

## What is Card Skimming?

Skimming is the unauthorized capture and transfer of payment data to another source for fraudulent purposes

With enough time and resources, any device can fall victim to physical or logical attacks. Limiting the time the device is unattended or unchecked reduces the effectiveness of an attack should an attempt be made against the device

Regardless of how it is achieved, skimming is a highly profitable criminal activity, difficult to prevent and detect.

### Question

- 1) \_\_\_\_\_  
Skimming is the unauthorized capture and transfer of payment data to another source for fraudulent purposes
  - a. True
  - b. False
- 2) \_\_\_\_\_  
With enough time and resources, any device can fall victim to physical or logical attacks.
  - a. True
  - b. False

### ***Data from Consumer Payment Cards***

The first type of skimming event is the acquisition of payment data directly from the consumer's payment device (payment card). This is normally accomplished through a small, portable card reader and usually involves internal merchant personnel who have both criminal intent and direct access to the consumer payment device. The majority of skimming attacks deal with the capture of payment data from magnetic-stripe payment cards outside of the payment terminal when the payment card is handled by the merchant personnel and when the consumer has little or no observation at the time of payment.

### Question

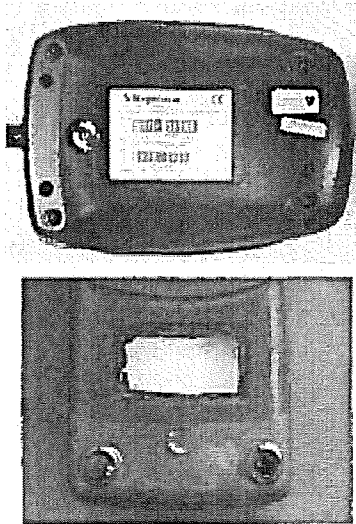
- 1) \_\_\_\_\_  
Skimming attacks deal with the capture of payment data from magnetic-stripe payment cards outside of the payment terminal
  - a. True
  - b. False
- 2) \_\_\_\_\_  
Skimming attacks on Payment Cards is normally accomplished through a small, portable card reader and usually involves internal merchant personnel who have both criminal intent and direct access to the consumer payment
  - a. True
  - b. False
  - c.

Print Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

The Following Photographs are designed to assist in understanding the attack techniques used by criminals at merchant locations.

Image	Attack Technique
	<p><b>Image 1</b></p> <p>Terminals will have a sticker attached to the underside, which provides details of the product and will include a serial number. The majority of terminals will also have a method of displaying the serial number electronically.</p> <p>As part of your regular checks, note the serial number on the back of the terminal and check this against the electronic serial number.</p> <p>Additionally, run your finger along the label to check that it is not hiding a compromise.</p>

1)

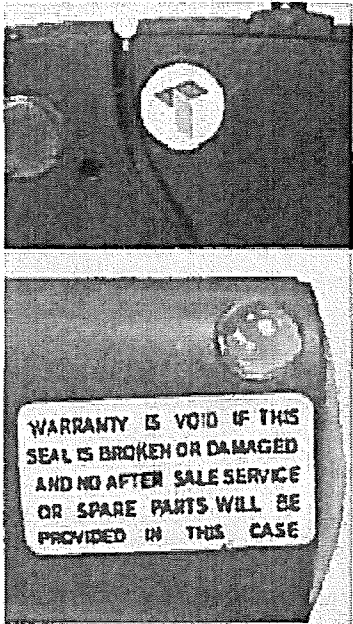
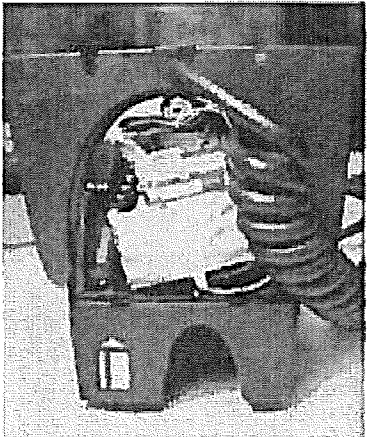
Image	Attack Technique
	<p><b>Image 2</b></p> <p>Terminals often have security stickers, or company stickers placed over screw holes or seams that will act as indicators if the case has been opened.</p> <p>Criminals often remove these labels when compromising terminals and may replace them with their own printed versions.</p> <p>When you first receive the terminal, make careful note of label position, colour, and materials used. Taking a picture of the device is a good practice.</p> <p>Also look for any signs that the label may have been removed or tampered with.</p>
	<p><b>Image 3</b></p> <p>Skimming devices hidden within the terminal will not be visible, and neither the merchant staff nor the cardholder will know that the card has been skimmed.</p> <p>This picture shows a skimming device inserted in a terminal. This would have been hidden by the SIM card cover plate.</p>

