The TJX Data loss and security breach case

TJX, the owners of TKMaxx were the targets of one of the largest data theft cases so far. The consequences are still ongoing, but over 45 million credit cards were affected and customer identity data such as driving licences was also stolen. This is an overview of the case, the investigation, and the long-term effects of the data theft.

Contents

The TJX case was easily one of the largest data theft cases in recent history with 45 Million credit cards compromised. When the case initially emerged it was believed to be an isolated incident, and then investigators discovered that the system had be compromised at least a year earlier than believed.

Despite the fact that many people know the name, the details of the case are scattered across a number of links. This lens is designed to pull the third party information together into a rough timeline, and give people an overview of what actually occurred during the case and investigation, as well as how to protect their own organisation.

Perhaps most disturbingly, it does not appear to have been an inside job. The company's network security was penetrated externally.

A timeline of the investigation - A brief overview of the case and investigation

The case first came into the public eye at the start of 2007. No one then was aware of what it would grow into.

On 17th January 2007, TJX released the information that thieves had had access to credit card information stored on its network. It was suggested that a breach had occurred and suspicious software was discovered on December 18th 2006. They notified law enforcement. Search Security - 18th Jan 2007

In January, a number of banks reported increased fraud incidents believed to be linked, including transactions from the US, Hong Kong and Sweden. (Security Focus)

In February, TJX released the information that the thieves had had access earlier than December (between May 2006 and January 2007), and over one million cards were believed affected.

Then in March 2007, the ongoing investigation released news that it believes there had been breaches back as far as July 2005 (Search Security - 21st Feb 2007).

These earlier intrusions did not steal credit card data they merely accessed it. However they also accessed data such as driving licences, which is useful for identity theft. Because of the way TJX stored data, which was completely unencrypted and held long-term, transactions as far back as 2002 were affected.

In April 2007, a set of banks announced they were beginning legal proceedings against TJX for its data storage.

On the 8th May 2007 the Wall Street Journal revealed the fraud was tied to Wi-fi. The thieves began by exploiting poor network security on a wireless network, allowing them to intercept card transactions, and then used their open access point to track back to the company's central database. TJX were storing customer's personal data (and complete credit card numbers) in an unencrypted format, allowing the thieves to simply download them. This meant that every piece of credit card data on the system had potentially been compromised - at least 45.7 million accounts were affected.

In October 2007 It was suggested as many as 95 million card numbers were exposed. TJX retaliated saying that most were expired when they were compromised. (6)

1. How it was done - A sophisticated attack

The entire operation proved to be a sophisticated set up, where the credit cards and data were carefully used to launder the money, not simply sold online.

8th May 2007 the Wall Street Journal revealed the fraud was tied to Wireless (Search Security). The thieves began by exploiting poor network security on a wireless network at a store. This allowed them to sit outside and intercept customers' credit card numbers as they made transactions.

They then used their open access point to track back to the company's central database.

TJX were storing customers' personal data (and complete credit card numbers) in an unencrypted format, allowing the thieves to simply download them. This meant that every piece of credit card data on the system had potentially been compromised - at least 45.7 million accounts were affected. They were also storing data from
transactions as far back as 2002, meaning that anyone who had made a transaction in the store in that period was potentially at risk.

The stolen credit card details were then used to buy gift cards to various stores which could be exchanged for goods. To launder the money, the gift cards were used for jewellery or electronic goods. (Computer weekly)

2. **Fines and settlements: The effects on TJX and the costs of data loss**

The full costs of the breach will probably never be known, but here are a few that are:

September 2007 - A Class action suit from consumers is settled as TJX will provide $30 vouchers to all consumers affected. Those who lost their driver's licence information will get three years of credit monitoring and $20,000 fraud insurance. (Security Focus)

October 2007 - Visa fines TJX $880,000 (SC Magazine US)

November 2007 - TJX settles with Visa for $40.9M to cover the costs of reissuing the cards. (Ecommerce Times)

April 4th 2008 - TJX settles with Mastercard for $24M (Boston Herald)

It is suggested that only 1% (Bloggersnews) of those affected by the breach will be able to claim from the class action suit, but that would still be another $13,650,000.

