

Litigation

Privacy & Data  
Protection

Global Sourcing

July 1, 2009

---

## TJ Maxx Settlement Requires Creation of Information Security Program and Funding of State Data Protection and Prosecution Efforts

by Tara M. Desautels and John L. Nicholson

---

*Last week, TJX (the parent company of TJ Maxx and Marshalls) settled an action with 41 state Attorneys General arising out of a 2006 security breach affecting millions of credit cardholders. An information security program required by the settlement covers a significantly broader collection of information than the Payment Card Industry Data Security Standards (PCI DSS) and may serve as a de facto minimum standard for information security compliance. Also, the settlement's funding of a Data Security Trust Fund anticipates future enforcement activities by the states and creates a precedent for states to look to future breaches as a source of continued funding.*

---

### Background

On December 18, 2006, TJX initiated an investigation after discovering suspicious software on its computer systems. That investigation led to the shocking discovery that for 18 months prior, hackers had stolen information dating as far back as 2002 from more than 94 million credit and debit cards. TJX reported the security breach to U.S. state and federal authorities and government authorities in Canada, France, and the United Kingdom. The related investigation initiated by a group of state Attorneys General revealed that TJX had failed to address the security flaws identified in a 2004 internal audit that revealed vulnerabilities concerning firewalls, encrypting cardholder data, uploading antivirus software, and regularly testing security systems.<sup>1</sup> Litigation immediately followed, as did evidence that TJX was not compliant with nine of the twelve PCI DSS requirements covering encryption, access controls and firewalls.<sup>2</sup>

<sup>1</sup> See June 23, 2009 Press Release, "Brown Forces Parent Company of TJ Maxx and Marshall's to Block Credit Card Hackers," Office of the Attorney General, State of California.

<sup>2</sup> See Brenner, "Don't blame PCI DSS for TJX troubles, IT pros say," SearchSecurity.com, Nov. 5, 2007, at [http://searchsecurity.techtarget.com/news/article/0,289142,sid14\\_qci1280854,00.html](http://searchsecurity.techtarget.com/news/article/0,289142,sid14_qci1280854,00.html) (last visited June 29, 2009).

On June 23, 2009, TJX settled the action with 41 state Attorneys General for \$9.75 million.<sup>3</sup> This settlement agreement follows the 2007 settlements of the consolidated consumer class action<sup>4</sup> and an action initiated by Visa, Inc.<sup>5</sup> But unlike the prior settlement agreements, in addition to monetary payments, the June 23 agreement requires TJX to implement a comprehensive “Information Security Program” and fund future state data protection efforts as part of “the most comprehensive relief achieved to date following a data breach investigation.”<sup>6</sup>

## The Terms

The settlement agreement between TJX and the states (known as the “Assurance”) breaks down the \$9.75 million payments into cost reimbursement and future data protection funding:<sup>7</sup>

- \$5.5 million will be dedicated to data protection and consumer protection efforts by the states;
- \$1.75 million will reimburse the states for their costs and fees incurred in the investigation; and
- \$2.5 million will fund a “Data Security Trust Fund” to be used by the state Attorneys General to “advance enforcement efforts and policy development in the field of data security and protecting consumers’ personal information.”

Within the next 120 days, TJX must also “implement and maintain a comprehensive Information Security Program that is reasonably designed to protect the security, confidentiality, and integrity of Personal Information.” The Assurance uses a definition of Personal Information that is generally consistent with numerous state data breach notification laws and is significantly broader than the definition of “cardholder data” used by the PCI DSS. According to the Assurance,

“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,



<sup>3</sup> The participating states are: Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Hawaii, 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.

