

May 4, 2007

PAGE ONE
BREAKING THE CODE

How Credit-Card Data Went Out Wireless Door

**Biggest Known Theft
Came from Retailer
With Old, Weak Security**

By **JOSEPH PEREIRA**

May 4, 2007; Page A1

The biggest known theft of credit-card numbers in history began two summers ago outside a Marshalls discount clothing store near St. Paul, Minn.

There, investigators now believe, hackers 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 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.

The \$17.4-billion retailer's wireless network had less security than many people have on their home networks, and for 18 months the company -- which also owns T.J. Maxx, Home Goods and A.J. Wright -- had no idea what was going on. The hackers, who have not been found, downloaded at least 45.7 million credit- and debit-card numbers from about a year's worth of records, the company says. A person familiar with the firm's internal investigation says they may have grabbed as many as 200 million card numbers all told from four years' records.

QUESTION OF THE DAY



¹ • Has your credit- or debit-card information ever been stolen?²

The previous record for card numbers exposed to thieves was 40 million. The TJX hackers also got personal information such as driver's license numbers, military identification and Social Security numbers of 451,000 customers -- data that could be used for identity theft. The company has apologized for its security lapse and beefed up its system. It rejects the 200 million figure as speculation, but

says it may never know the precise number. TJX deleted its own copies of the records stolen by the hackers and can't crack the encryption on files that the hackers left in its system.

The cost of the fraud may take years to count. Banks could spend \$300 million to replace cards from just one year's worth of stolen numbers, even though about half the numbers were expired and some were hidden in some of the stolen data. TJX, which discovered the fraud in December, privately projected \$20 million in fraudulent transactions from the breach, according to people familiar with the company's internal probe.

DOW JONES REPRINTS

 This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit: www.djreprints.com.

- [See a sample reprint in PDF format.](#)
- [Order a reprint of this article now.](#)

In March, police in Florida charged just one gang with buying some of the hacked TJX card data and using it to steal \$8 million in small transactions at **Wal-Mart Stores Inc.**, Sam's Club and other stores across the state. TJX-related fraud has occurred in at least six other states and at least eight countries from Mexico to China, bankers and investigators say. They are still working to find all the stolen numbers.

"All bankers are talking about these days is the TJX situation," says Boyd R. Boudreaux, chief executive of Fidelity Homestead Association, a small Louisiana savings bank that so far has been hit with \$23,000 in losses from the fraud. At a recent meeting of about 200 New England banking officials in Keene, N.H., a moderator asked who was still getting lists of compromised cards connected to the TJX breach. Nearly everyone raised their hands, says Daniel J. Forte, president of the Massachusetts Bankers Association, who was there. His association is suing TJX, in one of 21 U.S. and Canadian lawsuits seeking damages from the retailer.

The ease and scale of the fraud expose how poorly some companies are protecting their customers' data on wireless networks, which transmit data by radio waves that are readily intercepted. The incident also has renewed debate about who should be financially responsible. Banks that issue credit and debit cards so far have borne the brunt of the TJX losses, as opposed to the retailer or the credit-card networks such as Visa or MasterCard. Banks' lobbyists and some legislators have started pushing for laws to make the party that lets the data slip responsible for the costs.

Individual consumers so far have largely been covered for the fraudulent TJX charges. Debit-card holders legally can be held liable for unauthorized transactions if they don't report the fraud within 60 days, while credit-card customers can only be liable for the first \$50 in fraudulent charges.

Temporary Scare

Eleanor Dunning of Dana Point, Calif., got a temporary scare last fall when she opened her monthly Bank of America Visa bill: There were \$45,000 in charges for gift cards from a Wal-Mart in Florida. "What I saw was a whole page of \$450 charges, all identical and all in a row, all from the same place," she says. The bank removed the charges and issued her a new card, she said. When TJX's security breach was disclosed and she realized she was a victim of it, she decided to stop shopping at Marshalls.

