

ATM Skimming Spree Investigated Authorities Suspect Link to International Crime Ring

Tracy Kitten, Managing Editor
September 2, 2011

Police investigators in Florida's Tampa Bay region say fraudsters are increasingly focusing their [skimming](#) attacks on bank branch ATMs.

According to the Pasco County, Fla., Sheriff's Department, at least 44 customers have been defrauded of at least \$26,000 in recent weeks, after their cards were skimmed at two walk-up ATMs at area banks.

Kevin Doll, public information director for the sheriff's department, says one of the attacks, reported by a Bank of America branch in Pasco County, remains under investigation. The suspect was captured by the ATM's surveillance system, but neither the suspect nor the skimming device has been located. Doll did not have details about the other incident, which hit a bank in neighboring Pinellas County.

"I'm not sure how Bank of America found out about the skimming incident that hit them," Doll says. "I don't know if customers reported fraudulent transactions, or if they caught it on the surveillance footage. ... We do believe it is skimming, however. In some of the video clips, you could actually see super glue in one of his hands, which we believe he used to attach the skimming device."

Authorities also believe the suspect was attacking the BofA branch at night, after business hours, and then returning the following morning, sometime around 3 a.m., to remove the device. How many days the attacks spanned has not been determined.

"He hit 44 different accounts that we know of," Doll says. "These cases I've seen at bank ATMs have been picking up. We think it's a possibility that it could be connected to an international crime ring, but that's all we're saying. We aren't commenting further on that."

[Jerry Silva](#), a financial fraud and card skimming expert at PG Silva Consulting, says the suspected link to organized crime could be telling. "It must be that they're connecting it to the M.O. of a previous event," he says.

The backing from international crime rings for skimming attacks waged on U.S. ATMs is increasingly common. "The individuals are often highly trained in Eastern Europe before they make their way to the U.S.," says John Buzzard of FICO's Card Alert Service. "Most of the individuals enter the U.S. illegally or on a temporary tourist visa and end up overstaying their welcome. One of the reasons we are seeing such a compression of non-U.S. citizens perpetrating these scams in the U.S. also has to do with our lack of smart-card practices." [See [Visa Pushes EMV in U.S.](#).]

Banks: Prime Skimming Targets

The international connection to ATM skimming incidents is well documented. Earlier this summer, federal authorities indicted a [crime ring](#) for its alleged involvement in a \$1.5 million ATM skimming scheme that targeted Citibank and JPMorgan Chase bank branches in New York, Chicago and Miami. [See [See 4 Charged with \\$1.5M ATM Skimming](#).]

Bank ATMs also are prime targets, especially when they are walk-up or drive-up machines. High transaction volumes coupled with easy access make them ideal for fraudsters. "The Tampa case so far is really typical," Buzzard says.

The average loss per cardholder comes out to about \$590, "which we see more often these days, meaning that the criminals prefer large withdrawals instead of numerous smaller ones," Buzzard adds. "The cards will be trashed as soon as the unauthorized withdrawal is completed, so they like to go big in one clean withdrawal before moving to their next cloned card."

Silva says it's not surprising that these ATMs were targets, and, like Buzzard, the losses are not shocking.

"Banks have always been targeted by skimming fraud," Silva says. "The amount isn't really excessive. Most debit cards have a \$500 per day withdrawal limit, so it does seem reasonable, if you think about multiday fraud and higher limits on some of the cards."

For Silva, the greater question is why banking institutions continue to get taken by skimming. "Why don't more banks have anti-skimming devices?" Silva asks. "Both problem and solution have been well documented by now. ... BofA is listed as one of the banks that were hit. You would think they would have completed their upgrades."

Many ATMs, when upgraded from IBM's legacy OS/2 platform to Microsoft Windows, were enhanced with skimming detection technology and, in some cases, anti-skimming hardware and software, such as card readers with jitter. The jitter feature aims to distort card



details when cards are read by the ATM, so that if a skimming device has been attached, the copied information is useless. In recent years, however, fraudsters have figured out how to get around the jitter. [See [ATM Skimming: How Effective is Jitter?](#).]

It's challenging for banking institutions and other ATM deployers to keep up. [Chuck Somers](#), vice president of ATM Security and Systems for Diebold Inc., says organized crime groups are focusing their attention on technical sophistication that exploits ATM vulnerabilities, especially at branch ATMs. "We expect that industry regulations will continue to increase to ensure that the proper safeguards are put in place to reduce the loss to the industry, and focus on protecting personal identification information," Somers says.

[Close Window](#)

BankInfoSecurity.com is your source for bank information security news, regulations, and education.