Standards

The intent of this document is to provide supplemental information. Information provided here does not replace or supersede

About This Document

This document consists of the following:

Chapter 1 provides a general overview; describes exactly what card skimming is, who does it, and how it impacts the various payment constituents; and provides some real-life examples of compromised terminals.

Chapter 2 provides an extensive list of best practices and guidelines merchants need to consider if they have not done so already. The list identifies threats and challenges and possible remedies merchants can take to mitigate the risk of being victims of skimming attacks.

Appendix A provides a mechanism for the merchant to further quantify risk associated with merchant location and terminal infrastructure.

Appendix B provides a checklist merchants can use to identify and track terminal assets.

What is Card Skimming and Who Does It?

Skimming is the unauthorized capture and transfer of payment data to another source for fraudulent purposes. This unauthorized capture and transfer of payment data is different than mass data-compromise breaches, and can result from one of the event types listed below.

Data from Consumer Payment Cards

The first type of skimming event is the acqui

Data Capture from Overlays

Overlay attacks have traditionally been used in ATMs or other unattended devices to capture card account and PIN data. (See Image 16 in “Examples of Terminal Fraud” below.) In these types of attacks, an overlay that contains wires or an additional card reader is placed on the ATM or POS terminal. A sticker overlay may be added to the keyboard area to capture the PIN, (Image 12); or, using a 3D printer, a new casing maybe placed over the existing device (Image 13). These overlays can hide tamper evidence, add an additional reader, and slightly change the operation and look of the terminal.

Perpetrators and Targets

Understanding the lengths that criminals go to in order to obtain and compromise account data may help you understand the necessity of taking sufficient measures to make it significantly more

ATMs, Unattended, or Temporarily Unattended

tiUthat6( )63ftor c wede.0( )4(v)11(rarea)4(t)-4(y11(( )4(oft)8.0( )4(bu)-3siU)5(n8.04ss neede)4(s11(( )4(ha
T-8[M t

t tiU t63(t63en)-3(de.0d ti)-7o

termtna36lU

[illegible]

[illegible]

Terminals with Heavy Use

A single payment terminal used for a large number of transactions may attract criminal intent. (In-store ATMs are a good example, or locations where relatively few terminals support a business.) The idea is to capture as many accounts as simply and quickly as possible—it's more efficient to compromise one terminal with high activity than to attack three terminals with the same volume of accounts.

High-Volume Sales Periods

As you develop operational business and security controls for peak activity, keep in mind that criminals also target merchants during busy sales times, whether holidays or special events. Again, the intent is to capture as much account and PIN data in as short a time as possible.

The Impact of Skimming Attacks

The impact of skimming is significant for all the constituents involved in payment and ATM services. 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.

Card-Issuers and Payment Networks

For banks and the various sources of funding for payment cards, the issue is direct financial loss and loss of trust in the payment system. The cost of the fraud itself, incremental monitoring requirements, investigative efforts, consumer notification efforts, and the cost to replace cards are just some of the issues associated with a skimming incident for the issuing banks and payment networks.

