

Hackers Tap 40 Million Credit Cards

By [Joseph Menn](#)

[June 18, 2005](#) in *print edition A-1*

In the largest reported security breach of personal financial information, hackers infiltrated the computers at a Tucson credit card processing center and stole as many as 40 million card numbers, it was disclosed Friday.

MasterCard International said card numbers and expiration dates were harvested by a rogue program planted inside the computer network at CardSystems Inc., one of the firms that process merchant requests for credit card authorization. When a retailer swipes a customer's card, the information goes to companies such as CardSystems for approval before getting passed along to banks.

At least 68,000 accounts have had fraudulent charges posted to them, said MasterCard Vice President Linda Locke. Most credit card companies reverse bogus charges that are reported to them. Social Security numbers and other personal information were not taken.

The attack exposed the numbers of 13.9 million MasterCards and an unknown number of other brands of cards. Atlanta-based CardSystems processes \$15 billion in charges annually for MasterCard, Visa USA, American Express, Discover and other cards. Visa did not return a call seeking comment.

"I think all four [of the major card issuers] will be tainted," said Chris Hoofnagle, West Coast director of the Electronic Privacy Information Center, a Washington research group that studies civil liberties in the digital age. "This is the biggest security breach by far."

Hackers and identity thieves from around the world trade and sell pilfered credit card numbers in online chat rooms, making it relatively easy for a single big theft to affect thousands of cards quickly. That also makes it more difficult to catch the culprits.

MasterCard, which uncovered the incursion and announced it Friday (June 17, 2005), revealed few details about the fraud and how and when it was discovered. The company would not divulge the dollar amount of the fraud uncovered so far or say when the improper charges began.

"Several banks reported atypical patterns of fraud" this week, Locke said. "We traced disparate patterns of fraud back to CardSystems." After security firm CyberTrust Inc. examined the computers there, she said, "we believe that a hacker intruded and installed some malicious code that captured card information."

The FBI is investigating.

MasterCard said CardSystems had not been using industry safeguards at its Tucson processing center, suggesting to analysts that the numbers had not been encrypted for protection. CardSystems did not return calls seeking comment.

"There's no excuse for this," said Avivah Litan, a Gartner Inc. expert on the security of financial data. "This takes the cake."

MasterCard's revelation is the latest in a series of reported data breaches that began this year with word that identity thieves had accessed sensitive information on at least 145,000 people tracked by data broker ChoicePoint Inc. Major security lapses also have been disclosed at LexisNexis, [Bank of America](#) Corp. and, most recently, Citigroup Inc., which said the financial information of 3.9 million customers was lost by United Parcel Service Inc.

The reports, spurred by a California law requiring notification of consumers put at risk, have driven a spate of congressional hearings and proposals for tighter regulation. On Thursday, for instance, a Senate panel heard members of the Federal Trade Commission call for a national disclosure law and mandatory encryption.

Several members of Congress said the latest incident underscored the need for legislation to tighten the control on personal information. Some legislators have proposed banning the sale of Social Security numbers, except to help law enforcement. Various proposals are working through the House and Senate.

"Hardly a week goes by without startling new examples of breaches of sensitive personal data reminding us how important it is to pass a comprehensive identity-theft prevention bill in Congress quickly," said Sen. Charles E. Schumer (D-N.Y.), who has sponsored a consumer data protection law.

MasterCard said it would support applying stricter rules to credit card processors.

As typically happens when credit card information is stolen, MasterCard is leaving it up to the banks that issued the cards to warn the cardholders. It declined to name the banks.

Those banks usually don't pass the information along because most pilfered numbers don't get used and because issuing new cards, as many customers would demand, can cost \$35 or more each. If all 40 million cards were replaced, that might cost more than \$1 billion.

"They could contain the damage," Litan said. "All they need to do is put a stop on those cards and issue new ones. But of course they won't do that because it costs too much money."

All credit card holders should carefully review their statements because they will be reimbursed only if they report errant charges. And some consumer advocates recommend requesting a new card as a matter of course as often as every six months to guard against fraud.

Although cardholders won't be liable for fraudulent charges they report, they risk having their credit score damaged as well as spending hours setting the record straight.

Without mass replacement of the credit cards, the biggest financial losers could be retailers. The credit card associations hold merchants responsible for most fraudulent charges, even though they and their member banks often don't share their watch lists of compromised cards.

Retailer resentment of those fraud policies and of the fees they pay credit card processors is growing and could lead to class-action litigation, Litan said.

Financial data processors are obvious targets for hackers. In what previously may have been the largest known breach of credit card data, 8 million numbers were taken from a similar firm, Data Processors International, in 2003.

(BEGIN TEXT OF INFOBOX)

Exposed data

Personal data breaches in 2005:

Feb. 15: Data collection firm ChoicePoint Inc. begins notifying about 35,000 Californians that their personal information may have been compromised on ChoicePoint databases.

Feb. 16: ChoicePoint acknowledges that data on 110,000 Americans outside of California may have been stolen as well.

Feb. 25: Bank of America Corp. announces that it had lost computer tapes with personal information for 1.2 million credit cards used by federal employees.

March 8: Shoe retailer DSW Inc. says the credit card numbers of more than 100,000 customers may have been accessed illegally.

March 9: Information broker LexisNexis says identity thieves had tapped into data on more than 30,000 people through one of its databases.

April 12: LexisNexis announces that the number of people whose data was compromised is closer to 310,000 than 30,000.

April 14: Personal data for more than 180,000 MasterCard holders are reported stolen from Polo Ralph Lauren Corp.

April 18: DSW says as many as 1.4 million credit card numbers were exposed, rather than the 100,000 estimated earlier.

June 6: Citigroup Inc. says computer tapes containing Social Security numbers of 3.9 million customers were lost by United Parcel Service Inc.

Friday: MasterCard International says a security flaw may have exposed as many as 40 million credit card accounts to fraud.

Sources: Associated Press, Times research

Los Angeles Times