RUSSELL WALKER **KEL764**

Maxxed Out:
TJX Companies and the Largest-Ever Consumer Data Breach

In November 2005 Fidelity Homestead, a savings bank in Louisiana, began noticing suspicious charges from Mexico and southern California on its customers' credit cards. More than a year later, an audit revealed peculiarities in the credit card data in the computer systems of TJX Companies, an international retailer of apparel and home fashions.

TJX alerted the U.S. Secret Service, which was responsible for "maintaining the integrity of the nation's financial infrastructure and payment systems."[1] The U.S. Justice Department and the Royal Canadian Mounted Police later joined the investigation, which revealed that hackers had penetrated TJX's systems in mid-2005, accessing information that dated as far back as 2003. At the request of investigating officials, TJX delayed announcement of the intrusion until January 2007, when it admitted that hackers had compromised nearly 46 million debit and credit card numbers, the largest-ever data breach in the United States.[2]

TJX Companies

Based in Framingham, Massachusetts, TJX Companies was the parent company of more than 2,600 discount fashion and home accessories retail stores in the United States, Canada, and Europe. In the United States, TJX operated the TJMaxx, HomeGoods, Marshalls, and AJWright chains; in Canada it operated Winners, HomeSense, and STYLESENSE; in Europe a subsidiary oversaw the TKMaxx and HomeSense chains.

The majority of TJX's operations originated as part of Zayre, a retail conglomerate whose first store opened in the United States in 1956. In 1988 the Zayre chain of stores went bankrupt and a competing chain bought the stores and the Zayre name. The remainder of the operation rebranded itself TJX Companies and successfully expanded through acquisition and organic growth.

In its 2009 fiscal year, the company had net sales of $20.3 billion and was the thirty-eighth largest retailer—and second-largest fashion goods retailer—in the world.

[1] U.S. Secret Service, Criminal Investigations, http://www.secretservice.gov/criminal.shtml (accessed September 10, 2013).

[2] Later information indicated that as many as 94 million card numbers may have been compromised.

Credit Cards

Credit cards were the lifeblood of retail sales in the United States. As one trade magazine observed, "Major retailers have historically had somewhere between 45 percent and 50 percent of their annual sales on consumer credit."[3]

Paying with a credit card in the United States involved five parties:

- *Cardholder*—An individual who applied for and received a credit card.
- *Merchant*—A retailer that accepted one or more credit cards as payment for purchases made in person, online, or by telephone.
- *Acquiring bank*—A bank that processed credit card transactions for merchants and deposited payments into their accounts.
- *Issuer* (also called *issuing bank*)—A financial institution that issued credit cards to cardholders, billed cardholders for repayment, and assumed the risk of fraud and nonpayment (see **Exhibit 1** for top issuers in the United States).
- *Credit card association*—An association that developed and marketed credit card brands such as Visa, MasterCard, American Express, and Discover, and established transaction terms for merchants that accepted them as payment. Credit card brands were licensed to issuers for a fee based primarily on the volume of transactions. Visa dominated the U.S. market, as shown in **Exhibit 2**.

The credit card payment and settlement process was handled as follows (see **Exhibit 3**):

1. A cardholder used a card to pay a merchant for a purchase made in person, online, or by telephone.
2. The merchant submitted the credit payment electronically to the acquiring bank (or the acquiring bank's processor) for approval. The merchant had previously established a credit card processing account with the acquiring bank.
3. The acquiring bank (or processor) used the appropriate card association's network (e.g., BankNet for MasterCard, VisaNet for Visa) to request approval from the issuer, which approved or declined the request based on the cardholder's current balance and creditworthiness. The purchase amount less interchange fee was transferred to the acquiring bank.
4. The acquiring bank relayed the approval to the merchant, deducted additional fees, and deposited the net amount in the merchant's account.
5. The cardholder received a bill from the issuer and paid the amount due without interest immediately or in multiple payments with interest over time.

For merchants in the United States the total fees involved in a credit card purchase ranged from 1 to 3 percent of the purchase price. Fees varied based on size, credit history, and type of transaction.

---

[3] Craig Guilot, "Plastic's Comeback?" *Stores*, February 2012.

Credit Card Data Security

In December 2004 American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. established the Payment Card Industry Data Security Standard (PCI DSS) to standardize credit card data security requirements for merchants. PCI DSS included twelve major requirements that regulated more than two hundred elements of a firm's security network and payments processing system. Compliance with PCI DSS was required as part of the agreement a retailer signed with the credit card association for each card it accepted. To encourage compliance, credit card associations used both penalties and incentives: for example, Visa fined merchants that did not comply and gave financial bonuses to those that were on track to compliance.