3. **The legal consequences**

**The perpetrators**

August 8, 2008 the TJX President issued a statement saying they: "regret any difficulties you may have experienced as a result of the sophisticated criminal attack(s) on our computer system in 2005 and 2006" However he goes on to say that they are glad the people responsible are facing charges. (TJX Message)

Although the damage had already been done, the investigation managed to successfully track the people believed responsible and charges were brought against those within jurisdiction.

One of the ringleaders (from Miami) got five years in jail and a $300,000 fine (Computer weekly).

Another got thirty years in a Turkish jail. It was proved to be an organised operation which used the credit cards to buy gift cards which were then used to buy goods in a money laundering operation.

**Ecommerce security for merchants and card acquirers**

The Payment Card Industry Data Security Standard is designed to reduce the chances of such attacks, and the likelihood of such attempts succeeding.

It was not in place at TJX at the time the attacks took place. Visa had agreed to hold off on fines until the end of 2008 as long as the company showed diligence in working towards the standard. Understandably, the data breach and what it revealed about the security practices at TJX were held to leave the company liable for its non-compliance.

**TJX Settles with 41 States over Data-Theft Incident**

TJX, the parent company of Marshalls, T.J. Maxx, HomeGoods and other big retail chains, has settled with Attorney Generals from 41 U.S. states regarding what was once considered the biggest data breach in history. The company agreed to a total of $9.75-million payment that would cover investigative costs ($1.75 million), establishing a Data Security Trust Fund ($2 million) and supporting future data protection and consumer protection efforts by the states ($5.5 million).

Back in January 2007, a massive data breach incident that resulted in the compromise of between 45 and 95 million payment cards was announced by TJX. Eleven people from U.S, Ukraine, Estonia, Belarus and China have been charged for their roles in the hack, which involved penetrating the company's wireless network at various weak spots and intercepting unencrypted credit card data.

This latest settlement has received mixed responses from privacy advocates, business analysts, security experts and government representatives. "This settlement ensures that companies cannot write-off the risk of a data breach as a cost of doing business," Massachusetts Attorney General Martha Coakley, whose office headed up the investigation, said.
Some people have argued that it was inappropriate for the Massachusetts AG's Office to lead the probe, as the company was headquartered in the same state and was one of its largest employers. Furthermore, the investigation revealed few to none new information that wasn't already known since shortly after the incident.

Others questioned the impact of the $9.75-million amount, since TJX established a $216-million reserve back in 2007 specifically to cover costs related to this data breach, including lawsuits. The insurance check cashed by the company after the incident was alone almost two times this settlement's figure.

However, the agreement also imposes some security-related requirements on TJX, such as upgrading from WEP wireless encryption to WPA or better, limiting the credit card data on the company's network, separating systems that store or transmit personal information from the rest of the network and enforcing stricter access controls, employing two-factor authentication for remote access to the network and encouraging the development of new technologies within the Payment Card Industry, such as end-to-end encryption.

Some industry professionals pointed out that, while all of these requirements were good in principle, they did not exceed the boundaries of what the payment card industry already enforced or recommended. All companies handling credit card data, TJX included, already need to be compliant with the PCI DSS (Payment Card Industry's Data Security Standard) in order to do business.

