



Association of Contingency Planners Vulnerability Alert No. 2

From: ACP Corporate Information Director
June 6, 2008

Overview

This is an awareness of a form of theft called 'skimming' that can be used at ATM machines. "Card Skimming is the collection of ATM and/or Debit Card account numbers and personal identification numbers (PIN's) for the purpose of recreating the cards and subsequently making large fraudulent withdrawals in short periods."¹



Description

'Skimming' has been around for a while internationally. In recent years it has occurred in the US. Although the device can be put on any bank ATM, the 'skimmers' have frequently been installed on ATM's in mini markets where the employees are busy in the deli and at the cash register and the ATM is not in the direct line of view of the employees on duty.

A slide show of pictures demonstrating how 'skimming' is actually executed is currently posted on the Home Page of the ACP national website. You are free to download the slide show for your use. Copies of this slide show are also available on various websites on the internet.

In November 2007 Diebold, Inc. announced that they had perfected a device for their Opteva line of ATM's. Keep in mind that this is only for one specific line of ATM and the device must be purchased. It is not feasible to assume that every ATM machine has been fitted with this detection device.

"NORTH CANTON, Ohio - [Diebold Inc.](#) announced today it has engineering advanced skimming-detection technology into its Opteva line of ATMs. According to Celent LLC, card-skimming losses account for about \$1.2 billion a year worldwide."²

¹ http://www.beaconcu.org/education_atm_skimming.shtml

² <http://www.atmmarketplace.com/article.php?id=9390&na=1>

Actions Taken:

1. Research of ATM 'skimming' on the internet to ensure that the vulnerability presented in the slide show was legitimate and not contrived. The slide show has a Spanish title and Spanish author's name listed in the Properties.
2. The Vice President of Operational Risk of a bank in Wilmington, DE confirmed that this is a real threat in the US and has not been perceived or contrived to create a false alarm. He provided DelawareOnLine as a resource for more information.

DelawareOnLine:

By TERRI SANGINITI

The News Journal - December 4, 2007

Detectives investigating the origins of a skimming device found last month affixed to an automatic teller machine at a Bear convenience store have discovered that customers' debit card information was also compromised at ATMs at two other locations in Delaware, state police said Monday.

Only one of the skimmers has been recovered. It was found affixed over the existing card swiper on the ATM at a Wawa Food Market store at Pulaski Highway (U.S. 40) and Salem Church Road, and had captured the card holders' personal data used to pilfer money from their bank accounts.

As the investigation unfolded, banks began reporting to state police that theft of customer credit-card data had also occurred at Wawa stores at 1100 Pulaski Highway and at Del. 4 and Del. 72, state police spokesman Cpl. Jeff Whitmarsh said.

He said the other skimmer devices were probably removed by the criminals after the discovery of the first device Nov. 9.

"We estimate the losses at between \$50,000 and \$75,000," Whitmarsh said. "Fraud withdrawals have been made at various locations in Delaware, Pennsylvania and Maryland."

Further information was found at **www.bankrate.com:**

www.bankrate.com

Experts say crime rings sometimes skim ATMs, and the damage can be extensive. A New York ring installed more than 20 modified ATMs and compromised more than 26,000 transactions and thousands of cards from 1,400 issuers. Losses were pegged at \$3.5 million before the case was cracked.

There are approximately 360,000 ATMs nationwide. About half of them belong to banks, and the rest are so-called "nonbank" ATMs in convenience stores, malls, hotel lobbies, airports, etc.

ATMs that have swipe readers (you swipe your card through a raised slot) are the easiest to skim. Swipe readers are more likely to be found at non-bank ATMs.

"Most ATM manufacturers are aggressively moving away from swipe to a dip or manual insert reader that has less accessible external parts because the reader head is buried in the machine," say Jim Merrell of Ohio-based ATM manufacturer Diebold.

But that doesn't mean you should avoid ATMs that have swipe readers.

"There are tens of thousands of them. Just beware of something that doesn't look quite right," says Merrell.

Impact

The thief will install an external device (a computer) on the ATM immediately before a customer is about to approach the ATM. That computer will read the card and capture the PIN by keystroke. Some devices will capture the card and not return it. The device is then removed, the thief has the information to make a bogus card or may have the captured the

card in the device. In either case the thief has what is needed to access and empty your account.

Recommendations:

1. Look for new equipment or changes to the ATM machine you use. It helps to have a favorite ATM machine so you can recognize changes. If it doesn't look right, don't use it.
2. If you are using an unfamiliar ATM machine, beware of devices that protrude from the unit. (Take a good look at the picture on page1 of this document again.)
3. Read the labels on the ATM machines as many 'skimmers' are foreign made and labels on the 'skimmers' may have misspellings.
4. If an ATM machine has any unusual signage, don't use it. No bank would hang a sign that says, "Swipe your ATM card here before inserting it in the card reader" or something to that effect.
5. If your card is not returned after the transaction or after pressing cancel, immediately contact the institution that issued it.
6. Check your statements to be sure there are no unusual withdrawals.