

**OFFICE OF THE PRIVACY COMMISSIONER OF CANADA  
AND  
OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER  
OF ALBERTA**

**Report of an Investigation into the  
Security, Collection and Retention of Personal Information**

**September 24, 2007**

**TJX Companies Inc. /Winners Merchant International L.P.**

## **Background**

1. On January 17, 2007, the Office of the Privacy Commissioner of Canada (OPC) and the Office of the Information and Privacy Commissioner of Alberta (AB OIPC) were notified by TJX<sup>1</sup> and by Visa that TJX had suffered a network computer intrusion affecting the personal information of an estimated 45 million payment cards in Canada, the United States, Puerto Rico, the United Kingdom and Ireland. This notice was received the same day that TJX issued a press release about the breach of customer data.
2. We elected to conduct a joint investigation to determine whether the incident represented a contravention of the *Personal Information Protection and Electronic Documents Act* (“PIPEDA”) and/or the *Personal Information Protection Act* (“PIPA”).

## **Overview**

3. TJX/WMI’s experience illustrates how maintaining custody of large amounts of sensitive information can be a liability, particularly if the information does not meet any legitimate purpose or if the retention period is longer than necessary. Although the duty to safeguard personal information exists independent of the requirement to limit collection to the extent reasonable, the two principles are harmonious. Collecting and retaining excessive personal information creates an unnecessary security burden. Thus, organizations should collect only the minimum amount of information necessary for the stated purposes and retain it only for as long as necessary, while keeping it secure.
4. Every organization in Canada is subject to the safeguarding principles established in PIPEDA or in provincial privacy legislation to protect personal information. It is critical that organizations not only consider multiple layers of security, but also that they keep abreast of technological advances to ensure that their security safeguards have not become outdated and easily defeated. It is imperative that they take a “holistic” view of their personal information management, to actively monitor their safeguards with a view to maintaining a robust system.

---

<sup>1</sup>Throughout this report, there are references to both TJX Companies Inc. (TJX) and Winners Merchant International L.P. (WMI). Where TJX as the parent company has the greater involvement, we refer only to TJX. Where both TJX and WMI have involvement in the issue or recommendation, we refer to TJX/WMI. Any reference to the “organization” throughout this Report refers to TJX and WMI jointly.

5. Quite often, a security system can be compromised by stealth, without the organization's knowledge. Until the breach is discovered, customers' personal information can be accessed by the intruder and used to commit other crimes. As well as causing harm to customers, this can have a deleterious impact on an organization's reputation and its relationship with business partners. Thus, once in place, security measures must be actively monitored, audited, tested and updated when necessary.
6. The cost to an individual's privacy following a security breach is clear. From an organizational perspective, the energy and cost involved in responding to a security breach can far outweigh the cost of developing and maintaining an effective security regime. The organization that experienced the breach is not the only one that expends energy and money in resolving the situation; considerable resources are also spent by credit card companies, banks, merchants, law enforcement agencies and regulatory bodies, which also suffer negative impact.
7. The lesson? One of the best safeguards a company can have is not to collect and retain unnecessary personal information. This case serves as a reminder to all organizations operating in Canada to carefully consider their purposes for collecting and retaining personal information and to safeguard accordingly.

### **Jurisdiction**

8. The Office of the Privacy Commissioner of Canada had jurisdiction to investigate because TJX/WMI conducts commercial activities in Canada. The Information and Privacy Commissioner of Alberta had jurisdiction in this case because WMI is an organization, as defined in subsection 1(i) of PIPA, and it operates in Alberta. Some of the personal information in question was collected in the organization's Alberta stores. The jurisdiction of the two Offices in this joint investigation applies primarily to the personal information collected during purchases made in Canada and subsequently disclosed as part of the data breach, as well as personal information collected during unreceipted return transactions at WMI stores.

### **Summary of investigation**

9. The purpose of the joint investigation was to examine the collection, retention and safeguarding practices of the organization, in order to determine whether the breach could have been prevented.

