



Fraud, identity theft, grow at ATMs

17 July 2008

It's easy for crooks to rip you off at the cash machine, especially if you're not paying attention. And your PIN won't offer the protection you might assume it would.

Before Jay Foley inserts his bank card into an ATM slot, he sticks his finger in. Then he wiggles it. "If any portion of it wiggles with my pinky, I walk away, because odds are somebody has slapped a skimmer on the front," says Foley, the executive director of the [Identity Theft Resource Center](#) in San Diego.

"That applies to any kind of payment slot you might run across, such as gas station pumps. Those are favorite places for thieves to work now."

A skimmer is a device that reads and records all the account information stored electronically on the magnetic strip of an ATM card.

Its mere existence is proof that if you thought familiar, ubiquitous automated teller machines were much too low-tech to attract high-tech cyberthieves, you need to think again.

Fraudsters have returned to ATMs in force as a favorite fishing hole for that prize catch: your debit card.

With a little light mechanical tampering, thieves can "harvest" your account details and PIN number in seconds, then use them to either produce a "clone" card or to simply shop online until your account runs dry.

"The number of victims we get from debit fraud or ATM fraud is growing every year, and it's growing significantly," Foley says.

Increased danger

ATM crime is increasing now that stepped-up fraud detection software on the credit card side has made signature cards more difficult to attack. Increasingly, thieves are preying on more-vulnerable PIN-based debit cards.

Doug Johnson, a vice president and the senior adviser of risk management policy for the American Bankers Association, acknowledges that ATM skimming may be getting worse.

| ID theft by the numbers | |
|-------------------------|----------------|
| Period | 12 months |
| Number of victims | 3 million |
| Total losses | \$2.75 billion |
| Average loss | \$900 |

Source: Gartner, August 2005

"We have seen some increase in reports of ATM skimming that have been reported by the media," he says.

Identity theft resulting from ATM and debit card crime is increasing, according to a 2005 study by Gartner, an information-technology research and advisory company.

Johnson reminds nervous customers that banks issuing debit cards cover most of the losses associated with skimming as a matter of course. However, in some instances, debit theft can cause much greater financial damage than credit card fraud. While federal law limits your liability in credit card fraud to \$50, that same limit applies only to debit frauds reported within 48 hours. After that, you could be out anywhere from \$500 to the entire fraud amount.

Avivah Litan, a vice president at Gartner, says an August 2005 study by her company revealed \$2.75 billion in ATM/debit card fraud losses over 12 months. "ATM fraud is definitely on the rise," she says.

Though victims of credit card fraud might have to wrestle with their credit card issuers to remove disputed charges from a bill, debit card victims often face even greater aggravation.

With debit fraud, the thief actually drains the money directly from a checking account, leaving the victim to deal with bounced checks, missed payments and a downward-spiraling credit report while fighting with the bank to correct the wrong.

'Shoulder surfers' catch wave

Thieves compromise ATMs in a variety of ways. Most commonly, they attach a skimming device over the card slot of a legitimate ATM.

After the customer inserts a debit card, the transaction proceeds unimpeded while the thief electronically harvests the account data off the card's magnetic strip.

Crooks simultaneously record the PIN number during the transaction by using an inconspicuously placed camera or touch-sensitive keypad overlay on the keyboard. In some cases, a criminal may actually peer over the victim's shoulder (called "shoulder surfing") during the transaction.

Some enterprising thieves take it a step further and install phony ATMs, usually in out-of-the-way locations such as parking lots. At a recent security conference, Robert Morris Sr., a former chief scientist for the National Security Agency, said thieves have acquired old ATMs on eBay for as little as \$1,000.

Foley says some thieves place an out-of-order sign on a working ATM that directs traffic to their nearby bogus ATM.

"Or worse, they put up a machine that says, 'We will clean the mag stripe on your debit cards. Just insert it here, and it will improve the transaction process,'" Foley says. "What you're plugging it into is a skimmer."

Whatever the scam, the result is the same: It's become increasingly hard to tell a safe ATM from a bogus one.