Merchants

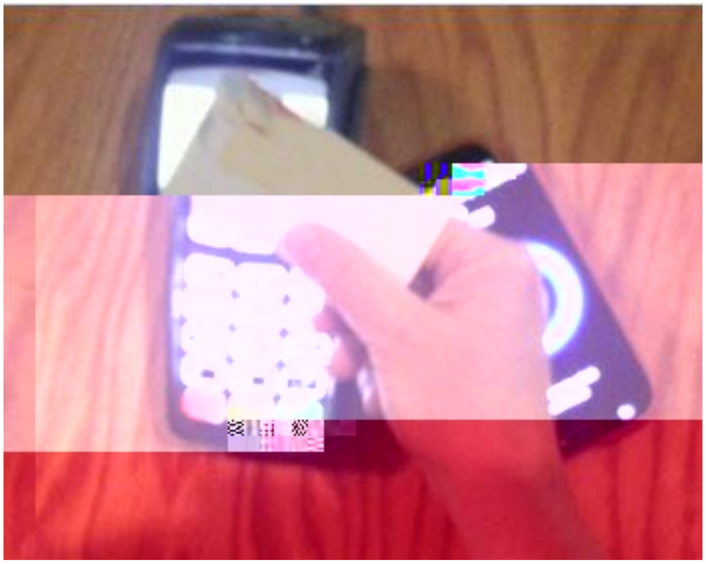
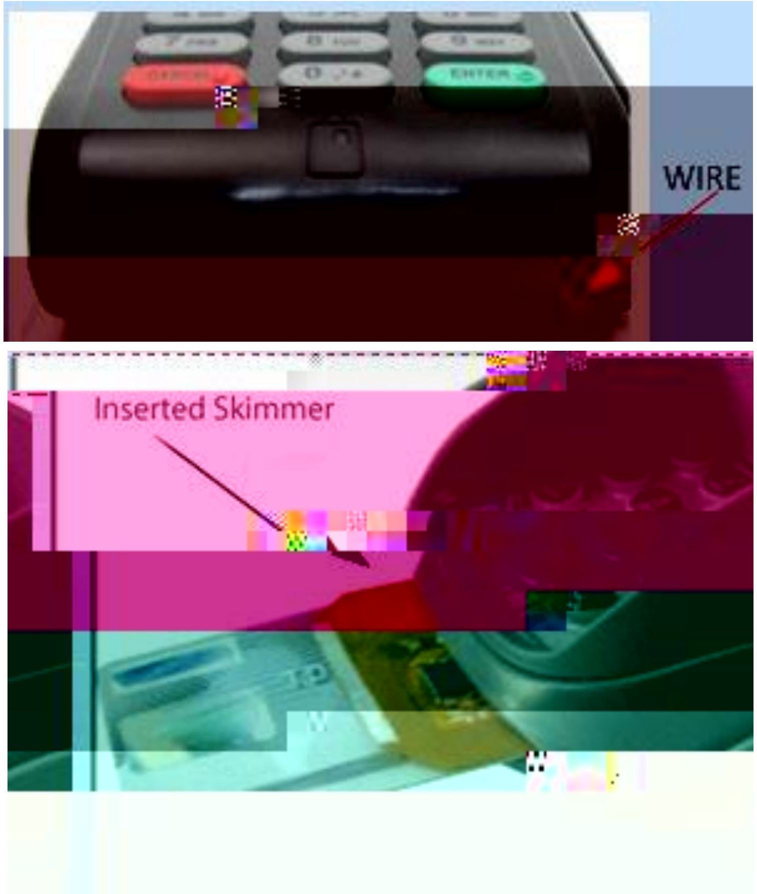
Recent attacks in the headlines have led merchants to realize that a single fraud incident can put them out of business, or at the very least significantly impact their brand and the trust consumers have in them. Skimming fraud is one of the top three fraud types a merchant must address. Consumers are becoming more aware of which merchants protect their information and which

Image	

Image	Attack Technique
	Image 4 Key loggers are used to record all keystrokes made, in this case by an electronic cash register. Key loggers can be very small and can look like part of the normal cabling. It is therefore

Image	Attack Technique
	Image 7

Image	Attack Technique
	Image 11 This aerial view clearly shows how Wi-Fi signals can extend far beyond the four walls of the merchant location, allowing anyone to intercept the signal. Data should never be sent unencrypted over any wireless connection.
	Image 12 Staff should also be aware of the addition of overlays. An overlay can be a small sticker that forms to the device and covers the keyboard area. Overlays may hide damage due to tampering or wires that can allow for keyboard logging. Overlays should not be used.