10. TJX is an off-price retailer of apparel and home fashion in the United States and around the globe. WMI is a wholly owned subsidiary of TJX. WMI owns and operates 184 Winners and 68 HomeSense retail stores across Canada.
11. On December 18, 2006, TJX learned that suspicious software had been detected on a portion of its computer system. TJX immediately initiated an investigation and determined that there was strong reason to believe that TJX's computer system had been intruded upon and that the intruder continued to have access to the system.
12. TJX states that it does not know who was responsible for the intrusion or whether there was one continuing intrusion or multiple, separate intrusions. TJX's investigation is ongoing. TJX has uncovered no evidence that any of its employees were involved in the computer intrusion. TJX is of the view that the intruder initially gained access to the system via the wireless local area networks (WLANS) at two stores in the United States.
13. On December 22, 2006, TJX notified various U.S. law enforcement agencies of the suspected intrusion. With the agreement of law enforcement, on December 26 and 27, 2006, TJX notified its contracting banks, credit card, debit card (collectively "payment card") and cheque processing companies, of the suspected intrusion. On December 27, 2006, TJX determined that customer information had also been accessed from one of its systems during the computer intrusion.
14. In early January 2007, TJX notified U.S. regulatory agencies and the Royal Canadian Mounted Police of the theft of customer information.
15. On February 18, 2007, TJX's investigation found evidence indicating that the intrusion may have been initiated earlier than previously reported and that additional customer information had possibly been accessed. On February 21, TJX publicly announced these additional findings regarding the timing and scope of the intrusion.

#### System affected in the computer intrusion

16. TJX believes that, during the computer intrusion, information relating to transactions conducted at the WMI stores was accessed from the Retail Transaction Switch (RTS) servers. The affected RTS servers process and store customer information related to transactions at TJX stores in North America, including information related to payment-card and merchandise-return transactions for which a receipt is not present at WMI stores in Canada.

17. TJX reports that the system was accessed by the intruder in July and September 2005, and from mid-May 2006 to mid-January 2007, but that no customer information was stolen after December 18, 2006.

Customer personal information affected by the intrusion

18. According to TJX, in July, September and November 2005, and at various times from mid-May 2006 to mid-January 2007, the intruder accessed, but did not steal, some credit card account data of WMI customers relating to a portion of the credit card transactions at WMI stores during the period from December 31, 2002, to June 28, 2004.
19. TJX claims that information from WMI Interac transactions made with debit cards issued by Canadian banks was not compromised in the course of the computer intrusion.
20. However, according to TJX, in 2005, the intruder also gained access to drivers' license and other provincial identification numbers (referred to as "ID numbers"), together with related names and addresses, of approximately 330 individuals with addresses in Canada. These customers provided this information to TJX in connection with unreceipted merchandise-return transactions at TJX stores located in the United States, primarily during the last four months of 2003 and in May and June, 2004.
21. TJX states that, in Canada, personal information provided in connection with unreceipted returns at WMI stores could not have been accessed in 2005 because WMI stores only began entering this personal information electronically in November 2005. Prior to this date, the names, addresses and telephone numbers of customers making unreceipted merchandise returns at WMI stores were retained in paper form.
22. TJX informed us that the intruder may have gained entry into the system outside of two stores in Miami, Florida. TJX stated that it is of the view that the intruder used deletion technology that, to date, has made it impossible for TJX to determine the contents of most of the files created and downloaded by the intruder.
23. In summary, the personal information relevant to this investigation consists of:
  - Credit card numbers, including expiration dates, used by customers of WMI. This information was collected and retained in order to process payments.
  - Names, addresses and telephone numbers of customers of WMI entered

- electronically after November 2005; and,
- Canadian drivers' license and other provincial identification numbers, and names and addresses used by customers of WMI. The information in the last two bullets was collected to prevent fraud.