<sup>4</sup> On November 14, 2007, parties reached a proposed settlement agreement in the Consolidated Consumer Class Action approved by the United States District Court for the District of Massachusetts on September 2, 2008. The settlement agreement provided for compensation to injured consumers through vouchers or checks-in-lieu, credit monitoring, identity theft insurance, reimbursements, a one-time sale event, and over \$6.5 million in attorneys fees and costs. *In re TJX Companies Retail Security Breach Litigation*, United States District Court, District of Massachusetts, Civil Action No. 07-10162, MDL Docket No. 1838, Dkt. 368.

<sup>5</sup> In the November 30, 2007 settlement agreement with Visa Inc., TJX agreed to provide U.S. credit card issuers up to \$40.9 million in alternative recovery payments. In a December 20, 2007 press release, TJX announced over 95% of the affected institutions accepted the proposal.

<sup>6</sup> See June 23, 2009 Press Release, “Attorney General Martha Coakley Announces Multi-State Settlement with the TJX Companies, Inc., Over Massive Data Breach,” Office of the Attorney General, State of Massachusetts.

<sup>7</sup> See *id.* and accompanying Assurance, *In the Matter of: The TJX Companies, Inc.*, at [http://www.mass.gov/?pageID=cagopressrelease&L=1&L0=Home&sid=Cago&b=pressrelease&f=2009\\_06\\_23\\_tjx\\_settlement&csid=Cago#materials](http://www.mass.gov/?pageID=cagopressrelease&L=1&L0=Home&sid=Cago&b=pressrelease&f=2009_06_23_tjx_settlement&csid=Cago#materials) (last visited June 29, 2009).

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.<sup>8</sup>

By contrast, under the PCI DSS, cardholder data is (1) the PAN and (2) the cardholder's name, the card expiration date and the service code, but only to the extent associated with the PAN. The Assurance also defines Cardholder Data in a manner consistent with the PCI DSS, but most of TJX's specific requirements under the Assurance are express as covering "Personal Information, including Cardholder Data." It is this structure that makes the information security obligations under the Assurance so much broader than those required solely by the PCI DSS.

The Assurance specifies that TJX's Information Security Program must include – at a minimum – certain administrative, technical, and physical safeguards that are listed in the Assurance. Although the information covered by the Assurance is broader than that required by PCI DSS, for the purposes of comparison, each of the Assurance's requirements is mapped against the relevant PCI DSS requirement(s) in the following list:

Assurance Requirement	PCI DSS Requirement
1. The designation of an employee or employees to coordinate and be accountable for the Information Security Program;	PCI DSS 12.5 requires a company to "Verify the formal assignment of information security to a Chief Security Officer or other security knowledgeable member of management."
2. The identification of material internal and external risks to the security, confidentiality and integrity of Personal Information that could result in 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. The risk assessment should consider 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 system failures;	PCI DSS Requirement 12 requires companies to "Maintain a policy that addresses information security for employees and contractors." As part of that requirement, PCI DSS 12.1 requires companies to "Establish, publish, maintain, and disseminate a security policy that accomplishes the following: ... Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment."
3. The design and implementation of reasonable safeguards to control the identified risks through risk assessment and regular testing and monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;	PCI DSS 12.2 requires companies to "Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures)." PCI DSS 12.6 requires an annual (or more frequent) formal security awareness program for employees, and PCI DSS 12.9 requires the implementation of an incident response plan, including for alerts from intrusion detection systems, intrusion-prevention systems and file-integrity monitoring systems.

<sup>8</sup> *Id.* at Assurance, *In the Matter of: The TJX Companies, Inc.*, p.4.

- |  |   |
|--|---|
| <p>4. The implementation and evaluation of any modification to the Information Security Program, in light of the results of the testing and monitoring of any material changes to TJX's operation 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 the Information Security Program.</p> | <p>As part of the maintenance of the security policy required by PCI DSS 12.1, PCI DSS 12.1.3 requires companies to include a "review at least once a year and updates when the environment changes."</p> |
|--|---|

Because of the increased breadth of the information covered by the Information Security Program, items 2-4 in the preceding table may require TJX to cover information and operations previously considered outside of the coverage of its PCI DSS program.

