IVEY | Publishing

908E03

SECURITY BREACH AT TJX[1]

R Chandrasekhar wrote this case under the supervision of Professor Nicole Haggerty solely to provide material for class discussion. The authors do not intend to illustrate either effective or ineffective handling of a managerial situation. The authors may have disguised certain names and other identifying information to protect confidentiality.

 Version: (A) 2017-05-18

INTRODUCTION

"The company collected too much personal information, kept it too long and relied on weak encryption technology to protect it — putting the privacy of millions of its customers at risk."

— Jennifer Stoddart, Privacy Commissioner, Government of Canada, on September, 26, 2007, in Montreal[2]

November 12, 2007, was the first day for Owen Richel as the chief security officer at the Framingham, Massachusetts, U.S., headquarters of The TJX Companies Inc. (TJX). As he was driving to work, Richel had mixed feelings. He was excited about his new role — but also apprehensive. Up before dawn, he had been reviewing some of the statements he had highlighted in the report of the Privacy Commissioner of the Government of Canada, including Stoddart's comment, which had been widely reported. These statements pertained to gaps in the company's systems security. The times ahead, he knew, would be troubled.

When Richel accepted the offer from TJX two months earlier, he'd been sure he was making a smart career move. As chief information officer (CIO) of a small Canadian retailer, Richel was aware of TJX as a mega-retailer and a market leader in a niche category in North America. He was also aware that the company had been hit by hackers in December 2006. The management had downplayed the attack during the job interview, at which Richel could not glean any information beyond what was available in the public domain. Richel had been moved to sign with the company because the panel had expressed confidence in his background in the retail industry and his ability to manage information technology (IT) security. The position was also being newly created for him. Richel was impressed. As far as hacking was concerned, he

---

[1] *This case has been written on the basis of published sources only. Consequently, the interpretation and perspectives presented in this case are not necessarily those of TJX Companies Inc. or any of its employees. Individuals represented in the case are fictional but represent accurate portrayals of decision-makers and customers typically involved in such situations.*

[2] *Quoted in Mark Jewell, "Encryption Faulted in TJX Hacking,"* USA Today, *September 27, 2007, available online at http://www.usatoday.com/tech/news/computersecurity/infotheft/2007-09-26-tjx-encryption-breach_N.htm, accessed November 6, 2007.*

knew from experience that all retailers, large and small, were vulnerable to attacks and that one of the best safeguards was top-level commitment to IT security.

As he started tracking the development in detail during the interim period, Richel realized the scale of intrusion had escalated. While TJX had said that the data of about 46 million credit and debit cardholders had been affected, a class action suit filed by interested financial institutions in late October 2007 had placed the number at about 94 million. Calling it the largest breach of personal data ever reported in the history of IT security, *The Boston Globe* quoted a Gartner Inc. professional as saying, "It is the biggest card heist ever. It has done considerable damage."[3] The lawsuits by affected customers and financial institutions were moving forward quickly. The Federal Bureau of Investigation (FBI) of the U.S. government was already part of the company's internal investigation.

Now, sitting in his car in traffic, minutes away from starting his position at TJX, Richel was mulling over the issues, several new to him, which he would have to deal with simultaneously and quickly.

COMPANY BACKGROUND

TJX was the largest apparel and home fashions retailer in the United States in the off-price segment. TJX ranked 138th in the Fortune 500 rankings for 2006. With US$17.4 billion in sales for the year ending January 2007, the company was more than triple the size of Ross Stores Inc., its closest competitor.

Founded in 1976, TJX operated eight independent businesses under a common umbrella — T.J. Maxx, Marshalls, HomeGoods, A.J. Wright and Bob's Stores in the United States; Winners and HomeSense in Canada; and T.K. Maxx in Europe. The group had over 2,400 stores, and about 125,000 associates.

As an off-price retailer, TJX occupied the space between deep discounters selling unbranded goods at low prices and department or specialty stores selling branded goods at premium prices. TJX sold branded apparel and home fashions at prices between 20 and 70 per cent lower than department or specialty stores. It bought merchandise directly from manufacturers at wholesale prices throughout the year, in contrast to department or specialty stores, whose buying was driven by current trends and was seasonal in nature. It also acquired merchandise from department and specialty stores themselves, who were often stuck with excess goods every season as a result of late order cancellations, missed production deadlines and scheduling changes.