#### Wireless security safeguards in place at the time of the breach

24. At the time of the breach, TJX had in place various technical measures in its North American stores to protect personal information, including the Wired Equivalent Privacy (WEP) encryption protocol.
25. At the end of September 2005, TJX made a decision to improve the protection of its wireless networks by installing the Wi-Fi Protected Access (WPA) encryption protocols in its stores.

#### Post-incident action

26. TJX/WMI has been responsive to this incident and has taken the following action on its own initiative after discovering the breach:
  - The organization undertook forensic and other investigations to audit and analyze the security of the TJX computer system, and to enhance the security of the TJX computer system in a continuing effort by TJX to safeguard against future attempted unauthorized intrusions.
  - It contacted law enforcement officials. Law enforcement investigations continue in the United States, and a number of regulatory investigations are being conducted with respect to the computer intrusion.
  - TJX has issued press releases about the computer intrusion, and posted updated customer alerts on its websites, including at [www.winners.ca](http://www.winners.ca) and [www.homesense.ca](http://www.homesense.ca). TJX, on behalf of WMI, has sent letters to the approximately 330 individuals with Canadian addresses whose personal ID numbers, together with related names and addresses have likely been accessed during the computer intrusion.
  - TJX also established a 24-hour, seven-day-a-week, toll-free help line for customers, including Canadian customers. TJX implemented a number of technical changes, which it specified to our Offices.
  - In addition, log files on the RTS servers are now purged after 24 to 48 hours, depending on what time the information arrives on the RTS servers.

## **Issues**

27. There are three key issues to address in our findings, namely:

- Did the organization have a reasonable purpose for collecting the personal information affected by the breach?
- Did the organization retain the information in compliance with PIPEDA and PIPA?
- Did the organization have in place reasonable safeguards to protect the personal information in its custody?

## **Findings**

### **Did the organization have a reasonable purpose for collecting the personal information affected by the breach?**

28. The first, and central, issue to consider is whether TJX had a reasonable purpose for collecting the personal information that was compromised in the intrusion.
29. In making our determinations, we applied subsection 5(3) of PIPEDA, which states that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. This is similar to the provision outlined in section 2 of PIPA.
30. Principle 4.2 of PIPEDA requires that the purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected. Principle 4.3.2 requires knowledge and consent. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. Similarly, subsection 13(1) of PIPA requires that “before or at the time of collecting personal information about an individual from the individual, an organization must notify that individual in writing or orally as to the purpose for which the information is collected.”
31. According to Principle 4.3 of PIPEDA and paragraph 7(1)(a) of PIPA, the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where the *Acts* specify. Even where consent is properly obtained, PIPEDA requires, under Principle 4.4, that the

collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

32. Subsection 7(2) of PIPA requires that organizations do not require individuals to consent to providing more personal information than necessary to provide a product or service. Even if consent is properly obtained, PIPA requires that an organization collect personal information only for purposes that are reasonable [subsection 11(1)]. Furthermore, subsection 11(2) of PIPA requires that the collection of personal information is limited to the extent that is reasonable for meeting the purposes for which the information is collected.
33. Principle 4.3.3 of PIPEDA states that an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes.
34. The personal information accessed by unauthorized individual(s) during the TJX intrusion included the following:
  - Payment card data, including credit card numbers and expiration dates; and
  - Names, addresses, telephone numbers, drivers' license and other provincial identification data collected in return-of-goods transactions.
35. The payment card data, including credit card numbers and expiration dates, is collected and is necessary to complete a sales transaction and is therefore reasonable.
36. The information outlined in the second bullet above is collected in relation to unreceipted returns. TJX stated that its practice of collecting personal information relating to unreceipted return of goods is for the purpose of detecting and deterring fraud.
37. TJX advised us that the collection of the driver's license number is necessary to implement an effective fraud-management system. The actual identification number must be collected for unreceipted returns because its business purpose goes beyond confirming identity. An actual unique numeric identifier is critical to determine whether a particular customer is excessively returning goods without a receipt. The organization maintains that the collection of personal information, along with provision of a notice to the returner that additional returns without receipts may not be accepted from a particular individual, has a deterrent effect.