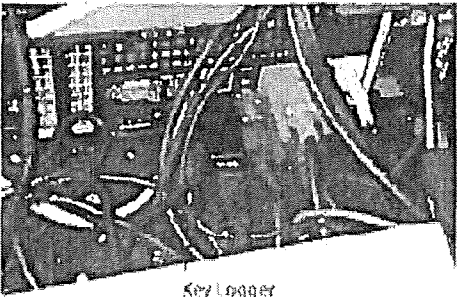
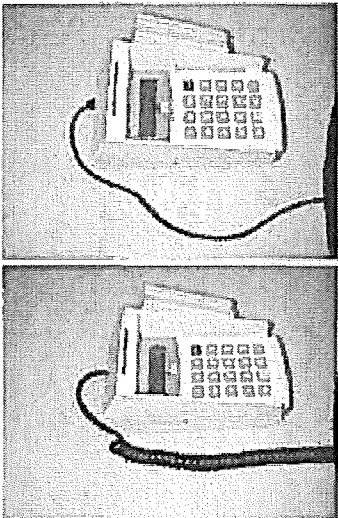
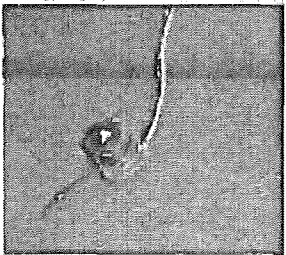
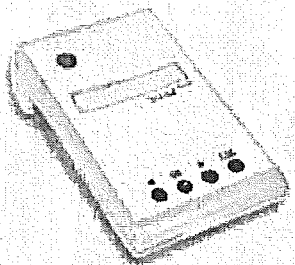
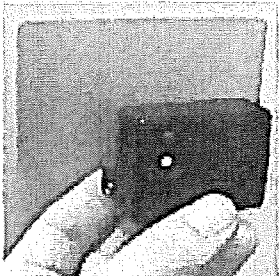
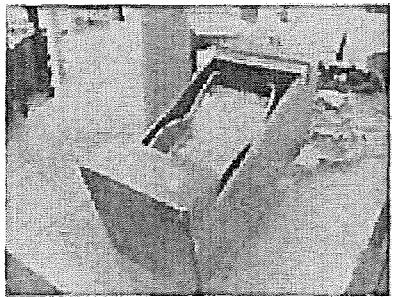

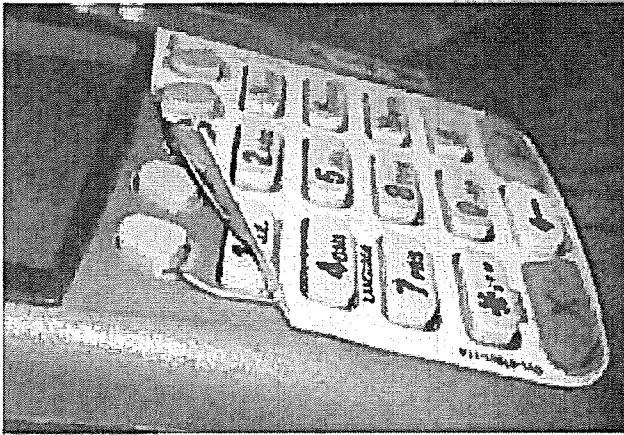
Image	Attack Technique
 <p data-bbox="483 554 574 575">Key logger</p>	<p data-bbox="862 281 943 302"><b>Image 4</b></p> <p data-bbox="862 319 1302 403">Key loggers are used to record all keystrokes made, in this case by an electronic cash register.</p> <p data-bbox="862 420 1302 529">Key loggers can be very small and can look like part of the normal cabling. It is therefore essential to pay close attention to detail when performing any inspection.</p>
	<p data-bbox="862 659 943 680"><b>Image 5</b></p> <p data-bbox="862 701 1252 753">Changes to terminal connections can be difficult to spot.</p> <p data-bbox="862 770 1260 854">In these images, the criminals completely changed the cable used to connect the terminal to the base unit.</p> <p data-bbox="862 871 1279 924">This was to incorporate the additional wires required to capture card data.</p>
	<p data-bbox="862 1194 943 1215"><b>Image 6</b></p> <p data-bbox="862 1236 1312 1320">The modern digital cameras used to record the cardholder entering his or her PIN are very small when removed from their cases.</p> <p data-bbox="862 1337 1312 1390">This makes them very easy to hide or disguise at the merchant location.</p> <p data-bbox="862 1407 1284 1459">This type of miniature camera can easily be hidden in a ceiling tile above the terminal.</p>