Operational efficiency, vendor relationships and scale were crucial to an off-price store, whereas fashion was the most important variable for department and specialty stores. For off-price stores, the quality of internal information systems was critical to maintaining margins, among the lowest in retail, and to staying competitive. IT systems helped large retailers like TJX connect people, places and information all along the value chain. They enabled rapid delivery of data, facilitating quick decisions at different levels. Vendors, buyers, merchandisers, stores associates, customers and financial institutions were inter-connected through IT networks, thereby boosting the retailer's productivity (throughput of product from manufacturing through sales). In-store technologies (such as kiosks and hand-held price/inventory barcode scanners) helped retailers enhance customer service and differentiate their stores from competitors. Many retailers invested in customer relationship management (CRM) technologies to increase revenues by targeting the most profitable customers.

---

[3] *Jenn Abelson, "Breach of Data at TJX Is Called the Biggest Ever," The Boston Globe, March 29, 2007.*

TJX had witnessed a change of guard at the top level of management in the fall of 2005. A focus on "profitable sales growth" had led to a rebound in financial results for the year ending January 2007. In a business in which margins were low, net income as percentage of sales had moved up (see Exhibit 1).

THE COMPUTER INTRUSION[4]

It was on December 18, 2006, that the company learned of hacking (see Appendix 1 for a glossary of terms used in computer intrusion and detection investigations). The presence of suspicious software, altered computer files and mixed-up data were among the first evidence of the intrusion. Involving the segment of the computer network handling payment cards (both credit cards and debit cards), cheques, and merchandise return transactions for customers, it seemed to affect all the eight businesses of the company and all the stores in the United States, Puerto Rico, Canada and the United Kingdom. The company quickly started an internal investigation and called in security consultants — General Dynamics Corporation and International Business Machines (IBM) Corporation — the next day. The latter confirmed, on December 21, that the company's computer systems had been "intruded upon" and that the intruder was still on the systems. While planning to contain the intrusion and protect customer data, the company notified law enforcement officials. The U.S. Secret Service suggested that disclosure of intrusion might impede an ongoing criminal investigation and that TJX should therefore maintain confidentiality until it was advised by the Secret Service to the contrary. The company was only allowed to notify contracting banks, credit and debit card companies and cheque-processing companies of the intrusion.

On February 21, 2007, TJX made a public announcement of the timing and scope of the intrusion. It said that its computer systems were first accessed by an unauthorized intruder in July 2005, on subsequent dates in 2005 and again from mid-May 2006 to mid-January 2007. It stated that no customer data had been stolen after December 18, 2006. The company said that in trying to identify the nature of data that was stolen by the intruder, TJX had faced three hurdles. First, before it had discovered the intrusion, it had deleted, in the ordinary course of business, the contents of many files that had been stolen. The files pertained to records going back as far as 2002. Second, the technology used by the intruder had made it impossible for TJX to determine the contents of most of the files stolen in 2006. Third, TJX believed some data was stolen during the payment card approval process. Thus, it was not able to precisely identify the nature of all of the data that was vulnerable to theft.[5]

The company said:

> We do not believe that customer personal identification numbers (PINs) were compromised, because, before storage on the Framingham system, they are separately encrypted in U.S., Puerto Rican and Canadian stores at the PIN pad, and because we do not store PINs on the Watford system.

The "Framingham system" processed and stored information pertaining to debit and credit card, cheque and unreceipted merchandise-return transactions for customers of T.J. Maxx, Marshalls, HomeGoods and A.J. Wright stores in the United States and Puerto Rico, and of Winners and HomeSense stores in Canada. The "Watford system" processed and stored information related to payment card transactions at T.K. Maxx in the United Kingdom and Ireland.

---

[4] *10-K Filings, www.tjx.com/investorinformation/SECfilings/10-K/03/28/2007, March 28, 2007.*

[5] *Frequently Asked Questions page, on company website, available at http://www.tjx.com/tjx_faq.html, accessed February 13, 2008.*

Until December 2006, when the intrusion was discovered, TJX was storing customer personal information on its Framingham system. The information, received from its stores in the United States, Puerto Rico and Canada, pertained to returns of merchandise without receipts and some cheque transactions. The personal information consisted of driver's license numbers and identification (ID) numbers (such as military and state ID, in some cases including social security numbers), together with names and addresses of the customers who had returned goods. Since April 7, 2004, the practice was to encrypt the information before it was stored. Actual characters were substituted by encryption, using an encryption algorithm provided by the software vendor.

