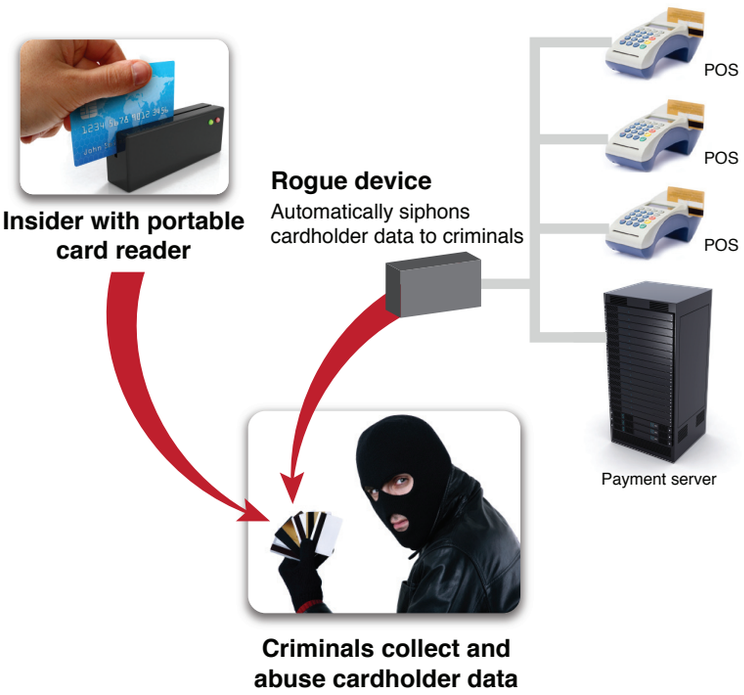
Skimming Prevention: Overview of Best Practices for Merchants

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" about skimming, examples, best practices and tools to thwart its use. This "At-a-Glance" provides a snapshot of skimming and introduces areas requiring countermeasures to ensure an appropriate level of security for cardholder data.



HIGHLIGHTS

Describes the problem of skimming with several examples of actual gear used to steal cardholder data

Provides best practices to mitigate the risk of skimming

Includes written methodology to quantify risk of skimming and a checklist for tracking assets in a specific merchant location and terminal environment

Merchants Must Take Steps to Prevent Skimming

Skimming equipment can be very sophisticated, small, and difficult to identify (see photos on back page). Merchants are the first line of defense because skimming gear is always 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.

Who Does It? Perpetrators skim because it is highly profitable. They may be sophisticated and organized criminals leading complex, effective attacks. Skimming is also done by 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 swiped with a fake PIN entry device; unattended or temporarily unmanned terminals; merchants with a high transaction volume (allowing a criminal to capture lots of data in a short period of time); terminals with a heavy volume of usage; and merchants with periods of high volume sales.

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

Using the Guidelines to Prevent Skimming

Download the document, "Skimming Prevention: Best Practices for Merchants" at www.pcisecruritystandards.org/education/info_sup.shtml.

The document provides specific recommendations for the contents outlined on the back side of this At-a-Glance, left sidebar. Please see the document for details, including guidelines and best practices, a risk assessment questionnaire, and evaluation forms.

SKIMMING CONTENTS

1. **Overview**
   - About This Document
   - What Is Card Skimming and Who Does It?
   - The Impact of Skimming Attacks
   - Examples of Terminal Fraud
2. **Guidelines and Best Practices**
   - Merchant Physical Location and Security
   - Terminal and Terminal Infrastructure Security
   - Staff and Service Access to Payment Devices
   - Risk Analysis of Terminals and Terminal Infrastructure
3. **Appendix A: Risk Assessment Questionnaire**
   - Risk Category
4. **Appendix B: Evaluation**
   - Forms
   - Terminal Characteristics Form
   - Merchant Evaluation Checklist

Examples of Terminal Fraud

Criminals use a variety of techniques to skim cardholder data from transactions at the point of sale and through the merchant's payment system. Photos and sidebars below show three examples of devices used to skim at the point of sale. The document has more examples.

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

This picture shows a skimming device inserted in a terminal. The device was hidden by the SIM card cover plate.

Changes to terminal connections can be difficult to spot.

In these images, the criminals completely changed the cable connecting the terminal to the base unit.

The fatter cable housed additional wires required to capture cardholder data.

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.

Guidelines and Best Practices

Guidelines and best practices mentioned are non-exhaustive. They cover:

Merchant Physical Location. Merchants must address measures affecting terminals, terminal infrastructure, cameras, placement, access, and image storage.

Terminals and Terminal Infrastructure Security. Areas requiring attention include terminal surroundings, IP connectivity, individual terminal data, terminal reviews, terminal purchases and updates, terminal disposal, PIN protection, and wireless terminals.

Staff and Service Access to Payment Devices. Areas affecting people include staff as targets, hiring and staff awareness, outside personnel, and service providers.

Risk Analysis of Terminals and Terminal Infrastructure. The analysis includes identification of assets, threat and probability, and severity. Tools are provided to help with the analysis.