38. If the organization initiates an internal investigation related to a frequent “returner,” identification numbers are not necessary for the investigation. If the internal investigation is escalated to law enforcement, the organization states that it would likely provide all information collected on the customer’s file to law enforcement. However, TJX could not confirm whether the driver’s license number would be necessary for police investigations.
39. We agree that, when merchandise is returned without a receipt, the collection of some personal information from customers is reasonable. In other cases, retailers have expressed concern about their vulnerability to financial loss from merchandise returned without a receipt. For example, individuals may return merchandise that was stolen or that does not originate from the retailer.
40. The OPC has found in earlier cases that, for the purposes of deterring fraud during the return of goods, the extent of reasonable collection of personal information was limited to name and address. Thus, the collection of customers’ names and addresses for this purpose is reasonable and appropriate in the circumstances, as per subsections 5(3) of PIPEDA and 11(1) of PIPA.
41. The collection of the drivers’ license information, however, is a different matter. In our view, we can draw an analogy between the collection of drivers’ license numbers as numeric identifiers and the collection of the Social Insurance Number. The OPC and AB OIPC have stressed that a SIN is not a *de facto* identifier and should only be used for legislated, social benefit purposes, as was intended.
42. A driver’s license is proof that an individual is licensed to operate a motor vehicle; it is not an identifier for conducting analysis of shopping-return habits. Although licenses display a unique number that TJX can use for frequency analysis, the actual number is irrelevant to this purpose. TJX requires only a number—any number—that can be consistently linked to an individual (and one that has more longevity and is more accurate than a name and telephone number).
43. Moreover, a driver’s license number is an extremely valuable piece of data to fraudsters and identity thieves intent on creating false identification with valid information. After drivers’ license identity numbers have been compromised, they are difficult or impossible to change. For this reason, retailers and other organizations should ensure that they are not collecting identity information unless it is necessary for the transaction.
44. We are not suggesting that identifying and investigating frequent returns for loss-prevention purposes is not a legitimate activity. The organization confirmed that

the refund-management system could operate with any unique numeric identifier. It does not specifically require a driver's license or other provincial identification number.

45. TJX has taken temporary measures while it considers revisions to its merchandise returns policy and other customer policies, and the outcome of this investigation.
46. In sum, we find that the collection of names and addresses is acceptable but the recording of ID numbers was excessive and contrary to Principle 4.4 of PIPEDA or subsection 11(2) of PIPA.
47. Although TJX/WMI has suspended the collection of drivers' license and other personal information in return-of-goods transactions, at the time of the breach this was a mandatory requirement. As we have found that this personal information exceeds what is reasonable for such a transaction, the activity was contrary to Principle 4.3.3 of PIPEDA and subsection 7(2) of PIPA.
48. Lastly, we were not provided with evidence that customers were notified of the purpose of the collection of drivers' license numbers. Considering the complexities of how this information could be used or disclosed, we are of the view that TJX and WMI contravened Principles 4.2 and 4.3.2 of PIPEDA and subsection 13(1) of PIPA. When considering the new policy for returns, TJX must improve notification of the purposes for its collection practices during merchandise returns.

#### **Did the organization retain the information in compliance with the Acts?**

49. In making our determinations regarding retention, we applied section 35 of PIPA states that "notwithstanding that a consent has been withdrawn or varied under section 9, an organization may for legal or business purposes retain personal information as long as is reasonable." Principle 4.5 of PIPEDA states that personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes. This provision requires organizations to limit the retention of personal information. It compels organizations to establish maximum periods of retention that meet legal (such as statutory limitation periods for civil lawsuits) and business needs.
50. TJX reported that drivers' license and other identification numbers were retained indefinitely. As the intrusions took place over an extended period of time, the hackers were able to take full advantage of downloading information that should

not have been retained.