Big Hacks

Some major breaches of credit- and debit-card data in the past three years:

- BJ's Wholesale Club Inc., March 2004
40,000 cards compromised
- DSW Retail Ventures Inc., March 2005
1.4 million cards compromised
- CardSystems Inc., June 2005
40 million cards compromised
- Dollar Tree Stores Inc., August 2006
800 cards compromised
- TJX Cos. July 2005–December 2006.
At least **45.7 million cards** compromised

TJX's breach-related bill could surpass \$1 billion over five years -- including costs for consultants, security upgrades, attorney fees, and added marketing to reassure customers, but not lawsuit liabilities -- estimates Forrester Research, a market and technology research firm in Cambridge, Mass. The security upgrade alone could cost \$100 million, says Jon Olstik, a senior analyst for Enterprise Strategy Group, a Milford, Mass., consulting firm, based on his conversations with industry experts and people familiar with the work being done.

TJX declined to comment on those numbers, but says it is undertaking a "thorough, painstaking investigation of the breach," hiring a team of 50 data security experts in December and taking a charge of \$5 million in its first fiscal quarter. It says it will also pay for a credit-card fraud monitoring service to help avert identity theft for customers whose

Social Security numbers were stolen. "We believe customers should feel safe shopping in our stores," says a letter from Chief Executive Carol Meyrowitz posted on TJX's Web site.

When wireless data networks exploded in popularity starting around 2000, the data was largely shielded by a flawed encoding system called Wired Equivalent Privacy, or WEP, that was quickly pierced. The danger became evident as soon as 2001, when security experts issued warnings that they were able to crack the encryption systems of several major retailers.

By 2003, the wireless industry was offering a more secure system called Wi-Fi Protected Access or WPA, with more complex encryption. Many merchants beefed up their security, but others including TJX were slower to make the change. An auditor later found the company also failed to install firewalls and data encryption on many of its computers using the wireless network, and didn't properly install another layer of security software it had bought. The company declined to comment on its security measures.

The hackers in Minnesota took advantage starting in July 2005. Though their identities aren't known, their operation has the hallmarks of gangs made up of Romanian hackers and members of Russian organized crime groups that also are suspected in at least two other U.S. cases over the past two years, security experts say. Investigators say these gangs are known for scoping out the least secure targets and being methodical in their intrusions, in contrast with hacker groups known in the trade as "Bonnie and Clydes" who often enter and exit quickly and clumsily, sometimes strewing clues behind them.

The TJX hackers did leave some electronic footprints that show most of their break-ins were done during peak sales periods to capture lots of data, according to investigators. They first tapped into data transmitted by hand-held equipment that stores use to communicate price markdowns and to manage inventory. "It was as easy as breaking into a house through a side window that was wide open," according to one person familiar with TJX's internal probe. The devices communicate with computers in store cash registers as well as routers that transmit certain housekeeping data.

After they used that data to crack the encryption code the hackers digitally eavesdropped on employees logging into TJX's central database in Framingham and stole one or more user names and passwords, investigators believe. 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, probes say.

Encrypted Messages

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. The company says the hackers may even have lifted bank-card information as customers making purchases waited for their transactions to be approved. TJX transmitted that data to banks "without encryption," it acknowledged in an SEC filing. That violates credit-card company guidelines, experts say.

While the hackers were stealing the data, they were selling it on the Internet on password-protected sites used by gangs who then run up charges using fake cards printed with the numbers, investigators say.

The problems first surfaced at credit-card issuers such as Fidelity Homestead, the Louisiana savings bank. Its customers were dealing with the aftermath of Hurricane Katrina when they began seeing strange transactions on their credit-card bills in November 2005, says Richard Fahr, Fidelity's security officer. First there were unauthorized transactions from Wal-Mart stores in Mexico, and then fraud started surfacing in Southern California, Mr. Fahr says.

Using bogus debit cards containing the data of just a handful of customers, thieves purchased \$5,600 worth of goods from Jan. 18 to Jan. 21, 2006. Over the four-day period, they made 25 shopping trips, moving among California supermarkets, department stores, a drug store and a videogame retailer, ringing up charges ranging between \$57 and \$561. The real cardholders were in Louisiana at the time, Mr. Fahr said.

Fidelity had no idea how the thieves had managed to obtain the debit-card data. "At that time TJX wasn't even in my vocabulary," he says.