TJX assured its payment card customers that their names and addresses were not included with the payment card data believed stolen for any period, because TJX did not process or store that information on either the Framingham or the Watford system in connection with payment card transactions. It also assured its customers that by April 3, 2006, the Framingham system was masking payment card PINs and some portions of cheque transaction information. For transactions after April 7, 2004, the Framingham system was encrypting all payment card and cheque transaction information. With respect to the Watford system, masking and encryption practices had been implemented at various points in time for various portions of the payment card data.

Subsequent investigations revealed that the data had been picked up by a group of East European residents specializing in collecting stolen credit card numbers, who, in turn, passed them on to a group in Florida. Both the groups were part of a diversified fraud ring whose activities included manufacturing "white plastic," a plain card with a properly encoded magnetic stripe. Although it could not be used in personal encounters with retail clerks, the white plastic could be swiped, without risk of detection, during self-checkouts (at gas stations and some big-box stores). The Florida group, under observation by the Secret Service, also specialized in manufacturing bogus credit cards complete with embossing, logos, holograms and properly encoded magnetic strips. The group was said to have applied new magnetic strips containing the stolen data to generate bogus cards. Having done so, it resorted to a tactic common among fraudsters: it used the bogus credit cards to purchase gift cards (usually up to $400, before additional identification was required) and then cashed the gift cards at the stores later. The gift card float technique was attractive to fraudsters because it bought them time. When a credit card was stolen and detected by the victim, it was only a matter of hours before the card was invalidated and its spending power had expired – an outcome which the purchase of gift cards circumvented.

HOW DID IT HAPPEN?

Richel learned through his preparatory research that there was a widely held view among IT security professionals that TJX systems had been intruded upon at multiple points of attack. This theory could partly account for the enormity of the intrusion, which affected millions of people. These multiple points included encryption, wireless attack, USB drives at in-store kiosks, processing logs and compliance and auditing practices. Though TJX identified encryption as a particular vulnerability, Richel felt he would need to fully investigate the other reports of multiple security vulnerabilities as a first priority in his new role.

Encryption

TJX had made the following announcement of how, it thought, the intrusion had occurred.

> Despite our masking and encryption practices on our Framingham system in 2006, the technology utilized in the Computer Intrusion during 2006 could have enabled the Intruder to steal payment card data from our Framingham system during the payment card issuer's approval process, in which data is transmitted to payment card issuers without encryption. Further, we believe that the Intruder had access to the decryption tool for the encryption software utilized by TJX.[6]

Widely used in the retail industry to protect credit card information in e-commerce transactions, encryption was a process of scrambling information so as to make it unintelligible until it was unscrambled by the intended recipient. Since credit cards could not be processed when their numbers were encrypted (or scrambled), a smart crook could seek a way to get the data during that window of time when it was in a state of being "in the clear" — that is, when it was decrypted (or unscrambled) — for less than a second. Additionally, as TJX found out, the intruders had the decryption key for the encryption software (WEP) that was in use at TJX.[7]

While TJX's view of how the attack occurred seemed legitimate, Richel felt there could be other points of entry for the computer intrusion.

Wireless attack

The *Wall Street Journal*[8] was among the first to suggest that the TJX break-in started in July 2005 with a wireless hack of a Marshalls store in St. Paul, Minnesota. Said the report:

> The thieves pointed a telescope-shaped antenna toward the store and used a laptop computer to decode data streaming through the air between hand-held price-checking devices, cash registers [point-of-sale, presumably] and the store's computers. That helped them hack into the central database of Marshalls' parent, TJX Cos. in Framingham, Mass., to repeatedly purloin information about customers.

Wireless was a popular means of attacking retail chains. "By focusing on those little handheld (price check) guns and their interactions with the database controller, you can capture IP addresses. That's your gateway," the *Journal* quoted an auditor as saying. It also reported that the attackers performed "most of their break-ins during peak sales periods to capture lots of data and used that data to crack the encryption code." It added:

> They digitally eavesdropped on employees logging into TJX's central database in Framingham and stole one or more user names and passwords. With that information, they set up their own accounts in the TJX system and collected transaction data, including credit card numbers, into about 100 large files for their own access. They were able to go into the TJX system remotely from any computer on the Internet. They were so confident of being undetected that they left encrypted messages to each other on the company's network, to tell one another which files had already been copied and avoid duplicating work.