Credit card associations monitored conformity with PCI DSS, but the stringency of monitoring depended on the merchant's total transaction volume; for the largest merchants, monitoring required an annual on-site review by an approved auditor and quarterly system scans using approved software. In 2007 PCI DSS compliance among merchants that processed more than six million card transactions was 40 percent.[4]

Merchants criticized PCI DSS as "a tool to shift risk off the banks' and credit card companies' balance sheets and place it on others."[5] In 2009 the average large merchant spent approximately $5 million on PCI compliance.[6] Merchants asserted that the total cost of compliance was much greater than what it would cost credit card companies to employ better card technology.[7] Further, compliance costs fluctuated because the standards were updated nearly annually to keep pace with new technology and threats.

In 2009 the Ponemon Institute, a nonprofit organization focused on data protection and information security policy, surveyed 517 security experts about their views on PCI DSS and data security. The responses illustrated a lack of commitment to managing data security and weak support of PCI DSS despite security vulnerabilities:[8]

- 71 percent did not think their organization handled data security as a strategic initiative.
- 56 percent did not think PCI DSS compliance improved their organization's data security posture.
- 55 percent thought their organization's CEO lacked strong support for PCI DSS compliance efforts.
- 60 percent did not think their organization had sufficient resources to achieve compliance with PCI DSS.
- 79 percent reported at least one data breach.

---

[4] Jaikumar Vijayan, "Breaches Pushing Retailers to Adopt PCI," *Computerworld*, August 6, 2007.

[5] Stephanie Condon, "Retailers: Credit Card Data Inadequately Protected," *CNET*, March 31, 2009.

[6] Ponemon Institute, "2009 PCI DSS Compliance Survey," September 24, 2009, p. 5.

[7] "Security Expert Believes Banks, Not Merchants, Should 'Own Up' to Responsibility to Protect Data," *Cardline*, January 19, 2007.

[8] Ponemon Institute, "2009 PCI DSS Compliance Survey," p. 1.

Data Security at TJX

Like most retailers, TJX used wireless networks to transmit data between hand-held price-checking devices, cash registers, and the company's computer systems. In the 1990s all wireless transmissions were protected by the Wired Equivalent Privacy (WEP) security protocol, but in 2001 Wi-Fi Protected Access (WPA) became the new standard after experts demonstrated that hackers could defeat WEP's defenses with off-the-shelf tools.

In 2005 TJX was still using WEP for its wireless systems. In a 2005 e-mail message, TJX's chief information officer wrote, "I think we have an opportunity to defer some spending from FY07's budget by removing the money from the WPA upgrade, but I would want us all to agree that the risks are small or negligible."[9] An employee responded, "It must be a risk we are willing to take for the sake of saving money and hoping we do not get compromised."[10] Audits in September 2006 warned the company that it needed to update its wireless security system to WPA protection to comply with PCI security standards.

In February 2007 Visa further disclosed that TJX had been storing credit card numbers and expiration dates in its systems, which violated PCI DSS and contradicted TJX's annual reports. Even more serious was the fact that the hackers gained access to some of the data in unencrypted form, either because the data was never encrypted or because TJX had failed to protect access to the encryption algorithm.

Uncovering the Breach

Investigators found that the first major intrusion into TJX's system had occurred in the summer of 2005 at a Marshalls discount clothing store near St. Paul, Minnesota. The criminals used "war driving," a hacking method that involved a laptop, antenna, and mobile wireless connection to locate vulnerable wireless signals. Once the hackers exploited TJX's WEP-secured wireless signal and successfully broke into the network, they established a connection with the main TJX server in Framingham and uploaded their own program that extracted card numbers from the network traffic. That program remained in place for eighteen months.

Investigators discovered that the TJX hackers were part of a large, sophisticated international network that loaded blank cards from China with stolen card numbers and sold them online for $10 to $100 each. Buyers used the cards to withdraw money from ATMs or purchase merchandise they could later sell.

In the summer of 2007 officials gained access to a suspect's hard drive in Turkey and identified the program on the drive as the same one used in the TJX intrusion. Messages between the suspect and his affiliates in the United States linked the crime to a well-known hacker whose username, "Soup Nazi," referenced a character from the American television show *Seinfeld*. The Secret Service knew the username well.

"Soup Nazi," real name Albert Gonzalez, had been arrested in 2004 as part of the Secret Service's Operation Firewall, a major investigation into a global network of credit card fraud. Gonzalez escaped prosecution after agreeing to become an informant. In March 2010 he was

[9] Donna Goodison, "TJX E-Mails Tell the Tale: Execs Knew of Info Security Flaws," *Boston Herald*, November 28, 2007.
[10] Ibid.

found guilty of hacking the TJX system and aiding and abetting other criminal intrusions. Gonzalez was sentenced to twenty years in prison.