TJX Security Breach Time Line

<table>
<thead>
<tr>
<th>The present day</th>
<th>The TJX Companies, Inc. is the leading off-price retailer of apparel and home fashions in the U.S. and worldwide, ranking 119 in the most recent Fortune 500 listings. With nearly $22 billion in revenues in 2010, more than 2,800 stores in six countries and over 160,000 Associates, we see ourselves as a global, off-price value retailer. “Our off-price mission is to deliver a rapidly changing assortment of fashionable, quality, brand name merchandise at prices that are 20-60% less than department and specialty store regular prices, every day”.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>Before the attacks began, TJX was issued a report on its security compliance that “identified numerous serious deficiencies at TJX, including specific violations”. An unnamed TJX consultant said that &quot;he had never seen such a void of monitoring and capturing via logs activity at a Level One merchant as he saw at TJX.&quot; TJX did not remedy many of these deficiencies.&quot;</td>
</tr>
<tr>
<td>2005, July</td>
<td>Data first accessed by an unauthorized intruder. The DES encryption standard was widely used in 2004, so it is probable that this is what TJX used.</td>
</tr>
<tr>
<td>2006, May</td>
<td>A traffic capture/sniffer program was installed on the TJX network by the cyber-thieves, where it remained undetected for seven months, &quot;capturing sensitive cardholder data as it was transmitted in the clear by TJX.&quot; &quot;After locating the stored data on the TJX servers, the intruder used the TJX high-speed connection in Massachusetts to transfer this data to another site on the Internet&quot; in California. More than &quot;80 GBytes of stored data improperly retained by TJX were transferred in this manner. The intruders then engaged in an increasingly popular tactic: post-event cleanup, deleting and otherwise tampering with log files, changing clock settings and moving data to hide their movements. This perhaps explains why TJX did not detect the activity.</td>
</tr>
<tr>
<td>2006, Oct 3</td>
<td>It is claimed that TJX first became aware of the breach when it learned of problems with Discover Cards. TJX has said that cyber-thieves accessed TJXs systems in July 2005, but that it didn’t learn of the multiple incidents until Dec. 18, 2006.</td>
</tr>
</tbody>
</table>
2006, Dec 18 | The filing also revealed a more-detailed timeline of the incident. TJX officials said they first learned of the situation on Dec. 18, 2006, when “we learned of suspicious software on our computer systems.”

The company has spent about $5 million in a three-month period dealing with this breach, “which includes costs incurred to investigate and contain the computer intrusion, strengthen computer security and systems, and communicate with customers, as well as technical, legal, and other fees.”

2006 Dec, 21 | Three days later, the filing said, investigators brought in by TJX concluded “there was strong reason to believe that our computer systems had been intruded upon and that an intruder remained on our computer systems.”

The filing confirmed that the U.S. Secret Service then asked them to keep the matter confidential because the intruder might be caught if he or she doesn’t know TJX discovered the software.

2006, Dec 26 | TJX notified contracting banks and credit and debit card and check-processing companies of the suspected computer intrusion” and “on Dec. 27, 2006,

2006, Dec 27 | TJX first determined that customer information had apparently been stolen from their computer systems. Due to the technology utilized by the intruder, they were unable to determine the nature or extent of information included in these files.

“The technology used by the intruder has, to date, made it impossible for us to determine the contents of most of the files we believe were stolen in 2006,” the filing stated. “We believe that we may never be able to identify much of the information believed stolen.”

2007, Jan 17 | TJX announced the security breach publically.

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 the payment card issuer’s approval process, in which data (including the track 2 data) is transmitted to payment-card issuer’s without encryption.”

It is believed that the intruder had access to the decryption key and the decryption tool for the encryption software utilized by TJX. Encryption has no value when data isn’t encrypted, obviously, but credit cards can’t be processed when their numbers are encrypted. Hence, a smart crook will seek a way to get the data during that window of time when it’s in that state of being "in the clear”—that is, unencrypted.

It was possible that the TJX intruder stumbled on a decryption key stored with the encrypted data, as in shared-key cryptography, or had access to a certificate server.