Image	Attack Technique
	**Image 14** In an NFC attack, an NFC reader (in this case a smartphone) is placed between the terminal and the customer to capture the card data during a tap transaction. Additional equipment should not be placed near or around terminals.
	**Image 15** EMV or chip cards are not immune to skimming. Staff and consumers should be aware of modifications or wires to the smart-card slot. If anything appears different with the device, it should be reported immediately.

Image	

Chapter 2: Guidelines and Best Practices

Best practices and security guidelines for the prevention of skimming are based on successfully establi

Threat-Mitigating Resources

The intent

Individual Terminal Data

An essential step in protecting your POS terminals and ATMs is recording the number, type, and location of each of your devices. Such details will allow you to easily determine whether you have been targeted. See Appendix B for an example checklist on how to track and mange this data. For each terminal:

Take multiple photographs of each terminal front and back, including any labels, serial numbers, and hardware identifiers when reviewing the device.

- Make the photographs available for a comparison review in the future. Comparing new photographs with old photographs makes it easier to spot differences.

Record its location in the store (unless the terminals are removed and secured when the store is closed).

Record the condition and location of any labels.

Record the exact details of any security labels.

For POI payment card devices connected to an electronic cash register or separate host

The notification and escalation process to report an event

The procedure for escalating concerns about a terminal

Who to contact if they have concerns about terminal security

How to contact senior management if they discover a compromise

How management or the employee shoi149 36.024 Ttdact ifWR

Risk Analysis of Terminals and Terminal Infrastructure

In addition to the guidelines, PCI SSC recommends that merchants seek out and use qualified security professionals and consultants27 1a1n1

Additional Resources

PCI SSC YouTube Channel

The PCI council has collected a number of videos. They're fun, entertaining, informative, and easy-to-share resources. Check them out on our SMB microsite or on the PCI SSC YouTube channel.

SMB Microsite:
https://www.pcisecuritystandards.org/smb/?utm_campaign=Monitor&utm_source=hs_email&utm_medium=email&utm_content=12847856&_hsenc=p2ANqtz--7AEoGrolIHyk8SGy6nmOuSrprOWuA312kzZCWAemYtuE88NhYZoogOuIO1WIpWXqO_PKEO-2Q3R7tte42XxEBa1iymt7G7yiE78Jc9mrWcPblVD0&_hsmi=12847856

PCI SSC YouTube Channel:
https://www.youtube.com/user/PCICouncil/videos?utm_campaign=Monitor&utm_source=hs_email&utm_medium=email&utm_content=12847856&_hsenc=p2ANqtz-9zRUEJUTi-aMNGrTz02xonCIR0eSTfTVB5ahyQMypayDJCwJknmbOobpMN7gn5vFON7ylnjJ1wJ8hLn1tW0CL6xA2LysAoAdslJYoHDmrFawvWGZI&_hsmi=12847856

Australian Payments Clearing Association

APCA

Appendix A: Risk Assessment

This Appendix enables you to determine the risk category that applies to your particular merchant location.

Complete the following questionnaire to determine a “vulnerability score,” and therefore the risk category applicable to your merchant premises. For each question, there are two or more possible answers, each of which has a particular value. For each question, enter the relevant value under “Your Score.”

Risk Assessment Questionnaire

No.	Question	Finding	Value	Vulnerability Score
1	Where are your merchant premises located?	Town center	1	
		Shopping mall	1	
		Out of town	2	
2	Are your merchant premises isolated?	Yes	1	
		No	0	
3	If the answer to question 1 is “Out of town” and to question 2 is “No,” how many shops or businesses are in the same location as your premises?	1 – 3	3	
		4 – 10	2	
		> 10	1	
4	Are your premises located at or near a major highway?	Yes	1	

The intent of this document is to providɿ m

No.	Question	

Risk Category

When you have answered all questions, total the scores in the right-hand column to determine your overall vulnerability score and therefore your risk category.

Vulnerability Score	Risk Category
More than 25	

The intent of this document is Ƙ ꓦ

[illegible]