51. TJX did not provide a persuasive argument for the necessity of collecting drivers' licenses for its business purposes, and we determined that this collection is not permitted under subsections 11(2) and 7(2) of PIPA or under Principle 4.4 of PIPEDA. Given this, TJX cannot retain the personal information that it has collected contrary to the *Acts*.
52. Section 35 of PIPA permits the organization to retain the drivers' license numbers if reasonably collected and then retained for some business purpose. Since we found that it was not reasonable to collect this personal information, it follows that it is not reasonable to retain it. We therefore find that TJX retained the information in contravention of PIPA and PIPEDA.
53. TJX is currently developing comprehensive retention policies and practices, including establishing retention periods for records in any form.
54. TJX also made an immediate decision to limit the retention period for data on its RTS server. The data is now retained for a specified and limited period of time for troubleshooting purposes. Such a measure reduces the risks and vulnerabilities exposed in the breach. TJX also states that it needs to retain credit-card and debit-card transactional data elsewhere in the organization for 18 months. This will allow time for customers to challenge charges, for audit purposes, for charge backs and for meeting its contractual obligations with the card issuers. The issue of retention is part of the broad privacy review process currently underway by TJX, and we expect that it will include this information in its completed retention policies.

### **Recommended actions**

55. Before we issued our findings in this complaint, and taking into consideration the steps already taken by TJX/WMI, we recommended that the organization:

#### **Collection**

- cease the collection of customers drivers' license and other provincial identification numbers during merchandise returns, and purge such information from all of its databases; and
- clearly notify individuals as to the purposes, uses and potential disclosures of all personal information, once it implements a new returns policy.

## Retention

- provide us with a copy of its finalized retention procedures and practices by September 1, 2007;

## **Response to Recommendations concerning the Collection and Retention of Personal Information**

56. TJX presented further information about the impact of our recommendations on its ability to effectively manage fraud prevention. TJX/WMI was concerned that it would no longer be able to effectively deter fraud if a unique identifier could not be collected and analyzed. It also responded to us that it retained drivers' license information for troubleshooting purposes and to meet its contractual obligations with financial institutions.
57. While we still maintain that the collection *and retention of drivers' license numbers alone* for unreceipted merchandise returns is not necessary to prevent fraud, TJX/WMI proposed an alternative refund-authorization procedure that means that drivers' license information will be kept temporarily. We find this acceptable.
58. The new process makes use of what is referred to as a cryptographic hashing function in which identification numbers are immediately converted into a new number referred to as a "hash value"<sup>2</sup>, thereby rendering actual drivers' license numbers unreadable to any WMI or TJX employee.
59. The hash value would accomplish the goal of establishing a unique numeric identifier. WMI's return management system could operate in the same way as it presently does since the same identification number could be repeated or transformed into the same hash value every time, but the driver's license number would no longer exist in WMI/TJX's system and could not be reproduced.
60. With respect to existing identification numbers already in TJX/WMI's custody, TJX/WMI is converting them into hash values, effectively removing them from

---

<sup>2</sup> A hash function is an algorithm that transforms a string of numbers—the customer identification number in this case—into another, new value of a fixed length or a key that represents the original value. It is virtually impossible to convert the hash value or short bit string back into the original identification number. A hash value is unique in the sense that two drivers' license numbers could not result in the same "bit string" hash value, and any attempt to make changes to the number would negate the value.

the TJX/WMI system permanently. Until the existing numbers have been hashed, TJX/WMI has committed to encrypting them. TJX/WMI proposed retaining the personal information of customers who make unreceipted returns for a period of three years. The information would include the customer's name, address and hash value identification number.