---

[6] *10-K Filings, March 28, 2007www.tjx.com/investorinformation/SECfilings/10-K/03/28/2007.*

[7] *WEP is short for wireless equivalent privacy, which is an encryption algorithm for wireless data. Information about cracking WEP is widely available online via simple Google searches.*

[8] *Joseph Pereira, "How Credit-Card Data Went Out Wireless Door," Wall Street Journal, May 4, 2007, available online at http://online.wsj.com/article/SB117824446226991797.html, accessed November 5, 2007.*

USB Drives at In-store Kiosks

An *InformationWeek* story suggested that the data breach had begun at TJX with in-store kiosks as entry points. "The people who started the breach opened up the back of those terminals and used USB drives to load software onto those terminals," said the story.

> The USB drives contained a utility program that let the intruder or intruders take control of these computer kiosks and turn them into remote terminals that connected into TJX's networks. The firewalls on TJX's main network weren't set to defend against traffic coming from the kiosks. Typically, the USB drives in the computer kiosks are used to plug in mice or printers. [9]

Processing Logs

In its filings before the U.S. Securities and Exchange Commission, TJX had put the number of cards at risk at 46 million. But in their filings in the courts, the banks had placed the number at 94 million.[10] The discrepancy suggested that TJX did not have the log data needed to do a forensic analysis. Such logs could generally provide information about files on the system — when they had been added, changed, accessed, the format of contents and so on.

Compliance Practices

The Payment Card Industry Data Security Standards (PCI DSS) were a strong security blueprint for retailers (see Exhibit 2). Court documents showed that TJX had not met nine of the dozen requirements covering encryption, access controls and firewalls.

Auditing Practices

Under PCI DSS, an approved auditor had to conduct an annual on-site audit and quarterly network scans on what were called Level 1 businesses, those that processed over six million credit card transactions per year. Level 2 and 3 companies — those that processed between 20,000 and six million credit card transactions per year — had to fill out an annual self-assessment questionnaire and have an approved vendor conduct quarterly network scans. TJX had passed a PCI DSS check-up. The auditors had not noticed three key problems with TJX systems — the absence of network monitoring, the absence of logs and the presence of unencrypted data stored on the system. They had also not asked why TJX had retained customer data years after it should have been purged. Some of the stolen information was from transactions concluded as long ago as 2002.

THE SUMMER OF DISCONTENT

During the summer of 2007, a number of class actions had been filed against TJX in state and federal courts in Alabama, California, Massachusetts and Puerto Rico, and in provincial Canadian courts in

---

[9] *Larry Greenemeier, "The TJX Effect," InformationWeek, online edition August 11, 2007, at http://www.informationweek.com/security/showArticle.jhtml?articleID=201400171&cid=RSSfeed_Tech, accessed November 5, 2007.*

[10] *Jaikumar Vijayan, "Court Filing Doubles Scope of TJX Data Breach," Computer World, October 25, 2007.*

Alberta, British Columbia, Manitoba, Ontario, Quebec and Saskatchewan, on behalf of customers whose transaction data were allegedly compromised by the computer intrusion. An action had also been filed against TJX in federal court in Massachusetts, putatively on behalf of all financial institutions who issued credit and debit cards used at TJX stores during the period of the security breach. The actions asserted claims for negligence and related common-law and/or statutory causes of action stemming from the intrusion, and sought various forms of relief, including damages, related injunctive or equitable remedies, multiple or punitive damages and attorney's fees. A number of government agencies were also conducting investigations as to whether TJX had violated laws regarding consumer protection.

RECENT DEVELOPMENTS

By August 2007, TJX had booked a cost of US$168 million for the data breach it had announced in February — $118 million in after-tax costs taken in the most recent quarter and $21 million projected as a possible hit for 2008, on top of the $29 million already reported in prior quarters. *The Boston Globe* had quoted a TJX official as saying that the US$118 million quarterly after-tax figure was about $196 million pretax, and that the $21 million for 2008 was about $35 million pretax.

