



Wednesday, July 4, 2007

[Nation & World](#) | [Health](#) | [Money & Business](#) | [Education](#) | [Opinion](#) | [Photos & Video](#) | [Rankings](#) |

## Money & Business

### Beware of Bank Account Skimmers

*By Kimberly Palmer*

Posted 6/27/07

Brad Lipman's dinner out with his family turned out to be much more expensive than he expected, at least temporarily. When he paid for the meal last summer with his debit card, someone in the restaurant—he still doesn't know who—swiped it through a portable card reader, which copied the account information. Within a few weeks, thousands of dollars had been stolen from his bank account.

Lipman, who lives in Thousand Oaks, Calif., is one of thousands of people affected by "skimming," criminals stealing credit card information when cards are used at ATMs, restaurants, or other retail locations. Skimmers siphon about \$60 million a year from bank accounts, according to the Electronic Funds Transfer Association.

"We're seeing more of it," says Todd Davis, chief executive of the security company LifeLock, in Tempe, Ariz. One common technique, he says, is placing a skimming device over the card slot of an ATM. The skimmer looks like a piece of plastic to guide cards into the slot, but it picks up bank information as the card slides through.

People can purchase skimming machines, which are also called portable magnetic credit card readers, through online sites such as eBay for around \$200. The devices, which are about the size of a small stapler and contain a slot for card swiping, electronically read cards' magnetic strips and store the data. The data are then transferred to a computer and used to make copycat cards, which can make purchases.

The devices are also used for legal purposes, such as registering conference attendees or making sales at small retail stores. An eBay spokeswoman said that the company allows the sale of the devices, because they are legal, but that sellers are prohibited from marketing the devices for fraudulent use under the company's policy against encouraging illegal activity.

Kurt Helwig, president of the [Electronic Funds Transfer Association](#), which promotes electronic commerce, says that while the number of skimming incidents as a percentage of overall ATM use hasn't grown, the increase in ATM use overall means that it is happening more often. Although it's still a rare occurrence and there's no need to avoid ATMs, he says, consumers should be wary. "If you see something that looks funny or doesn't look right, with wires hanging out or a stupid sign [directing consumers to a different card slot], don't use that ATM, and let someone know," Helwig says.

Many banks have added security measures, such as monitoring ATMs with physical inspections as well as electronically during off hours, when skimming is most likely to occur. Margie Green, a spokeswoman for Wachovia, says the bank's ATMs are under watch 24 hours a day. Like most banks, Wachovia reimburses customers for any losses they incur from a skimming scam. By law, banks must reimburse customers for all but \$50 of their losses, as long as they report the problem in a timely fashion.

Still, falling victim to skimming is not pleasant. Even though his credit company refunded his money, "I felt absolutely as violated as can be," says Lipman, who has since started a company, [TablePay Solutions](#), to help prevent skimming. The company distributes a machine to retailers that allows customers to swipe their own card, never allowing it out of their sight.

Copyright © 2007 U.S. News & World Report, L.P. All rights reserved.