Last fall, a spate of fraudulent card purchases appeared in Florida, where police now say a band of 10 thieves traveled in rented cars purchasing gift cards from Wal-Mart and Sam's Club stores, using bogus credit cards stolen from hundreds of TJX customers. Within four months, the gang bought \$8 million worth of gift cards and used them to buy flat-screen TVs, computers and other electronics across 50 of the state's 67 counties.

"They covered a lot of territory in a relatively short period of time," says Dominick Pape, a special agent with the Florida Department of Law Enforcement. The thieves gradually became bolder, with one of them eventually making \$35,000 in fraudulent purchases in a single day, police said.

Marilyn Oliver, of San Marcos, Calif., received a phone call from Bank of America alerting her that 40 \$400 gift cards had been purchased with her Visa card from cashiers at a single Florida Wal-Mart. "It sort of unnerves you," she says. "I'm very cautious, I shred everything."

Suspicious Purchases

A Wal-Mart clerk in Gainesville, Fla., eventually became suspicious of multiple gift-card purchases and alerted authorities, who reviewed store surveillance tapes and card transaction data at numerous Wal-Mart outlets before making arrests.

As the stolen TJX numbers were being used in Florida, the company was getting a stern warning about its poor security from a routine audit. The auditor told the company last Sept. 29 that it wasn't complying with many of the requirements imposed by Visa and MasterCard, according to a person familiar with the report. The auditor's report cited the outmoded WEP encryption and missing software patches and firewalls.

Then on Dec. 18, another auditor found anomalies in the company's card data. At that point, TJX hired forensics experts from International Business Machines Corp. and General Dynamics Corp. and notified the U.S. Secret Service, which spent a month trying to catch the hackers in the act. But the data thefts stopped and the hackers had obscured their whereabouts by using the Internet addresses of private individuals and public places such as coffee houses. Investigators did find traces of the hackers: altered computer files, suspicious software and some mixed-up data such as time stamps in the wrong order.

On Jan. 17, the company announced its systems had been hacked, affecting "a limited number of credit and debit card holders." It began sending lists of compromised numbers to credit-card issuers as it pored through the data. Some fraudulent activity has continued to pop up this year.

'Hot Lists'

Only last month did Fidelity in Louisiana find out the fraudulent charges in 2005 were linked to the TJX breach, when its card numbers showed up on one of TJX's "hot lists" of stolen cards. New lists keep arriving, and losses for the small bank have climbed from about \$7,000 to about \$23,000. "The fraud cuts

right into our profits," says Fidelity's Mr. Fahr. He says the credit union has asked Visa to reimburse it for the losses, but the credit-card association so far hasn't done so. Visa declined to comment.

Chuck Bower, the chief technical officer of Middlesex Savings Bank, Natick, Mass., says about 18,000 of its Visa debit cards were stolen by TJX thieves, with "at least three dozen claims of fraudulent activities," mostly committed in January and February. The thefts have occurred in Italy, Australia, Mexico and Japan, Mr. Bower reports. Robert Mitchell, chief financial officer of the retail division of Eagle Bank Corp., in Lowell, Mass., says 1,300 of its MasterCards were compromised. The bank has replaced all of them.

Lobbying by banking associations since disclosure of the TJX breach has helped persuade lawmakers in several states and in Congress to consider new legislation. One bill in Massachusetts would impose full financial responsibility for any fraud-related losses, including costs of reissuing of cards, on companies whose security systems are breached. Another bill, in Minnesota, would bar any company from storing any consumer data after a transaction is authorized and completed.

Massachusetts Rep. Barney Frank, chairman of the House Financial Services Committee, said in March he believes Congress will move to require a company responsible for allowing a breach to bear the costs of notifying customers and reissuing cards.

Write to Joseph Pereira at joe.pereira@wsj.com³

URL for this article:

<http://online.wsj.com/article/SB117824446226991797.html>

Hyperlinks in this Article:

(1) <http://forums.wsj.com/viewtopic.php?t=463>

(2) <http://forums.wsj.com/viewtopic.php?t=463>

(3) <mailto:joe.pereira@wsj.com>

Copyright 2007 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.