

40 million cards hit by data theft**Large-scale hacking raises fresh questions about protection of cardholder information**- [Carrie Kirby and Jenny Strasburg, Chronicle Staff Writers](#)

Saturday, June 18, 2005

Holders of more than 40 million credit cards are vulnerable to financial fraud because their credit card information was stolen from an Arizona company that processes transactions for Visa, MasterCard, American Express and Discover, it was disclosed Friday.

A computer hacker infiltrated the network of CardSystems Solutions Inc. in Tucson, apparently in late 2004, according to MasterCard. The credit card giant said it has given its member banks lists of card numbers involved in the theft so they can protect their customers.

But experts say credit card users should be protected by their customer policies and don't need to take action unless they notice fraud on their accounts or receive a warning that they were part of the breach.

The theft is by far the biggest in a recent stream of security breaches and mishaps that have raised questions about whether the financial and personal data of cardholders and bank account holders is safe with the corporations and government entities that store it in databases.

Data aggregator ChoicePoint grabbed the nation's attention in February when it disclosed that it apparently had lost extensive details about 145,000 Americans to criminals, and many companies, most recently Citigroup, have admitted losing tapes containing information from millions of consumers. The breaches prompted congressional hearings on the issue this week, and numerous bills have been introduced aiming to improve consumers' data security.

The majority of the exposed accounts carry the Visa brand.

Visa USA, based in San Francisco, said Friday that roughly 22 million Visa accounts had been compromised. Visa first learned about the problem two weeks ago from CardSystems, and Visa was given access to the affected account numbers Thursday night, said spokeswoman Rhonda Bentz.

The breach was discovered in late May, when MasterCard's fraud detection system began connecting fraudulent transactions, MasterCard spokeswoman Jessica Antle said. The card companies worked with the Federal Bureau of Investigation and other law enforcement agencies, as well as with private forensics firms, to investigate the breach. That inquiry is still going on. Antle would not say whether there were suspects.

In the Arizona situation made public Friday, Visa and the other credit card firms were asked by the FBI not to discuss the breach publicly and had no plans to do so immediately, Bentz said.

"We're concerned that this might compromise the investigation," she said regarding Friday's release of information.

MasterCard would not comment on whether it had agreed not to release the information, but spokeswoman Antle said, "We had a responsibility to share this information with the marketplace."

Friday, Visa started contacting banks that issue the affected cards, a process that will take several days. Neither MasterCard nor Visa have immediate plans to contact individual cardholders whose information was compromised.



Card companies stressed that federal law and the firms' policies dictated that cardholders were not liable for losses stemming from unauthorized transactions.

American Express said that it was monitoring card activity but that "an extremely small number" of its cardholders were affected. Spokeswoman Judy Tenzler didn't give a number but said the American Express transactions potentially exposed by the breach involved less than one-half of 1 percent of the firm's U.S. purchase volume.

'Don't be worried'

Californians affected by the Arizona breach should receive letters warning that their cards were compromised, as is required by state law. However, it's not clear if those letters will come from issuing banks or from CardSystems. Until those letters arrive, people should not panic, advised Beth Givens, director of the Privacy Rights Clearinghouse, a nonprofit organization in San Diego.

"I'm telling people don't be worried, you are not going to be held responsible if your credit card is among those that hit," because credit card companies are required to reimburse customers for losses due to fraud after the first \$50, and most companies have a policy of waiving the first \$50 as well. "Wait to hear from your credit card company and don't worry about it."

One proactive step concerned card users can take right away is to carefully check credit card accounts for unfamiliar transactions by logging onto their accounts online, calling the card issuers or reviewing the paper statements that comes in the mail.

Credit card numbers, bank account numbers, Social Security numbers and other personal data are in great demand among perpetrators of fraud, who can use the information to profit in a number of ways, such as creating counterfeit credit cards or opening new credit accounts in victims' names.

In this case, victims should not be at risk for identity theft, because the information stolen appears to be transaction data taken from the strip on the back of cards, which generally does not include sensitive details such as Social Security number and date of birth that can be used to open new accounts in a person's name.

Demand for bigger and bigger heists of consumer data is driven by burgeoning online black markets, where such information is bought and sold. Years ago, hacking was a hobby in which computer enthusiasts broke into networks out of curiosity. But more and more, law enforcement officials say, hackers are in it for the money, and the barrage of high-profile security breaches is evidence of that. They're also organizing into gangs, which David Thomas, chief of the Federal Bureau of Investigation's computer intrusion squad, called "nontraditional organized crime" in a recent interview

"They can sell these cards (online) for a few dollars apiece," said Avivah Litan, an analyst for Gartner Research who advises merchants and banks on Internet security and fraud. "I bet this is going to yield \$200 million to \$350 million" for the thieves, who will probably sell it in parcels of 10,000 or so card numbers.

Costly for banks, merchants

Criminals who buy stolen credit card numbers then try to profit by buying merchandise -- often computer equipment -- on the Internet or by collaborating with dishonest merchants or card processors to get goods or cash advances from the cards.

The breach will prove far more costly for card-issuing banks and merchants. The banks will have to close and reissue any accounts where fraud is detected, at a cost of \$10 to \$25 per account, while the merchants may not get paid for merchandise bought with the stolen cards.

CardSystems Solutions is one of several hundred transaction processors that route card information from merchants to banks. The largest companies in the field are First Data Corp. of Greenwood Village, Colo.;

Total Systems of Columbus, Ga.; and Nova Information Systems of Atlanta. CardSystems is a large player in the industry but not among that top tier, Litan said.

Neither MasterCard nor Visa would say what was lacking in the firm's security, except to say it was out of compliance with their minimum security standards. But experts say that in order for a hacker to steal and use the information, it could not have been encrypted, a basic step that is required by the card companies' standards.

Even though it was CardSystems that failed to comply with the policy, MasterCard and Visa should share the blame, Litan said.

"They weren't actively monitoring compliance," Litan said. "It wouldn't take that much to send an auditor to see if that data is encrypted or not."

The Federal Trade Commission, the agency charged with regulating the credit-card industry, also mandates minimum standards a card-processing firm must meet. Those standards aren't necessarily the same as those defined by the card companies, an FTC spokeswoman said.

If the FTC finds through an investigation that a card-processing firm did not take reasonable steps to protect the confidentiality of cardholders, the FTC can seek penalties through federal court.

MasterCard said in its release that it was giving CardSystems "a limited amount of time to demonstrate compliance with MasterCard security requirements."

E-mail the writers at ckirby@sfgchronicle.com and jstrasburg@sfgchronicle.com.

Page A - 1

URL: <http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2005/06/18/CREDIT.TMP>

[©2005 San Francisco Chronicle](#)