“It’s incomprehensible that what amounts to a computer worm was placed on mission-critical systems at one of the world’s largest retailers and remained there—undiscovered—for 18 months. The scope of the theft is stunning,” she said. "My biggest fear is that it lays down a gauntlet for other would-be hackers, subtly daring them to ‘top this one. It also lays down the gauntlet for other retailers. This could be happening to you right now. PCI compliance and data security do not have obvious return on investment. Neither does paying taxes. But avoiding either can result in irreparable harm.”

2007, Jan 17 | TJX provided more details about what they believe happened that led to the card information of some 46 million consumers to get into unauthorized hands.

Veteran retail technology analyst Paula Rosenblum, a vice president with Retail Systems Alert Group, said the fact that the software went undiscovered for so long is most troubling.
In an interview with eWEEK, McAfee Chief Security Officer Dr. Martin Carmichael said that after he had read TJX’s take on the intrusion, he was curious if TJX was using data masking as articles indicated, or some sort of data encryption. Dr. Carmichael indicated there were different methods of encryption key methods: shared key, in which the sender and receiver of encrypted data both have the same key, or asymmetric, which uses a public/private key pair.

Shared-key encryption is inherently risky, since humans think up convenient but absurdly insecure places to store their keys. "We have seen … some companies that chose to use shared-key [encryption] that stores the key with the data," Carmichael said. "Which is outside of most policy. Sometimes ease of development can be [counter to] good security process."

In fact, Carmichael has seen keys in data files that are named "key to data."

Another encryption trap is the use of weak encryption. Original DES (Data Encryption Standard) encryption is now considered to be insecure for many applications, chiefly due to its 56-bit key size being too small. DES keys have been broken in less than 24 hours. Some analytical results point to theoretical weaknesses in the cipher, as well, although those have not been proven in practice. In May 2002, DES was superseded by AES (Advanced Encryption Standard) following a public competition, but DES remained in widespread use as late as 2004; Carmichael said it was "very common in a lot of applications."

2007, Feb 21
The mountains of data apparently taken from $15 billion retailer TJX were taken a lot earlier than had previously been announced, with the intrusions starting in 2005 and some of the impacted transactions dating back to 2003, TJX said in a statement issued Feb. 21.

2007, May
TJX reported May 15 that, in the three months leading up to April 28, it spent $12 million dealing with the data breach the company announced in January. That’s on top of $5 million the company said it spent in the previous three months to deal with the breach.

2007, Jun 22
Visa fined TJX: a $50,000 penalty for violating Visas Cardholder Information Security Program (CISP), an "egregious fine" of $500,000 "due to the seriousness of this security incident and the impact on the Visa system and the rest in retroactive monthly fines.

Visa said they would also fine TJX $100,000/month because of their "storage of prohibited data," and would continue to do so until compliance was obtained. Visa also reserved the right to further escalate fines and/or impose additional conditions, up to and including consideration of possible disconnection from the Visa payment system if TJX did not remediate track data storage in a timely manner."

2007, Sep 24
TJX has settled consumer lawsuits resulting from the breach by paying $6.5 million in attorney fees and offering consumers some programs aimed at compensating those directly impacted.

TJX has agreed to compensate consumers for any time they lost "as a result of the intrusion," but those calculations will assume a rate of $10 per hour.

The compensation also seems to be limited to $60 and will be in the form of $30 vouchers for making purchases at TJX only. Further, if a lot of consumers agree and "the total of such claims exceeds $7 million, the dollar amount of each voucher will be proportionately reduced."

Customers will get one $30 voucher. If they can prove costs exceeding $60, they will get two $30 vouchers.

Intruders intercepted wireless communications and used them to access the corporate TJX LAN and that the cyber-thieves might have broken into some job-application kiosks and used that as entry into the network.

