June 5, 2017

Stopping Skimmers

Protect Yourself at the ATM

As Americans hit the road for summer vacation season, many will visit an ATM expecting quick and easy access to their cash. Yet that convenience makes ATMs an easy, year-round target for fraudsters looking to steal your money.

Romanian citizen Ilie Sitariu, 37, and a co-conspirator who has since fled the United States did just that in 2015. From August through October, the Romanians traveled along the I-87 corridor in the Albany, New York area, going from bank to bank and secretly installing skimming equipment on ATMs—often at night, when their nefarious activities could go unnoticed.

Skimming typically requires two devices to be installed on an ATM or other card reader: one piece skims, or captures, data from a card's magnetic stripe, while an accompanying pinhole camera captures cardholders' PINs as they're entered. While Sitariu's devices were considered relatively primitive—two simple pieces of metal with a skimmer hidden in one and a camera hidden in the other—they were sophisticated enough to do damage. (Some skimming devices incorporate Bluetooth technology, so criminals can access the information remotely without having to return to the ATMs and remove the devices.)

The men left the skimming equipment in place at each machine for about a day before returning to collect it—along with the account numbers and PINs of those who had used the ATMs during that time. They then loaded that information onto another card and used it to pull cash out of the victims' accounts. The money was then loaded onto gift cards to help cover their tracks.

Some banks noticed the skimming devices right away, minimizing their losses, while others had their customers' accounts drained. At one bank, the fraudsters took $63,000. In total, they stole more than $127,000 from accounts at three banks.

Despite wearing hats and sunglasses while installing the skimmers, security footage from the various ATMs—taken during a relatively short time period at locations in close proximity to each other—helped officials identify the thieves. In these types of cases, data sharing between local law enforcement is critical to catching up to the criminals, as is alerting local banks before they are victimized.

“At the end of the day, greed gets to these people,” said Special Agent Paul Scuzzarella, one of the agents who worked the case from the FBI’s Albany Division. “They do too much at one time and eventually get caught.”

Sitariu, who lived in New York City, is now behind bars thanks to the collaborative work of the FBI, U.S. Secret Service, and law enforcement partners in New York. He pleaded guilty to bank fraud, access device fraud, and aggravated identity theft and was recently sentenced to four years in federal prison.

For skimming victims who find their money mysteriously missing, it’s like having your wallet stolen without it ever leaving your possession. Though banks do typically refund the money, skimming not only causes inconvenience to its victims, it costs everyone. Experts estimate card skimming costs consumers more than $1 billion annually.

Additionally, many ATM skimming cases are linked to Eurasian crime groups, and the stolen funds can wind up overseas as a funding source for international criminal activity, Scuzzarella said.

While law enforcement is constantly working to catch skimmers, the public should take basic precautions to protect against skimming at ATMs, gas stations, and other vulnerable card reader locations.

“You really should be cognizant of where you’re using one,” Scuzzarella said of ATMs. “If it’s in a hidden area in a building, like in a gas station around the corner, who knows who’s back there. If it’s in the main area, it’s less likely someone has tampered with that.”

Also, if you notice anything unusual on an ATM, don’t use it, Scuzzarella warned. He also noted that covering the ATM keypad could have helped thwart the skimmers in this case.

“I find myself checking more and more,” Scuzzarella said of his own ATM use. “When I log in, I notice if something looks different, if it seems as if there’s something that’s attached. Sometimes it’s not very noticeable.”