Citibank ATM breach reveals PIN security problems

By JORDAN ROBERTSON, AP Technology Writer Tue Jul 1, 4:39 PM ET

SAN JOSE, Calif. - Hackers broke into Citibank's network of ATMs inside 7-Eleven stores and stole customers' PIN codes, according to recent court filings that revealed a disturbing security hole in the most sensitive part of a banking record.

The scam netted the alleged identity thieves millions of dollars. But more importantly for consumers, it indicates criminals were able to access PINs — the numeric passwords that theoretically are among the most closely guarded elements of banking transactions — by attacking the back-end computers responsible for approving the cash withdrawals.

The case against three people in U.S. District Court for the Southern District of New York highlights a significant problem.

Hackers are targeting the ATM system's infrastructure, which is increasingly built on Microsoft Corp.'s Windows operating system and allows machines to be remotely diagnosed and repaired over the Internet. And despite industry standards that call for protecting PINs with strong encryption — which means encoding them to cloak them to outsiders — some ATM operators apparently aren't properly doing that. The PINs seem to be leaking while in transit between the automated teller machines and the computers that process the transactions.

"PINs were supposed be sacrosanct — what this shows is that PINs aren't always encrypted like they're supposed to be," said Avivah Litan, a security analyst with the Gartner research firm. "The banks need much better fraud detection systems and much better authentication."

It's unclear how many Citibank customers were affected by the breach, which extended at least from October 2007 to March of this year and was first reported by technology news Web site Wired.com. The bank has nearly 5,700 Citibank-branded ATMs inside 7-Eleven Inc. stores throughout the U.S., but it doesn't own or operate any of them.

That responsibility falls on two companies: Houston-based Cardtronics Inc., which owns all the machines but only operates some, and Brookfield, Wis.-based Fiserv Inc., which operates the others.

A critical issue in the investigation is how the hackers infiltrated the system, a question that still hasn't been answered publicly.

All that's known is they broke into the ATM network through a server at a third-party processor, which means they probably didn't have to touch the ATMs at all to pull off the heist.

They could have gained administrative access to the machines — which means they had carte blanche to grab information — through a flaw in the network or by figuring out those computers' passwords. Or it's possible they installed a piece of malicious software on a banking server to capture unencrypted PINs as they passed through.

What that means for consumers is that their PINs were stolen from machines that showed no signs of tampering they could detect. In previous PIN thefts, thieves generally took steps that might draw notice — sending "phishing" e-mails, for example, or installing false-front keypads or even tiny cameras on ATMs.

Getting the PINs is a key step for identity thieves. It lets criminals encode stolen account information onto blank ATM cards and withdraw piles of cash from compromised accounts.

Don Jackson, director of threat intelligence for SecureWorks Inc., said he has seen an "alarming" spike in the number of attacks on back-end computers for ATM networks over the past year.

"This was fairly large, but I don't think it's anything out of the ordinary — these kinds of scams go on every day," Jackson said. "What makes this case unique is the sheer luck of happening upon these guys and catching them red-handed. But there are a whole lot of other ATM and PIN compromises going on that aren't reported."

The alleged plot is outlined in court papers supporting the prosecution of three people — Yuriy Rakushchynets, Ivan Biltse and Angelina Kitaeva. They were indicted in March on two counts each of conspiracy and fraud. Prosecutors say their activities generated at least $2 million in illegal profits.

Defense lawyers for all three people did not return calls for comment, and it was not clear where they had been living. The main defendant, Rakushchynets, was described as having Michigan and Florida's driver licenses in a February FBI affidavit for an arrest warrant.

Citibank, part of Citigroup Inc., has declined to comment on the technique or how many customers' accounts were compromised. It said it notified affected customers and issued them new debit cards.

"We want our customers to know that, consistent with legal requirements, we do not hold them responsible for fraudulent activity in their accounts," the bank said in a statement.

Cardtronics said it is cooperating with authorities but otherwise declined to comment. Fiserv spokeswoman Melanie Tolley said the intrusion didn't happen on Fiserv's servers.

"Fiserv," she said, "is confident in the integrity and security of our system."