No one has been charged with breaking into the network, and law enforcement officials have not identified any prime suspect. However, several people have been arrested on charges of trying to sell the information taken from TJX.
<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007, Oct 24</td>
<td>&quot;Beginning in July 2005, TJX experienced a massive intrusion into its computer systems, resulting in the largest data security breach in history and the compromise of an unprecedented amount of confidential non-public consumer personal data,&quot; said the plaintiff filing. &quot;Although TJX suggests that the breach only affected approximately 45.7 million accounts, in fact the breach during a period of 17 months affected more than 94 million separate accounts. To date, Visa has calculated the fraud losses experienced by issuers as a result of the breach to be between $68 million and $83 million on Visa accounts alone.”</td>
</tr>
<tr>
<td>Florida officials said the group used the increasingly common tactic of using the bogus credit cards to purchase gift cards and then cashing them at Wal-Mart and Sams Club stores. The group usually purchased $400 gift cards because when the gift cards were valued at $500 or more, they were required to go to customer service and show identification, Pape said.</td>
<td></td>
</tr>
<tr>
<td>2007, Nov 29</td>
<td>U.S. District Court Judge William Young denied the request to grant the banks class action certification, ruling that the many of the banks situations were too different from each other.</td>
</tr>
<tr>
<td>2007, Nov 30</td>
<td>That Visa-TJX statement said Visa would forgive &quot;a portion&quot; of the $880,000 that it had imposed on TJXs credit card processor. In exchange, TJX will pay an unspecified amount, not to exceed $40.9 million, to an unspecified number of plaintiff banks.</td>
</tr>
</tbody>
</table>
| 2007, Oct 25 | A TJX consultant found that not only was TJX not PCI-compliant, but it had failed to comply with nine of the 12 applicable PCI requirements. Many were "high-level deficiencies.”  
Revised complaint linked the bad security practices with the computer breach, which forced banks to take expensive actions to defend themselves. One key issue in civil cases such as this is whether the defendant can be shown to be simply careless or deliberately reckless. That distinction relies on showing what was likely in the defendants mind at the time of the acts that led to the data breach.  
Attorneys suing TJX want a jury to evaluate TJXs security professionalism.  
Attorneys for the banks indicated they would try to show that intent with internal TJX documents obtained during discovery. "TJX knew—and discussed internally prior to the breach—that its deficiencies in network and data security could lead to the exact losses incurred here in the many millions of dollars," said the filing. "Had TJX properly disclosed information about the extent of its noncompliance with network security requirements prior to the breach, then actions to correct the deficiencies and prevent the breach could have been taken," the filing said.  
"The data breach at TJX affected more than 100 million separate and distinct credit and debit card account numbers, more than twice the size of the next largest data breach in the history of the country.”  
The filings confirmed that both Visa and MasterCard have fined TJX. Visa issued "a substantial fine" in connection with the TJX data breach, dubbing it an "egregious violation” of security procedures. The sizes of the fines were not specified. |
| 2007, Oct 26 | Documents filed by Visa in federal court On Oct. 27, The Boston Globe quoted a TJX spokesperson as saying that TJX is now PCI compliant. No details were given. |
No one has been charged with breaking into the network, and law enforcement officials have not identified any prime suspect. However, several people have been arrested on charges of trying to sell the information taken from TJX.

TJX is also offering a plan for consumers who "returned merchandise to a TJX store without receipts and who were sent letters from TJX stating that TJX had specifically identified that their names, addresses and drivers license or military, state or tax identification numbers were believed to have been stolen in the intrusion." For those consumers—and TJX estimated that there are about 455,000 of them—TJX will pay for three years of credit monitoring (the settlement specifies the Equifax Credit Watch Gold with 3-in-1 Credit Monitoring product) and $20,000 worth of identity theft insurance.

TJX is also pledging to give those "Unreceipted Return Customers" the documented actual replacement cost of drivers licenses replaced between Jan. 17 and June 30.

In addition, there is the possibility of additional compensation for those customers who lost more than $60 from identity theft, but it excludes credit- and debit-card charges. The company also said that if the total of those "exceeds $1 million, such claims will be prorated."

References:
The Case, Evan Schuman, October, 2007