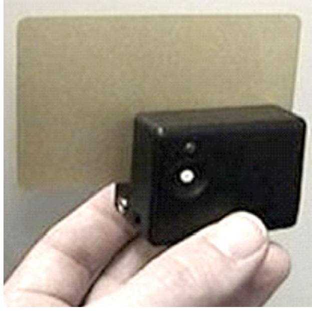
Skimming

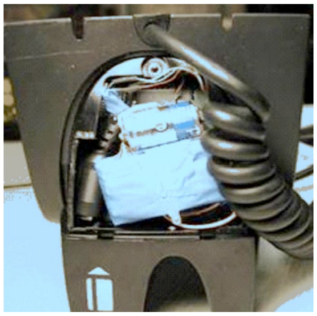
A Resource Guide from the PCI Security Standards Council

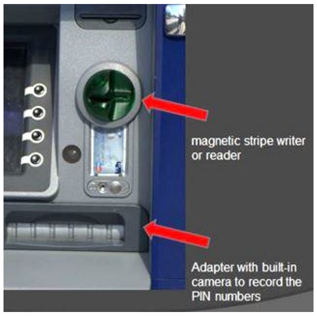
WHAT IS SKIMMING?

Skimming is copying payment card numbers and personal identification numbers (PIN) and using them to make counterfeit cards, siphon money from bank accounts and make fraudulent purchases.

Criminals install equipment at merchant locations, on point-of-sale (POS) devices, automated teller machines (ATM), and kiosks that captures the information from the magnetic stripe.






magnetic stripe writer or reader
Adapter with built-in camera to record the PIN numbers

HANDHELD SKIMMER

Handheld skimmers used by corrupt staff are very small, fitting in the palm of a hand. Despite their size, these devices can store a significant amount of cardholder data.

POS TERMINAL SKIMMER

Skimming devices hidden within the terminal are invisible, and neither the merchant staff nor the cardholder will know that a card was skimmed.

ATM SKIMMER

Criminals may not use a single attack against a device, but can use a combination of attack scenarios. In this attack we see an overlay has been placed on the ATM's card reader to capture the card data, and an additional overlay was added to the plastic that allowed for a hidden camera to capture the PIN.

FACTS & FIGURES

$2 billion

The estimated global cost of skimming[1]

$50,000

The average loss from skimming crime[2]

Skimming-related counterfeit card fraud is the leading type of third-party card fraud[3]

92%

Skimming is the #1 ATM crime globally making up 92% of all attacks at the ATM[1]

From Jan-Apr 2015, the number of attacks on debit cards used at ATMs reached the highest level for that period in at least 20 years[4]

All amounts are in U.S. Dollars

IN-DEPTH BACKGROUND MATERIALS

AT A GLANCE:
SKIMMING PREVENTION

PCI Security Standards Council®

Skimming Prevention:
Overview of Best Practices for Merchants

Skimming is the unauthorized capture and transfer of payment data to another source. Its purpose is to commit fraud, the threat is serious, and it can hit any merchant's environment. With skimming, thieves steal payment data directly from the consumer's payment card or from the payment infrastructure at a merchant location. Both techniques typically require the use of a rogue physical device planted onsite. PCI Security Standards currently contain a number of requirements and recommendations to guard against skimming. In addition, the Council has introduced an overview document for merchants, containing a "deep dive" into skimming with examples, best practices, and tools to thwart its use. This "At-a-Glance" piece provides a snapshot of skimming and introduces areas requiring countermeasures to ensure an appropriate level of security for cardholder data.

MERCHANTS MUST TAKE STEPS TO PREVENT SKIMMING

Skimming equipment can be very sophisticated, small, and difficult to identify (see photos on reverse). Merchants are the first line of defense because skimming gear is frequently deployed at the merchant's point of sale or network. Consequently, it is critical for merchants to become familiar with this category of threats and to take precautions.

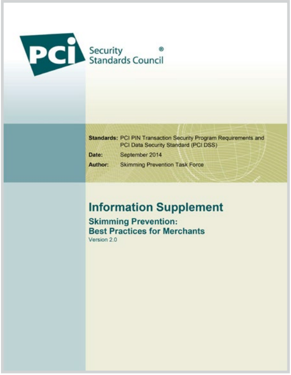
Video Resources
- PCI SSC YouTube Channel
- APCA

Who Does It? Perpetrators skim because it is highly profitable. They may be sophisticated and organized criminals leading complex, effective attacks. Or they may be relatively unsophisticated criminals who use readily available, simple technology to steal cardholder data.

Targets for Attack. There are at least five potential targets for skimming. These include PIN data, often visually captured by people standing near a POS device or by use of fake PIN entry devices; unattended or temporarily unattended terminals; merchants with a high overall transaction volume (allowing a criminal to capture a large amount of data in a short period of time); individual terminals with a heavy volume of usage; and merchants with periods of high-volume sales.

Impact of Skimming Attacks. There is a cost to skimming attacks that is over and above the actual loss of monies, goods, and services: Skimming attacks undermine the integrity of the payment system, employee trust, industry relationships, and consumer trust in the merchant.

Insider with portable card reader
Rogue device
Automatically siphons cardholder data to criminals
POS
POS
POS
Payment server
Criminals collect and abuse cardholder data

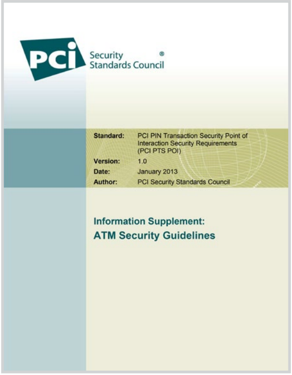


PCI Security Standards Council®

Standards: PCI PIN Transaction Security Program Requirements and PCI Data Security Standard (PCI DSS)
Date: September 2014
Author: Skimming Prevention Task Force

Information Supplement

Skimming Prevention:
Best Practices for Merchants
Version 2.0



PCI Security Standards Council®

Standard: PCI PIN Transaction Security Point of Interaction Security Requirements (PCI PTS POI)
Version: 1.0
Date: January 2013
Author: PCI Security Standards Council

Information Supplement:
ATM Security Guidelines

pdf **Skimming Prevention – Overview of Best Practices for Merchants**

pdf **Skimming Prevention – Best Practices for Merchants**

pdf **ATM Security Guidelines**

RELATED VIDEOS

▶ **Safeguard Against Skimming**

▶ **The ATM Scam**

RELATED INDUSTRY RESOURCES

pdf **Skimming the Surface**

www **All About Skimmers**

pdf **Skimming is a Scam**

1: Source: ATMmarketplace.com 2: Source: Aite Group 3: Source: Mercator Advisory Group 4: Source: FICO

www.pcisecuritystandards.org

PCI Security Standards Council®