

Security Products

Negative Cash Flow

ATM skimming costs banks money and reputation

By John Pearce Jul 01, 2009



There is a growing and highly effective breed of bank robbers at work around the world. Money is not particularly safe and secure, and no city is immune.

This spring, police in Australia reported more than \$1 million was taken from about 40 bank ATMs in several cities. At least 10 suspected thieves, believed to be part of an international organization originating in Europe, have been arrested. More arrests are expected. Thousands of bank customers were likely affected.

Late last summer, a Seattle man opened his bank statement and found that \$2,000 was missing from his account—along with about \$700 in overdraft fees. Over a period of several days, someone withdrew funds at the rate of \$300 per transaction at ATMs the man said he had never visited.

A Staten Island, N.Y., firefighter noticed last fall that his bank account was about \$1,600 lighter than he expected. He had not withdrawn the money, nor had his wife. When he checked with his local bank branch, he learned that he, and more than 100 other bank customers, had fallen victim to high-tech thieves who may have taken more than \$100,000 over a single weekend from one neighborhood ATM.

Recently, employees from two banks in Bethlehem, Pa., found a sticky residue on their ATMs. That, along with \$20,000 missing from about 36 accounts from the two banks, led local police to believe that one or more hightech thieves had struck.

All of the real-life stories above highlight a practice known as ATM skimming. It is one of the financial industry's fastest-growing electronic crimes, now costing institutions and consumers \$8 billion annually, according to the U.S. Secret Service. There are indirect costs as well for law enforcement and financial institution security staffs to investigate, document and report these incidences of skimming. And skimming can affect any of the more than 400,000 ATMs in the United States.

A Growing Threat

Statistics from the global ATM Industry Association give a sense of the opportunity for skimming on an international basis.

- There are more than 1.7 million ATMs worldwide.
- About every six minutes, a new ATM is installed somewhere in the world.
- Annually, there are 40 billion worldwide ATM cash withdrawals.

ATM skimming is the electronic "bank job" of the decade, and its practitioners have become the modern-day Bonnie and Clyde. But unlike that legendary couple, skimmers choose card readers and

miniature cameras or keypad overlays rather than guns to steal personal financial information and money.

Skimming is a highly profitable crime with a relatively low risk of being caught. It is much easier to use an ATM to withdraw \$1,500 from someone's bank account than it is to steal a home entertainment system worth the same amount.

Internet sites offer skimming equipment and training guides for sale, which makes it very easy for criminals to become involved in financial identity theft. With a little practice, installing and removing the equipment is simple.

The Modern Bank Job

Many skimmers operate in organized gangs, taking large amounts of money from a few high-volume ATMs over a couple of hours and then moving to another location, often in another city. By moving so quickly, they are less likely to draw attention or be apprehended. With few exceptions, financial institutions are required to reimburse consumers' losses.

In a matter of seconds, criminals can place a skimming device on an ATM card reader that blends in with the machine's appearance and does not interfere with its operation. The device is able to read personal financial information from the magnetic stripe on the back of the consumer's card. A small wireless camera, concealed near the ATM fascia—or a keypad overlay—captures the user's PIN as it is entered. Information from the device and camera is sent wirelessly to the criminal, who is usually parked with a laptop computer nearby. The ATM user typically has no idea that his or her information has been compromised.

Criminals upload the stolen account information onto the magnetic stripes of purchased blank cards, cloning an inventory of duplicate credit/debit cards. They write the passwords on the face of the cards to keep them linked. These new cards allow the thieves to cash out debit accounts or use the information to complete Internet purchases. There also are electronic markets in which the cardholder's data can be sold to worldwide crime syndicates.

By the time the consumer receives a bank or credit card statement, notices the discrepancies and reports them to his or her bank, the skimmer is usually long gone, having left few traces behind for police to follow.

Criminals generally find it easier to attack unmanned ATMs, of which more than 250,000 are onsite at financial institutions. Since most banks are closed in the evenings and on weekends, criminals have plenty of time to install and remove their skimming equipment without interruption. Many off-premise ATMs are located in well-lit, 24-hour manned locations such as convenience stores or other retail environments.

Fighting Back

Financial institutions acknowledge that skimming is a very serious problem and are taking steps to combat it. Banking security and risk compliance teams can establish anti-skimming plans and procedures. Effective plans may include random daily inspections, even during weekends, of ATMs by security and other branch personnel to help spot irregularities, such as the addition of a skimmer or a camera to the unit. By taking a picture of the ATM, it will be easier to notice if small changes such as reader attachments or cardholders have been added.

Also, employees should be instructed to look for traces of adhesive or tape residue—evidence that skimming equipment may have been installed and removed. If skimming equipment or residue is found, federal and local law enforcement should be immediately notified to begin processing a potential crime scene. Bank officials should quickly contact all of their ATM networks to advise

them of a possible security breach.

Typically busy ATMs that show uncharacteristic periods of overnight downtime, without a known cause, could be the target of a skimming attempt that prevented normal operation. That should be cause for further investigation.

Cameras focused on the ATM can act as a 24/7 deterrent to skimming and other crimes, while also providing video to help identify skimmers as they install and remove their equipment. In the event of a security compromise, the video can be invaluable in helping to establish an accurate timeframe for the placement of skimming devices.

Even simple, low-tech solutions, such as bright lighting around ATMs and While skimming results in significant losses due to fraud and investigative costs each year, perhaps the greatest damage to U.S. financial institutions is inflicted upon their reputation and the loss of customer confidence.

A recent study by Harris Interactive reported that 67 percent of U.S. adults who use financial institutions with ATMs would likely switch to another institution after experiencing ATM fraud or a data breach.

Such studies stress the importance for financial institutions to act immediately to help protect themselves and their customers from personal financial data theft.

About the Author

John Pearce is the marketing director of financial, banking and government systems for ADT Security Services.

Copyright 2009, [1105 Media Inc.](#)