61. OPC and AB OIPC accepted TJX/WMI's proposal as a means of resolving this matter since hashing identification numbers, as presented by TJX/WMI, appears to address our concerns about the collection of drivers' licenses. This acceptance is conditional on the requirement that the hashing proposal meets the highest level of industry standards.
62. With respect to collecting and retaining credit card data, TJX/WMI advised that WMI customer credit card data from 2003 had been stored for at least 18 months. When the RTS servers came on line in 2003, TJX encountered problems that required troubleshooting efforts. TJX/WMI argued that this constituted a reasonable business purpose since troubleshooting required staff to review and analyze transaction data as far back as 2003. Furthermore, TJX/WMI indicated that they are required by contract with financial institutions that process credit card transactions to retain transaction data for at least 18 months for charge-backs, audits, and other unspecified purposes.
63. With respect to the retention of credit card information to process transactions, it is our position that it may be reasonable to retain this personal information for the length of time specified in the organizations' contracts with financial institutions as this meets the requirement of retention "for legal or business purposes." Processing payments according to the terms and conditions of the organizations' contract with financial institutions is directly related to the purpose for which the information was collected in the first place.
64. However, with respect to retaining this information for "troubleshooting" purposes, TJX/WMI has not presented a persuasive argument regarding the retention of this information for longer than 18 months, nor any rationale as to why *all* the information needed to be retained in an identifiable format for such a lengthy time for this purpose. Further, "troubleshooting" is not directly related to the purpose for which the information was collected in the first place. Principle 4.5 of PIPEDA specifically requires that personal information be retained only as long as necessary for the fulfillment of the purposes for which the information was collected—not for a new purpose arising after the fact.
65. With regard to the recommendations concerning the retention procedures and practices and its privacy notice, TJX/WMI notified us that it has agreed to

provide us with a copy of its updated written personal information retention policies and procedures.

66. TJX/WMI has also informed us that it has agreed to update its privacy notices to reflect its new return policy by enhancing the notices to address modifications in WMI's refund authorization process, to clearly state the purpose for the information collected as part of the merchandise returns process, and to otherwise address concerns brought forward during the investigation.

### **Conclusion concerning collection and retention of personal information**

67. In conclusion, we are of the view that TJX/WMI contravened the provisions of PIPEDA and PIPA concerning the collection and retention of personal information held by it. We are pleased, however, that TJX/WMI has agreed to implement our recommendations to the extent that OPC and AB OIPC consider the matter to be resolved.

### **Did the organization make reasonable security arrangements to protect the personal information in its custody?**

68. The last issue to address is security safeguards. In making our determinations, we applied Principle 4.7 of PIPEDA, which states that personal information shall be protected by security safeguards appropriate to the sensitivity of the information. Principle 4.7.1 of PIPEDA stipulates that the security safeguards shall protect personal information against loss or threat, as well unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held. Principle 4.7.2 adds that the nature of the safeguards will vary depending on the nature of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. Under Principle 4.7.3, the methods of protection should include (a) physical measures, for example, locked filing cabinets and restricted access to offices; (b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and (c) technological measures, for example, the use of passwords and encryption. Principle 4.7.4 notes that organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information. Principle 4.7.5 requires that care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.
69. The safeguards will also be evaluated against section 34 of PIPA. It states that an organization must protect personal information that is in its custody or under

its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

70. TJX/WMI have a duty under PIPEDA and PIPA to safeguard personal information in its custody or under its control. The matter to be examined is whether its protection measures constituted “reasonable security arrangements” for the risks outlined. Both PIPEDA and PIPA require an organization to guard against reasonably foreseeable risks.

#### TJX’s Safeguards

71. We have already established that TJX/WMI was collecting too much data and retaining it for too long. During the investigation, we examined whether TJX looked at its entire systems and fully assessed their vulnerabilities. In addressing this issue, we considered whether TJX took “reasonable” security precautions, whether the security risk was foreseeable, the likelihood of damage occurring, the seriousness of the harm, the cost of preventative measures, and relevant standards of practice.
72. With respect to physical security, measures such as security personnel, photo ID, swipe cards, surveillance cameras and locks were in place at the time of the breach.
73. With respect to organizational or administrative safeguards, at the time of the breach, TJX had an information-security governance structure overseen by the Chief Information Officer; an employee Code of Conduct; a limited number of security clearances and background checks carried out on employees; procedures for departing employees to return ID cards, key and swipe cards; ongoing employee training; and security policies and guidelines.
74. With respect to network security, excluding wireless security, some measures to restrict access to the network were in place at the time of the breach.