On September 21, 2007, the company had entered into a settlement agreement, subject to court approvals, in regard to customer class actions. As per the agreement, customers who had returned merchandise without a receipt and to whom TJX had sent letters reporting that their driver's license or other identification information may have been compromised, were offered three years of credit monitoring, along with identity theft insurance coverage paid for by TJX. The company would also reimburse these customers for the documented cost of driver's license replacements. The company was to offer vouchers to any customers who showed they shopped at TJX stores during the relevant periods and who had incurred certain costs as a result of the intrusion. TJX would also organize a one-time, three-day customer appreciation special event, in which prices would be reduced by 15 per cent.

NOVEMBER 12, 2007

As the TJX headquarters sign came into view, Richel felt renewed determination to see the blossoming crisis at TJX as an opportunity. He would use his business leadership skills, combined with his abilities to work with the IT organization, to stay on top of the situation. He saw his priorities as falling into two distinct areas — short-term and long-term. The short-term priority was to understand the failure points and tighten and improve systems security at TJX. In the long term, Richel had to work on minimizing risks, so that an intrusion would not happen again. Most importantly, he needed to secure management buy-in to the fact that IT security was a business issue and not a technology issue.

The first visitor he had at his office that day was Vincent George, who introduced himself as the company's manager of customer service. "Welcome to the party," he said, giving him a copy of a letter he had received in the mail the previous day (see Appendix 2); "I will catch up with you later in the day."

Exhibit 1

THE TJX COMPANIES, INC. — CONSOLIDATED STATEMENT OF INCOME
(Years ending January 31, in thousands of US$)

	2007		2006		2005	
	Amount	%	Amount	%	Amount	%
Net sales	17,404,637	100.0	15,955,943	100.0	14,860,746	100.0
Cost of sales	13,213,703	75.9	12,214,671	76.5	11,357,391	76.4
Selling, general & administration	2,928,520	16.8	2,703,271	16.9	2,487,804	16.7
costs	15,566	0.1	29,632	0.2	25,757	0.2
Interest cost	1,246,848	7.2	1,008,369	6.3	989,794	6.6
Income from continuing operations						

Source: Company annual reports

Exhibit 2

PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARDS

	Control Objectives	Requirements
1	Build and Maintain a Secure Network	• Install and maintain a firewall configuration to protect cardholder data • Do not use vendor-supplied defaults for system passwords and other security parameters
2	Protect Cardholder Data	• Protect stored cardholder data • Encrypt transmission of cardholder data across open, public networks
3	Maintain a Vulnerability Management Program	• Use and regularly update anti-virus software • Develop and maintain secure systems and applications
4	Implement Strong Access Control Measures	• Restrict access to cardholder data by business need-to-know • Assign a unique ID to each person with computer access • Restrict physical access to cardholder data
5	Regularly Monitor and Test Networks	• Track and monitor all access to network resources and cardholder data • Regularly test security systems and processes
6	Maintain an Information Security Policy	• Maintain a policy that addresses information security

Source: https://www.pcisecuritystandards.org.

Appendix 1

GLOSSARY OF TERMS USED IN SECURITY AND INTRUSION DETECTION

Access Control: A mechanism that ensures that resources are only granted to those users entitled to them.

Activity Monitors: They prevent virus infection by monitoring the system for malicious activity and blocking that activity when possible.

Advanced Encryption Standard (AES): An encryption standard meant to specify an unclassified, publicly disclosed, symmetric encryption algorithm.

Algorithm: A finite set of step-by-step instructions for a problem-solving or computation procedure, especially one that can be implemented by a computer.

Asymmetric Cryptography: A modern branch of cryptography in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm.

Brute Force: A form of attack involving an exhaustive procedure trying all possibilities, one by one.

Business Continuity Plan (BCP): The plan for emergency response, backup operations and post-disaster recovery steps ensuring the availability of critical resources and facilitating continuity of operations in an emergency situation.

Covert Channels: Means by which information can be communicated between two parties in a covert fashion using normal system operations.

Data Encryption Standard (DES): A widely used method of data encryption using a private (secret) key. There are 72 quadrillion possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. As with other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

Day Zero: The day a new vulnerability is made known.

Decryption: Process of transforming an encrypted message into its original plaintext.

Defacement: The method of modifying the content of a website in such a way that it becomes vandalized, embarrassing to the website owner.

Defense In-Depth: Usage of multiple layers of security to guard against failure of a single security component.

Demilitarized Zone (DMZ): Network area that sits between an organization's internal network and an external network, usually the Internet.

Appendix 1 (continued)

Dictionary Attack: An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words, unlike a brute force attack, which tries all possible combinations.