Liability Questions

Following TJX's announcement of the data loss, affected parties filed lawsuits in an attempt to recoup their costs. The question of liability was complicated because there were no laws defining who was liable when a retailer that was not in compliance with PCI DSS lost credit card data. "Under current law, financial institutions (FIs) that issue the debit or credit cards often ultimately wind up footing the bill for both fraud-related losses and costs of issuing new cards and/or accounts for their customers . . . . FIs have also been involved in lobbying efforts designed to statutorily shift fraud losses and associated costs away from FIs to the entities actually responsible for the data security breach. A legal fight is brewing in both the courts and legislatures over who will ultimately bear the losses of identity theft–related fraud."[11]

The U.S. government had an interest in minimizing fraud and maintaining confidence in electronic payments so the public could continue to benefit from an efficient, credible payments system.[12] However, a national law covering credit card data security did not exist because legislators and industry analysts predicted companies would treat any legislation as a baseline for action and not look for reasons to advance security.[13] In any case, the slow pace of legislative change likely would have made it difficult for government-mandated standards to keep pace with new technology. Free market supporters opposed legislation because they believed companies that failed to enact proper standards would suffer not only from legal repercussions but also from reduced sales to wary consumers.

However, a lack of information about credit card security at retailers made it nearly impossible for consumers to choose to patronize stores with the best security practices; as a result, retailers found it difficult to charge higher prices to pay for better data security and often chose not to invest in it.[14] The situation was exacerbated by the fact that apart from time spent resolving any instances of credit card fraud, American cardholders had essentially no liability for fraudulent charges and thus little incentive to demand information about their retailers' data security practices.[15]

In addition, cardholders, merchants, and other participants in the credit card payment network did not bear any of the costs of finding, prosecuting, and jailing those who committed fraud, as all taxpayers shared the cost for law enforcement. When one participant in the payment network paid full costs for good security practices, it only received a portion of the benefits; conversely, when a breach occurred due to a weak link in the chain, the rest of the network had to share the costs. For example, when one U.S. retailer or merchant experienced a data breach, credit card issuers would

---

[11] Erin Fonté, "Who Should Pay the Price for Identity Theft?" *Computer and Internet Lawyer* 25, no. 2 (February 2008): 1–11.

[12] Stacey L. Schreft, "Risks of Identity Theft: Can the Market Protect the Payment System?" Federal Reserve Bank of Kansas City Economic Review (Fourth Quarter 2007), p. 26.

[13] "Retailer TJX Suffers Data Breach; PCI Compliance Unknown," *Warren's Washington Internet Daily* 8, no. 12 (January 19, 2007).

[14] Schreft, "Risks of Identity Theft," p. 24.

[15] An individual who is the victim of identity theft will spend an average of twenty-one hours resolving the issue. See Javelin Strategy & Research, "2010 Identity Fraud Survey Report: Consumer Version," February 2010, https://www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraudSurveyConsumer.pdf.

attempt to charge the merchant for the financial impact.[16] Because of increases in breach complexity and the way breaches were experienced, the actual amount of losses in breaches varied and generally were on the rise. However, data-breach liability contracts between banks and merchants did not clearly outline responsibility in sufficient detail, resulting in many breach cases being settled or adjudicated.

TJX Impact

In 2009 the average total cost to a merchant for a data breach was $6.75 million, or $204 per compromised record. At that rate the cost to TJX of 46 million compromised records would have exceeded $9 billion. Through the end of 2009 TJX reported expenses and reserves for probable losses of $171.5 million.

Although the Federal Trade Commission (FTC) did not have the power to impose a fine on TJX, it settled with the company after charging it with engaging "in practices that, taken together, failed to provide reasonable and appropriate security for sensitive consumer information."[17] As part of the settlement TJX agreed to an FTC review conducted by an independent third-party auditor every other year for twenty years to ensure the company is establishing and maintaining "a comprehensive security program reasonably designed to protect the security, confidentiality, and integrity of personal information it collects from or about consumers."[18]

A year after the announcement of the intrusion, TJX's first-quarter 2008 sales were up 6 percent and net income (after the settlement payouts) was down less than 2 percent compared with the previous year.[19] In 2009 net sales were up another 7 percent and TJX planned to expand its retail space by 5 percent in 2010 and 6 percent in 2011.[20]

Lesson Learned?

In May 2008 information about TJX's network security appeared on an Internet forum. A TJX employee revealed that blank passwords could be used on the company's servers and that the servers were always in administrator mode, "making it easy for hackers—or store employees—to have escalated privileges on the system once they entered it."[21] The employee alleged he brought the security problems to the attention of his store manager before he chose to blog about it.

TJX fired the employee and did not comment on the matter in public.[22]

---

[16] Richard J. Sullivan, "Risk Management and Nonbank Participation in the U.S. Retail Payments System," Federal Reserve Bank of Kansas City Economic Review (Second Quarter 2007), p. 28.

