Indictment of card hacker unlikely to end thefts

August 18 2009, By JORDAN ROBERTSON , AP Technology Writer

(AP) -- This week's indictment of a hacker believed responsible for the biggest retail-store data breaches in U.S. history doesn't necessarily make shoppers safer from having their credit card numbers plundered.

Accomplices to the crimes are believed to be on the loose in Russia or other countries where U.S. authorities are less likely to get them. And the underlying security holes mined by the hackers still exist in many payment networks.

Albert Gonzalez, a Miami hacker who once worked as a government mole tracking down identity thieves, is accused of playing a critical role in all the largest credit-card heists on record.

With Monday's indictment of Gonzalez on conspiracy charges in U.S. District Court in New Jersey, the Justice Department says he helped steal 130 million card numbers from payment processor Heartland Payment Systems, 4.2 million card numbers from East Coast grocery chain Hannaford Bros. and an undetermined number of cards from 7-Eleven. He was previously charged in other computer break-ins, most significantly at TJX Cos., the chain that owns discount retailers T.J. Maxx and Marshalls, in which as many as 100 million accounts were lifted.

Gonzalez is in jail and awaiting trial next month in New York for allegedly helping to hack the computer network of the Dave and Buster's restaurant chain. Attorneys for Gonzalez did not comment to The

Associated Press.

The fact that hundreds of millions of card numbers could be stolen from retailers illustrates the flaws in a payment system that's built more for speed than security, as an Associated Press investigation found this year. For instance, credit and debit card numbers are not always encrypted as they move from retail stores to banks for approval.

Consumers don't directly pay the costs of most fraud. Banks and retailers eat those charges. But consumers bear it indirectly, in the form of higher prices.

According to prosecutors, Gonzalez and his associates exploited vulnerabilities that remain widespread. Among them: flaws in the way retailers' computers handle requests in the so-called Structured Query Language (SQL), which is used to manage data - such as credit card information - stored in databases. Hackers who detect these holes can trick databases into coughing up more information than they should.

The vulnerability sometimes can be exploited as simply as entering a specially crafted command into, say, a search box on a badly configured Web site. Instead of returning normal search results, the site would surrender confidential information or allow a hacker to place malicious programs on the site.

Authorities allege Gonzalez and the others infiltrated the Heartland, Hannaford and 7-Eleven computer networks using SQL-based attacks.

In a statement Tuesday, 7-Eleven Inc., which hadn't commented on its breach before, said the attack affected ATMs operated by a third party inside its stores and lasted for 12 days in 2007. That is likely referring to an attack in which criminals infiltrated Citibank's network of ATMs inside 7-Eleven stores and stole the mother lode in the ID theft world:

customers' PIN codes. Neither 7-Eleven nor Citibank would elaborate Tuesday.

Security experts also noted that Gonzalez's latest indictment charges two unnamed co-conspirators who live "in or near Russia" and allegedly helped with the attacks.

Dan Clements, president of CardCops, which tracks stolen credit card data online, called it a "cleverly written indictment" that suggests the government might be trying to squeeze its former informant for more information about Hacker 1 and Hacker 2. However, extraditing those suspects is unlikely, Clements added.

"We are not safe," Clements said. Gonzalez is "here on U.S. soil. That was his big flaw. If he were anywhere else, he's not going to jail."

Ori Eisen, founder of Scottsdale, Ariz.-based security firm 41st Parameter and previously worldwide fraud director for American Express, added that Gonzalez is "most likely not the kingpin. The kingpin would not risk being in the United States. They operate out of the Ukraine or Russia, and they're former militants or ex-KGB who know their way around just enough not to get caught."

As for Gonzalez, "by no means will catching him stop what's going on out there," Eisen said.

Consumers don't have many options for monitoring whether the stores they frequent are good at protecting their card numbers. Stores aren't given public grades on their computer security, like the scores restaurants get on their cleanliness in some places. The best advice: Regularly check your credit reports for suspicious activity, and set free fraud alerts with the credit-reporting agencies.

In this case, the thieves might have failed by being too successful. It's hard to unload hundreds of millions of stolen credit card numbers on the black market.

Clements said criminals usually sell stolen card numbers in batches of 10,000 or less. That helps avoid drawing the attention of law enforcement and the card providers, which might replace cards pre-emptively if they see a mound of them being fenced. Many of the card numbers stolen in the breaches cited in the Gonzalez indictment have already been canceled and replaced.