Image	Attack Technique
	<p><b>Image 7</b></p> <p>Staff should also be aware of additional, unfamiliar electronic equipment connected to the terminal, the cash register, or the network connections.</p> <p>This device records and decrypts ISDN data.</p>
	<p><b>Image 8</b></p> <p>Handheld skimmers used by corrupt staff are very small, fitting in the palm of one's hand.</p> <p>Despite their size, these devices can store a significant amount of card data.</p>
	<p><b>Image 9</b></p> <p>In this picture, the criminal entered the merchant location posing as a service engineer.</p> <p>He stated that to prevent credit card fraud the terminal must be placed in this secure box. He then gave the staff a sheet of printed instructions.</p> <p>The box contained a card skimmer and miniature camera.</p> <p>Be cautious of unannounced service visits.</p>
	<p><b>Image 10</b></p> <p>These devices were used to connect into the telephone exchange of a shopping mall to record all transmissions from the stores to the merchants' financial institutions.</p> <p>Such devices usually consist of voice recorders or MP3 players with very large memories. Often they have external batteries for improved life.</p>



**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.

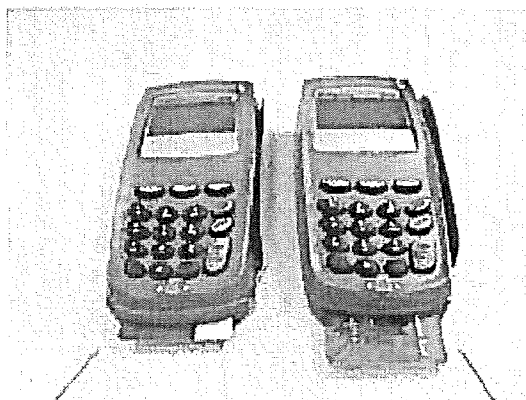


**Image 12**

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



Modified Terminal

Legitimate Terminal



## Attack Technique

### Image 13

3D printers have made duplicating plastics easier. In these examples, an overlay that included a card-data and PIN skimmer was added to the device.

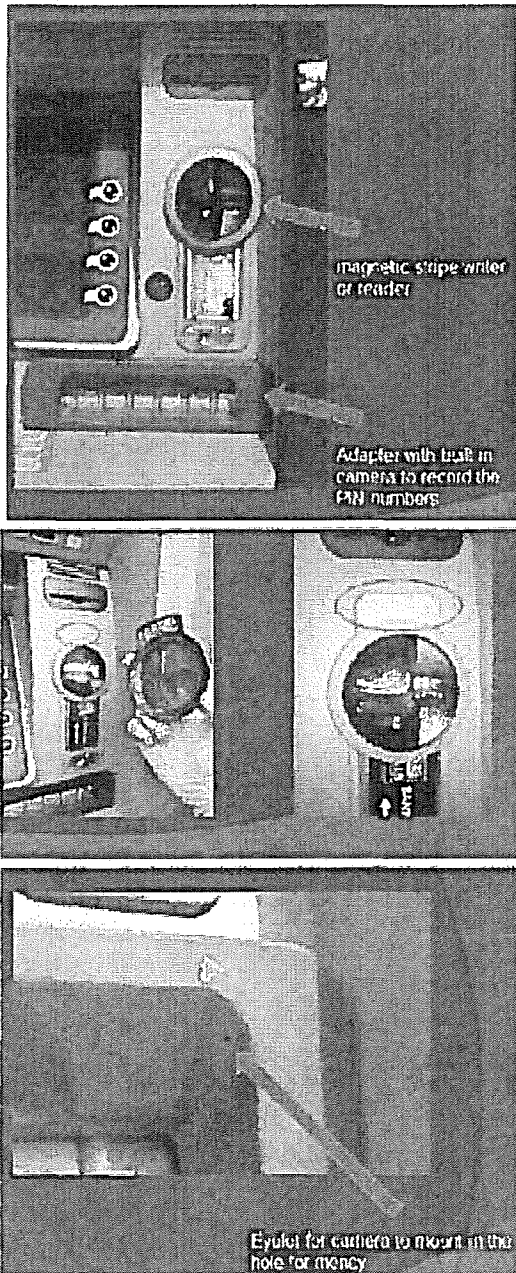
It is important to be aware that if the device remains off or unattended for a period of time, it should be checked periodically.

The staff should be aware and report actual or suspected changes in the operation of the device. If something is not right, report it.

Image	Attack Technique
	<p><b>Image 14</b></p> <p>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.</p>
 <p>WIRE</p> <p>Inserted Skimmer</p>	<p><b>Image 15</b></p> <p>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</p>



## Image



## Attack Technique

### Image 16

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.

Again, it is important to be aware that if the device remains off or unattended for a period of time, it should be checked periodically.

The staff should be aware and report actual or suspected changes in the operation or look of the device. If something is not right, report it.