#### Seriousness of the Harm

75. The sensitivity of personal information is a consideration in an assessment of harm and risk. Certain types of personal information can be used to harm or perpetrate fraud against individuals more easily than other information.
76. We are of the opinion that “reasonable security measures” compels organizations to consider the possible harm to individuals if the information were in the wrong hands. Principle 4.7.2 of PIPEDA explicitly recommends that

organizations consider sensitivity when implementing security measures.

77. Given the nature of the personal information that was accessed by the intruders, the number of affected individuals, and the time that elapsed before the intrusion was detected, the harm caused could be quite serious. The perpetrator(s) had access to millions of credit card numbers for an extended period of time—long enough to commit credit-card fraud or to pass information on to others to do the same. While individuals who do notice unusual charges on their credit cards may not be responsible for the charges, the credit-card companies or merchants are. This could amount to significant losses to these organizations, not to mention the costs of replacing compromised credit cards.
78. Moreover, the breach exposes individuals to an increased level of anxiety. If their credit cards have been misused, they must deal with credit-reporting agencies to ensure that their credit rating is not affected. In some cases, this includes placing a true fraud alert on their files and requiring that they be vigilant concerning future financial statements.

#### Reasonable Security Precautions

79. Legislative requirements typically establish minimum standards for conduct. The fact that encryption is included as a safeguard under Principle 4.7.3 of PIPEDA suggests that it is an established measure of protection.
80. TJX had an encryption protocol in place (WEP) that was in the process of being converted to WPA at the time of the breach. We are of the view that WEP does not provide adequate protection as it can be defeated relatively easily. It appears that the intruder may have accessed the RTS servers and client data due to a weak or inadequate encryption standard. WEP cannot be relied on as a secure system since the encryption is easily bypassed, and it is not adequate for protecting a network. We understand that TJX was in the process of changing to a higher encryption standard, and we acknowledge that a conversion of this nature requires lead time for budget, planning and implementation.
81. However, since 2003, experts have questioned the use of WEP as a secure protocol. The Institute of Electrical and Electronic Engineers (IEEE) is the organization that originally developed the WEP standard. In June of 2003, the IEEE itself recommended that the wireless encryption standard move from WEP to WPA.

### Cost of Preventative Measures

82. The cost of upgrading to secure equipment must be measured in relation to the cost of a potential intrusion. Since a compromised wireless LAN can allow an intruder into the corporate network, the potential for significant damage is quite high.
83. Replacing wireless products to secure the wireless network is a cost-effective way to close a vulnerable gap since protecting business assets is critical for any company. While the cost for different strengths, types and management strategies for data safeguards may vary, they are arguably less than an organization's cost of recovering from a data breach.
84. TJX commenced its WPA conversion project in October 2005 and completed it in mid-January 2007.

### Relevant Standards of Practice

85. Payment Card Industry Data Security Standard (PCI DSS) version 1.1, was released September 2006. (Prior to that, PCI DSS version 1.0 was released in December 2004.) The PCI DSS was developed and endorsed by the Payment Card Industry (PCI) Security Standards Council. The Council, formed as an independent body in September 2006, consists of VISA International, MasterCard Worldwide, American Express, Discover Financial Services, and JCB. The Council works with merchants and payment service providers to ensure that customer data is protected by ensuring the compliance of the PCI DSS. The standards were created as a means of addressing the growing problem of credit card data theft. While the guidelines are not mandatory, organizations are encouraged to follow them in order to help lower financial risks associated with account payment data breaches.
86. The PCI DSS is a set of requirements for enhancing payment account data security. The standards, based on 12 principles, cover such aspects as security management, policies, procedures, network architecture, software design and other critical protective measures such as monitoring and testing networks.
87. Version 1.0 did not mandate WPA technology; version 1.1 did. By late 2006, TJX should have been adhering to PCI DSS version 1.1, which was released in September of that year. The breaches, we note, took place over a period of time and extended beyond the new PCI version.
88. Information technology experts routinely refer to "layers" of data security because they are generally easier to install and maintain, and it is generally

accepted that organizations need more than one protection measure to thwart a dedicated hacker. Layers of protection—administrative, physical and technical—require significantly more effort and skill to penetrate, thereby reducing the risk of unauthorized access.