The Assurance further requires that TJX implement the following security provisions (to the extent it has not already done so). As with the preceding table, for the purposes of comparison, each of the Assurance's requirements is mapped against the relevant PCI DSS requirement(s):

<b>Assurance Requirement</b>	<b>PCI DSS Requirement</b>
<p>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.</p>	<p>PCI DSS 2.1.1 requires a company to "ensure that all wireless networks implement strong encryption mechanisms (for example, AES)" and that "Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2)...".</p>
<p>2. Not store or otherwise maintain on its network subsequent to the authorization process the full contents of magnetic stripe of a credit or debit card, or of any single track of such a stripe, or the CVC2/CVV2/CID, or the PIN or PIN block of any 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 any such Cardholder Information must be securely stored in encrypted form, be accessible only to essential personnel, and retained for no longer than necessary to achieve the business, legal or regulatory purpose;</p>	<p>These requirements are covered by PCI DSS 3.2.1 ("Do not store the full contents of any track from the magnetic stripe ..."), 3.2.2 ("Do not store the card-verification code or value ... used to verify card-not-present transactions."), 3.2.3 ("Do not store the personal identification number (PIN) of the encrypted PIN block."). The encryption, storage and access requirements are covered in PCI DSS 3.1 and 3.4 – 3.6.</p>
<p>3. Segment the network-based portions of the TJX computer system that store, process, or transmit personal information from the rest of the TJX computer system through firewalls, access controls, or other appropriate measures;</p>	<p>These requirements are covered by, among others, PCI DSS 1.2 ("Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.") and 1.3 ("Prohibit direct public access between the Internet and any system component in the cardholder data environment.").</p>
<p>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</p>	<p>PCI DSS 8.2 requires "In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: password or passphrase; two-factor authentication..." PCI DSS 8.3 requires companies to</p>

- |   |  |
|---|--|
| <p>to remote access to the network, two-factor authentication;</p>  | <p>“Incorporate two-factor authentication for remote access ... to the network by employees, administrators, and third parties.”</p>   |
| <p>5. Implement security patching protocols for the portions of the TJX computer system that store, process or transmit Cardholder Information;</p>   | <p>PCI DSS 6.1 requires companies to “Ensure that all system components and software have the latest vendor-supplied security patches installed.” The PCI DSS goes further to also require all critical security patches to be installed within one month of release.</p>  |
| <p>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;</p>   | <p>PCI DSS 4.1 requires the use of “strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.”</p>  |
| <p>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;</p>  | <p>This requirement is covered by PCI DSS 5.1 (“Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers)”), 5.1.1 (“Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.”) and 5.2 (“Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.”)</p>  |
| <p>8. Implement and maintain security monitoring tools such as intrusion detection systems and other devices to track and monitor unauthorized access to the portions of TJX’s computer systems 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; and</p>  | <p>PCI DSS Requirement 10 requires companies to “Track and monitor all access to network resources and cardholder data.” Requirement 11 requires companies to “Regularly test security systems and processing.”</p>  |
| <p>9. Implement Personal Information 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.</p> | <p>PCI DSS section 9 covers physical security with regard to cardholder data, including PCI DSS 9.1 (“Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.”), 9.6 (“Physically secure all paper and electronic media that contain cardholder data.”), and 9.9 (“Maintain strict control over the storage and accessibility of all media and conduct media inventories at least annually.”)</p> <p>PCI DSS 7.1 requires companies to “Limit access to system components and cardholder data to only those individuals whose job requires such access.”</p> <p>Assignment of user IDs is covered by PCI DSS 8.1 (“Assign all users a unique ID before allowing them to access system components</p> |

or cardholder data.”), and, as noted above, PCI DSS Requirement 10 requires companies to “Track and monitor all access to network resources and cardholder data.”