Disaster Recovery Plan (DRP): The process of recovering IT systems in the event of a disaster.

Due Diligence: A protection plan that organizations must develop and deploy to prevent fraud and abuse.

Dumpster Diving: Obtaining passwords and corporate directories by searching through discarded media.

Encapsulation: Inclusion of one data structure within another to hide it for the time being.

Encryption: Transformation of data (called "plain text") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

Escrow Passwords: Passwords written down and stored in a secure location (like a safe) for use by emergency personnel when privileged personnel are unavailable.

Firewall: A logical or physical discontinuity in a network to prevent unauthorized access to data.

Flooding: An attack causing a systems failure by providing more input than the entity can process properly.

Fragmentation: The process of storing a data file in several "chunks" or fragments rather than in a single contiguous sequence of bits in one place on the storage medium.

Hardening: Process of identifying and fixing vulnerabilities on a system.

Hybrid Encryption: An application of cryptography combining two or more encryption algorithms.

One-Way Encryption: Irreversible transformation of plaintext to cipher text, such that the plaintext cannot be recovered from the cipher text even if the cryptographic key is known.

Scavenging: Searching through data residue in a system to gain unauthorized knowledge of sensitive data.

Shadow Password File: A system file in which encryption user passwords are stored so that they are not available to people who try to break into the system.

Spoof Attempt: An unauthorized user trying to gain access to a system by posing as an authorized user.

Steganography: Method of hiding the existence of a message or other data. This is different from cryptography, which hides the meaning of a message but does not hide the message itself. An example of a steganographic method is "invisible" ink.

Appendix 1 (continued)

Symmetric Cryptography: A branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption and decryption, or signature creation and signature verification).

Virus: A hidden, self-replicating section of computer software that propagates by inserting a copy of itself into and becoming part of another program.

Wireless Application Protocol: A specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access.

Wireless Equivalent Privacy: A security protocol for wireless local area networks.

Source: http://www.sans.org/resources/glossaryReferenced January 30, 2008.

Appendix 2

LETTER FROM A CUSTOMER

November 08, 2007

Mr Vincent George
Customer Service Manager
The TJX Companies Inc
Framingham, Massachusetts, US

Dear Mr George:

I have been a loyal shopper at Winners and HomeSense for a long time so I was deeply shocked when I heard about the computer problems which put my personal information at risk. In fact, I have stopped shopping at both stores because of the losses I have personally suffered. Let me explain.

December 05, 2006 was a horrible day for me. That was the day when I went into my bank to withdraw cash for holiday shopping and was surprised when the teller said that there was no balance in my checking account. He then turned the screen towards me and I noticed five consecutive ATM withdrawals, during the preceding six days, of $1,000 each. I knew I had not made these withdrawals because since my monthly pay arrived in late November, I had been really busy at work and basically didn't do anything other than work and go home to sleep. But, the teller and then the bank manager were categorical that I could not lodge a claim because ATM transactions were not covered by the bank's liability policy.

The next day, I faced a double whammy when I received the credit card statement for the previous month by mail. The statement showed a series of ten purchases of US $400 each, spread over a week, at a well known big box store. I had never shopped in US currency while in Toronto. I immediately called up the credit card company. The call center representative told me that he would trigger an investigation right away, assuring me that I would be fully covered for all unauthorized transactions on which my valid signature could not be found.

So after two weeks of scrambling to cover mortgage and bill payments and worrying about a huge increase in my credit card debt, I got a call from the credit card company to say that $4,000 was being returned to my account because none of the ten signatures matched mine for the gift cards that had been purchased. The company offered to cancel my card and re-issue a new one, which I'm still leery of using for fear this will happen again.

I had given up on the loss of $5,000 on my debit card till I saw a newspaper report on February 22, 2007 about your public disclosure on a hit on your computer systems. The report said that the segment of computer network hacked at TJX included "merchandise return" transactions. It was then that I recalled that I had returned two items I had purchased at your store in Toronto a few months ago – in early November 2006. One return transaction pertained to my debit card and the other to my credit card. I had to produce a lot of identification at the time of return, as required, since I could not locate the receipts. I am absolutely certain that YOUR organization is responsible for the financial loss I've suffered. I expect full compensation. If you are an honorable organization you'll take care of my concerns swiftly – otherwise, I'll see you in court.

Mary Smith