89. TJX had policies and procedures in place at the time of the breach. It had physical security; administrative measures (behavioural rules and their enforcement, such as policies to restrict the amount and type of data and its retention time, “need-to-know” rules); and technical protection measures (such as encryption, remote access).
90. However, there were flaws. TJX relied on a weak encryption protocol and failed to convert to a stronger encryption standard within a reasonable period of time. The breach occurred in July 2005, conversion began in October 2005, and the pilot project was completed in January 2007. We are also aware that the final conversion to a higher level of encryption will be completed soon.
91. Furthermore, while TJX took the steps to implement a higher level of encryption, there is no indication that it segregated its data so that cardholder data could be held on a secure server while it undertook its conversion to WPA.
92. TJX had a duty to monitor its systems vigorously. If adequate monitoring of security threats was in place, then TJX should have been aware of an intrusion prior to December 2006.
93. In our view, the risk of a breach was foreseeable based on the amount of sensitive personal information retained and the fact that the organization issuing industry standards had identified the weakness of WEP encryption. Information should have been segregated and the systems better monitored. Therefore, TJX did not meet the safeguard provisions of either PIPEDA or PIPA.

### **Recommended actions**

94. Before we issued our findings in this complaint, and taking into consideration the steps already taken by TJX/WMI, we recommended that the organization:

#### **Safeguards**

- provide us with an Executive Summary of its audit, including findings and recommendations, to ensure that the recommendations are examined against those safeguards for which TJX/WMI has a corporate obligation to protect personal information in accordance with provincial and federal privacy legislation and industry standards;

- notify us of how it will monitor its systems more vigorously; and
- complete the conversion to higher encryption standards, itemize these standards, and notify us of the conversion's completion, consistent with the reasoning and analysis of this report;

### **Response to Safeguard Recommendations**

95. The organization responded as follows:

- TJX provided us with documentation that satisfies our first recommendation.
- TJX informed us that since the intrusion, it has dedicated significant resources to enhance the security of its systems, including strengthening the monitoring of its systems that were compromised by the intruder.
- TJX informed us that all of its stores (including all WMI stores) now use WPA encryption technology.

96. We reviewed the proposed safeguard enhancements, and are satisfied that they are extensive and logical. They should contribute to a more secure system that will allow TJX/WMI to detect and respond to any future intrusion incidents.

97. However, on the matter of security arrangements, TJX maintains its position that it acted within a reasonable amount of time in converting to an improved encryption protocol, and, as a retailer, it acted earlier than most of its counterparts in its conversion program.

98. We acknowledge that, at the time, few retailers had converted to WPA technology in relation to PCI data standards compliance. Yet, we note that there were organizations that converted to WPA due to risk analyses of their business needs, and were ahead of the curve in ensuring that their customers' personal information was adequately safeguarded. However, whether or not other retailers made the move to enhance their data by using better encryption methods, the fact of the matter is that TJX was the organization subject to the breach.

99. We continue to contend that TJX did not have reasonable security arrangements in place at the time of the breach. Too much sensitive information was retained, and safeguards in place had inherent weaknesses. Robust security safeguards include a variety of elements, such as asset management, network segregation and active monitoring. We believe that TJX did not have as robust a system in place at the time as it could have had.

100. Notwithstanding this disagreement, we are pleased that TJX is implementing our recommendations concerning safeguards.

**Conclusion concerning safeguards**

101. TJX complied with our recommendations in such a manner that we consider the safeguard component of the complaint to be “well-founded and resolved” by the OPC and “resolved” by AB OIPC.