The Attorneys General will issue TJX a compliance certification only after TJX provides satisfactory documentation of its implementation of all of these security measures. Given the breadth of the definition of “Personal Information” used in the Assurance, it seems unlikely that a successful audit by a PCI DSS Qualified Security Assessor, by itself, would satisfy the requirements. Under the Assurance, TJX will be required to obtain a CISSP (Certified Information System Security Professional) or CISA (Certified Information Systems Auditor) third-party assessment and report of its security and compliance efforts within the next 180 days and bi-annually thereafter for the next 20 years. Since TJX’s regular PCI DSS audits may not be sufficient, this could represent a significant additional cost to TJX. If TJX has outsourced any functions to third parties that must be covered by such an audit, TJX may need to determine whether the contracts with those third parties will permit the level of detailed investigation required. In some cases, TJX may be caught between the “rock” of the state Attorneys General and the “hard place” of a supplier that does not want to permit auditing of its services (except in exchange for a significant payment).

In addition, if TJX discovers a future security breach, it must also notify the Attorneys General within 10 business days (or earlier if required by applicable law) after mailing notice to resident consumers pursuant to each of the affected states’ security breach notification laws.

Finally, TJX has agreed to participate in substantial payment card system pilot programs and security enhancements. For the next two years, TJX will, if invited, participate in pilot programs testing new security-related payment card technology, such as “chip-and-PIN” technology. TJX will also take proactive steps within the next 180 days to encourage the development of new security-based technologies within the payment card industry to encrypt cardholder information.

### What the TJX Settlement Means for You

The TJX Settlement is a warning. All companies maintaining personal information that meets the definition used in the Assurance (*i.e.*, name, address or telephone number in combination with Social Security Numbers, drivers license numbers, credit/debit card account numbers or other similar account/identification numbers, as well as the information specifically covered by the PCI DSS, in paper, electronic or other forms) – whether for consumers, employees, or third-parties – must implement a secure information protection program with regular auditing procedures. In setting up such a program, the specifics set forth in the TJX Assurance and the PCI DSS can serve as a guide, but companies must tailor their program to their particular circumstances.

Companies that have outsourced any data processing to third parties should review the security obligations under those contracts to determine whether the service provider is obligated to meet requirements that comply with the Assurance and whether the company is permitted to audit the service provider’s compliance. Companies in the process of negotiating (or renegotiating) such agreements should include these security and audit obligations in the terms of the contract.

Companies should also keep in mind that the states now have an additional \$8 million among them allocated specifically to advance data and consumer protection efforts – which means increased enforcement of state data breach notification and consumer protection laws. Once the Data Security Trust Fund is established, companies can expect states to use such increased enforcement efforts to secure future funding, which not only makes state Attorneys General look proactive to their constituents, but does

so in a manner that pays for itself. Payments into the Fund may become the rule rather than the exception.

In the world of security breaches, the question is not, "Will you have a breach?" It is, "When will you have one?" When you discover that inevitable security breach, your company must have the appropriate incident response procedures in place, along with certified evidence of all of your regular, prior, and audited compliance efforts. The TJX Settlement, including the broad definition of information to be covered by a company's information security program, may now serve as the baseline for such programs, and companies that fall short of meeting these obligations may fare far worse than TJX.

---

For further information, please contact:

Deborah S. Thoren-Peden  
Los Angeles  
+1.213.488.7320  
deborah.thoren-peden@pillsburylaw.com

Tara M. Desautels  
San Francisco  
+1.415.983.1311  
tara.desautels@pillsburylaw.com

John L. Nicholson  
Washington, DC  
+1.202.663.8269  
john.nicholson@pillsburylaw.com

Catherine D. Meyer  
Los Angeles  
+1.213.488.7362  
catherine.meyer@pillsburylaw.com

This publication is issued periodically to keep Pillsbury Winthrop Shaw Pittman LLP clients and other interested parties informed of current legal developments that may affect or otherwise be of interest to them. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.

© 2009 Pillsbury Winthrop Shaw Pittman LLP. All Rights Reserved.