing, storage, transmission, and
4 disposal; and (c) prevention, detection, and response to attacks, intrusions, or other systems
5 failures.

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

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

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

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

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

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

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

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

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

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

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

22 8. Implement and maintain security monitoring tools, such as intrusion
23 detection systems or other devices to track and monitor unauthorized access to the portions of
24 TJX's computer system that store, process, and transmit Personal Information, including
25 Cardholder Information. Conduct regular testing or monitoring of the key systems and
26 procedures used to protect Personal Information, including Cardholder Information.

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

8 C. Confirmation of Compliance with Specific Provisions.

9 1. Within one hundred twenty (120) days following the Effective Date of
10 this Assurance, TJX shall identify in writing the provision(s) in section IV.B of this Assurance
11 with which it has achieved Compliance ("Compliance Certification") and/or shall submit a
12 Compliance Plan (as defined below) with respect to any such provision(s) with which it has not
13 achieved Compliance by that date. "Compliance" with such provisions shall mean (A) that
14 TJX has taken the relevant measure(s) where technologically feasible and otherwise reasonable
15 or has taken alternative measure(s) that alone or in the aggregate provide for substantially
16 equivalent security, or (B) with respect to the application of subsections (4) and (9) of section
17 IV.B to the point of sale terminals in TJX's retail stores, that TJX has developed a reasonable
18 and appropriate plan to evaluate the technological and operational feasibility of such
19 provisions. If TJX has not achieved Compliance with any such provisions by that date, it shall
20 provide written notice to the Attorneys General identifying: (a) the provision(s) with which it
21 has not yet achieved Compliance; (b) the reason(s) that Compliance has not yet been achieved
22 or cannot be achieved; and (c) a reasonable and appropriate plan and timetable for achieving
23 Compliance with such provisions ("Compliance Plan"). After the submission by TJX of a
24 Compliance Plan, and until such time as TJX submits a Compliance Certification with respect
25 to each of the provision(s) identified in such Compliance Plan, TJX shall submit to the
26 Attorneys General an updated Compliance Plan within the earlier of (i) thirty (30) business

1 days after the expiration of the latest timetable specified in the most recent Compliance Plan
2 that TJX provided to the Attorneys General (or at such later time as TJX and the Attorneys
3 General may agree) or (ii) one hundred eighty (180) days after the date of the submission of
4 the most recent Compliance Plan that TJX submitted to the Attorneys General (or at such later
5 time as TJX and the Attorneys General may agree).

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

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

19 4. Notwithstanding any other provision of this Assurance, TJX shall
20 provide any documents under this section IV to the Attorney General for The Commonwealth
21 of Massachusetts (the "Designated Representative Attorney General"), and the Designated
22 Representative Attorney General shall treat such documents as exempt from disclosure under
23 the relevant public records laws, pursuant to this Assurance or, as necessary, by employing
24 other means to ensure confidentiality. These documents may contain sensitive information
25 about the current state of TJX's security infrastructure and mechanisms, which could be
26 harmful to TJX's ability to secure data if disclosed. The Designated Representative Attorney