Unacceptable losses

Banks and financial institutions generally cover cardholder losses in some -- but by no means all -- fraud cases with their much-ballyhooed "zero liability" promises.

However, at some point those losses land back on consumers in the form of higher bank fees and product costs.

Gartner's Litan says the recent increase in attacks now has banks reassessing their traditional view of ATM/debit fraud as an acceptable business loss.

"I think that's changing; I don't think it's so acceptable to them now," she says. "Their (anti-fraud) systems are out of date. The neural networks only catch the second (fraudulent) transaction, not the first. They've been eating a lot of losses and having to reissue cards. They're not happy about it. I don't think it's acceptable like it used to be."

Johnson says the American Bankers Association is working with its member banks, ATM vendors and networks to shore up ATM security.

One promising area, known as "jitter technology," would enable the ATM itself to detect when it has been tampered with and to shut itself down. ATM maker Diebold has unveiled its Vectra line that replaces the keypad with a dial, making it more difficult for thieves to obtain PIN information. Johnson says there's a silver lining for nervous banks: "The solutions are not expensive on an individual unit basis and can be deployed in the current ATM environment. It's not like you need to swap out ATMs."

Plastic or cash?

That's all well and good for banks, but where does it leave consumers when their snatched debit cards lead down the rabbit hole to identity theft?

Foley says one 2007 study estimated that identity theft cost U.S. businesses and consumers \$56.6 billion in 2005 alone, a bill that ultimately gets slipped to the public in higher banking fees and product costs.

"Let's be very upright here: When we're talking about credit and debit cards, we're talking about trillion-dollar industries," Foley says. "They're not affected by \$56 billion in losses. That's not even 1%."

Litan predicts the ultimate solution to ATM/debit fraud may involve the chip-enabled "smart card," which is more difficult to clone. The chip in a smart card is combined with the user's PIN -- a system known as "chip and PIN" -- to verify transactions as nonfraudulent.

But smart-card technology has been slow to catch on due to its higher costs. The use of smart cards raises the question of who's going to foot the bill for all those chip-enabled merchant point-of-sale terminals.

"I'm starting to hear talk from some major banks that they are going to move to it. It's just a matter of time," Litan says.

Chip-and-PIN technology is being used in Canada and Mexico, and all over Europe and Asia, Litan says.

"The United States is the last holdout," she says. "That may not be the best technology at this point, but we need to keep it ubiquitous and interoperable around the world. People traveling around the world can't have different cards for different countries."

Despite the growing risk of fraud during ATM transactions, Foley says plastic is here to stay for one very good reason: "If we all go back to using cash, the identity thieves are going to go back to using clubs. It's called armed robbery. That's why we went to credit and debit cards in the first place."

Watch for signs of foul play

When choosing an ATM, keep the following things in mind:

- Use a familiar and trusted ATM, preferably one attached to your bank. Avoid using ATMs in unfamiliar or remote locations, or around suspicious persons.
- Check the card slot, keyboard and machine for signs of tampering. Do not use the machine if the card slot jiggles, the keyboard has an overlay or anything else seems suspect.
- Look for security cameras on the machine and in the vicinity. If they appear suspicious, do not use the ATM.
- Avoid ATMs with signs or messages affixed to them. Banks and legitimate ATM owners do not direct customers to another machine with signs attached to the machine itself.

Smart ways to avoid ATM fraud

Always safeguard your information by following these steps when using an ATM:

- Maintain a safe distance from others in line. Do not allow anyone to distract you or offer assistance.
- Have your card out of your purse or wallet and ready for use.
- Stand close to the screen and shield your keystrokes from cameras and others waiting in line by using the knuckle of your middle finger to key in your PIN.
- If you think the ATM is not working properly, press cancel, remove your card, and report the machine to your financial institution.
- Secure your cash and card, and make sure the transaction is complete and the screen is clear before leaving the ATM.
- Keep your printed receipt to compare against your bank statement.

This article was reported and written by Jay MacDonald for Bankrate.com.