[17] Federal Trade Commission, "Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data," March 27, 2008, http://www.ftc.gov/opa/2008/03/datasec.shtm.

[18] Ibid.

[19] Larry Greenemeier, "The TJX Effect," *Information Week*, August 11, 2007.

[20] Elizabeth Holmes, "TJX's Profit Rises 58%," *Wall Street Journal*, February 24, 2010.

[21] Kim Zetter, "4 Years After TJX Hack, Payment Industry Sets Security Standards," *Wired*, July 17, 2009.

[22] Robert McMillan, "TJX Staffer Sacked After Talking About Security Problems," *CSO*, May 27, 2008.

Exhibit 1: Top 15 Issuers of General-Purpose Credit Cards in the United States

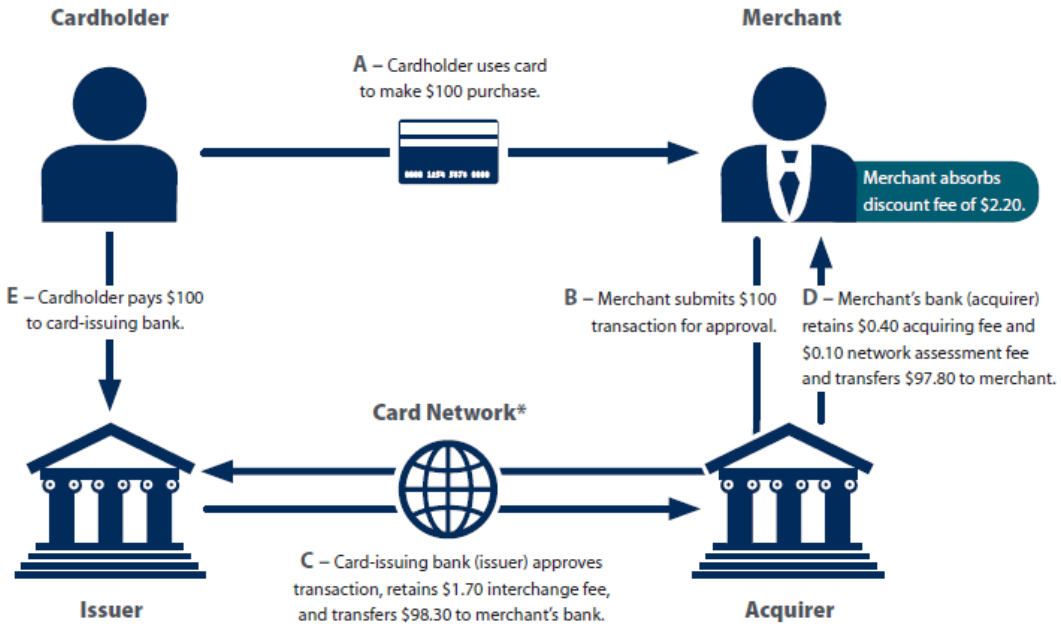
Issuer	Outstanding balance (US$ in billions)	Market Share (%)
Chase	166	19
Bank of America	145	16
Citi	103	12
American Express	78	9
Capital One	55	6
Discover	49	6
Wells Fargo	31	3
HSBC	25	3
US Bank	20	2
USAA	13	1
Barclays	11	1
Target	8	1
GE Money	7	1
PNC Bank	5	1
First National	4	1

Note: Based on January–June 2009 outstanding balances.

Exhibit 2: Market Share by Credit Card Network (as of February 2010)

	Number of Cards in Circulation (in millions)	*Percent (%)*	Credit Receivables Outstanding (US$ in billions)	*Percent (%)*	Purchase Volume (US$ in billions)	*Percent (%)*
Visa	302	*49.6*	366	*47.4*	764	*43.4*
MasterCard	203	*33.4*	268	*34.7*	477	*27.1*
American Express	49	*8.0*	86	*11.1*	420	*23.8*
Discover	54	*8.9*	53	*6.8*	100	*5.7*

Exhibit 3: Credit Card Authorization and Clearing and Settlement Process



Notes: Fees in this example are typical but not average. Dollar amounts, except network assessment fee, are from a similar flow chart in U.S. Government Accountability Office, "Credit Cards: Rising Interchange Fees Have Increased Costs for Merchants, but Options for Reducing Fees Pose Challenges," Report GAO-10-45, November 19, 2009.

The card network assesses additional fees on the issuer and the merchant.

Source: Tim Mead, Renee Courtois Haltom, and Margaretta Blackwell, "The Role of Interchange Fees on Debit and Credit Card Transactions in the Payments System," Federal Reserve Bank of Richmond Economic Brief, May 2011.