
DhanlaxmiBank
established 1927

ATM Card Skimming & PIN Capturing

Customer Awareness Guide

DhanlaxmiBank
established 1927

What is ATM Card Skimming?

A method used by criminals to capture data from the magnetic stripe on the back of an ATM card.

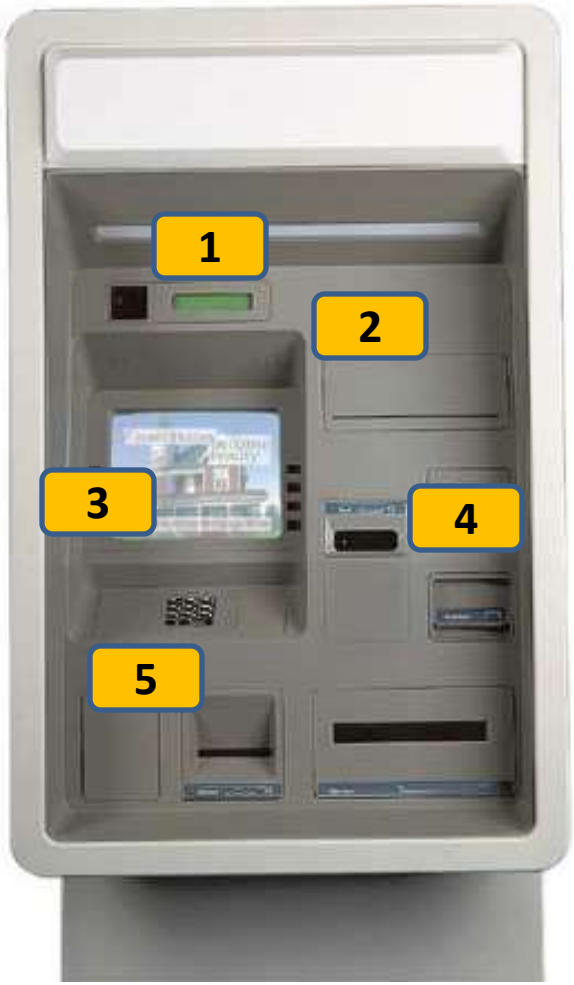
Devices used are smaller than a deck of cards and are often fastened in close proximity to, or over the top of the ATM's factory-installed card reader.

ATM skimming is a world-wide problem.

Where to spot a device on an ATM

Check these areas for any suspicious tampering:

1. Light diffuser area
2. Speaker area
3. ATM side fascia
4. Card reader entry slot
5. ATM keyboard area



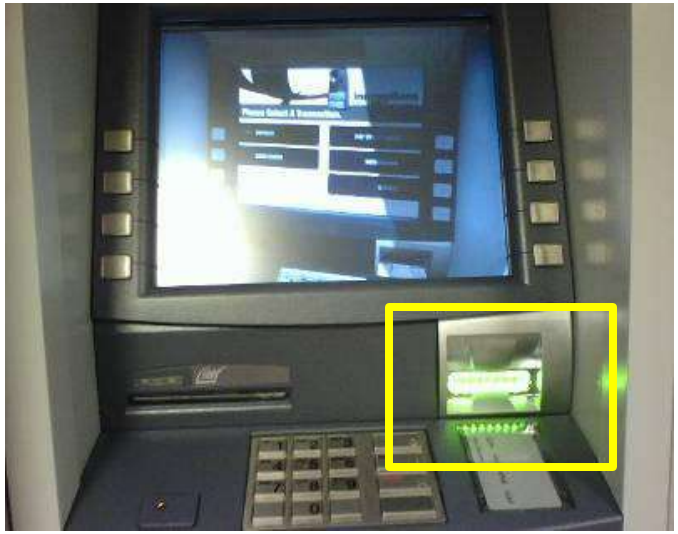
What is PIN capturing?

Strategically attaching / positioning cameras and other imaging devices to ATMs to fraudulently capture PIN numbers.

Once captured, the electronic data is put onto a fraudulent card and the captured PIN is used to withdraw money from accounts.

PIN capturing is a world-wide problem.

Skimming devices: spot the difference



Normal fascia

• The flashing card entry indicator can easily be seen.

•Most skimming devices will obscure the flashing card entry indicator.

•This detail serves as a vital clue identifying suspect tampering.

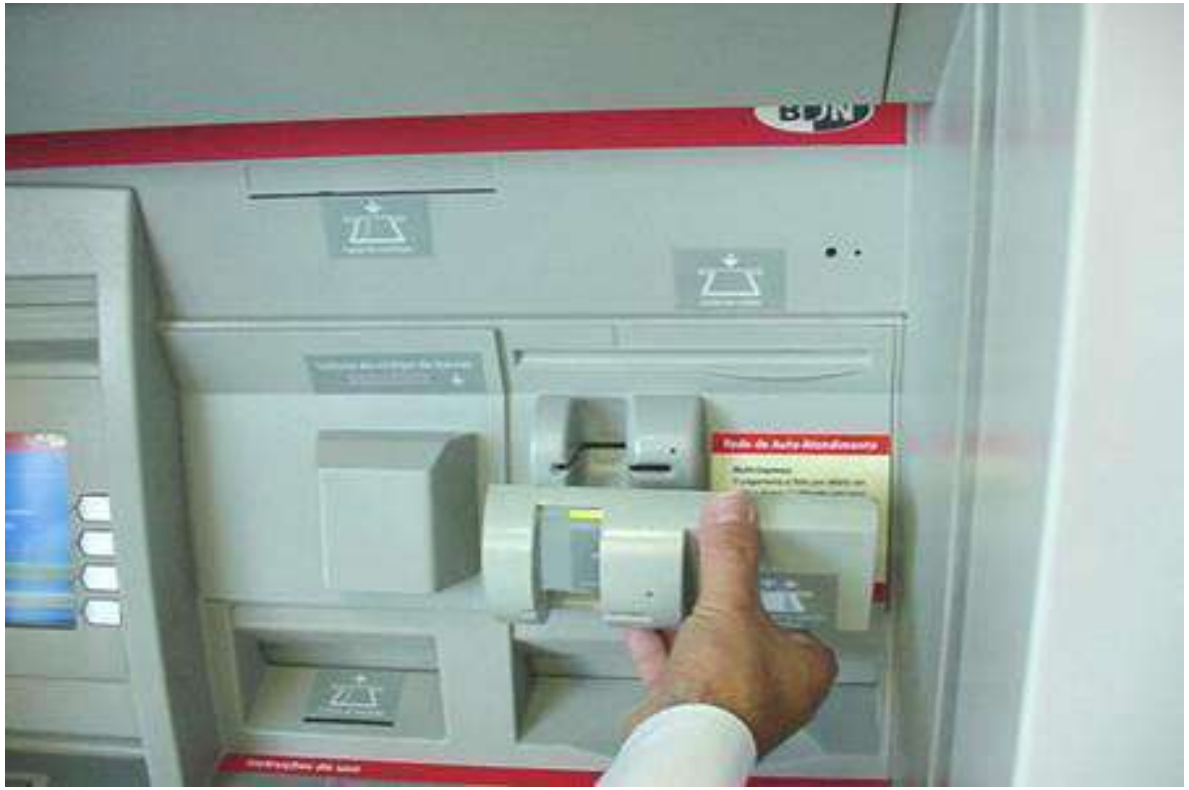
Skimmer device attached to card entry slot.

•The device is designed to look like a standard part of the terminal – its clearly different from the photo on the left.

•No flashing card entry indicator can be seen & the shape of the snout is different.

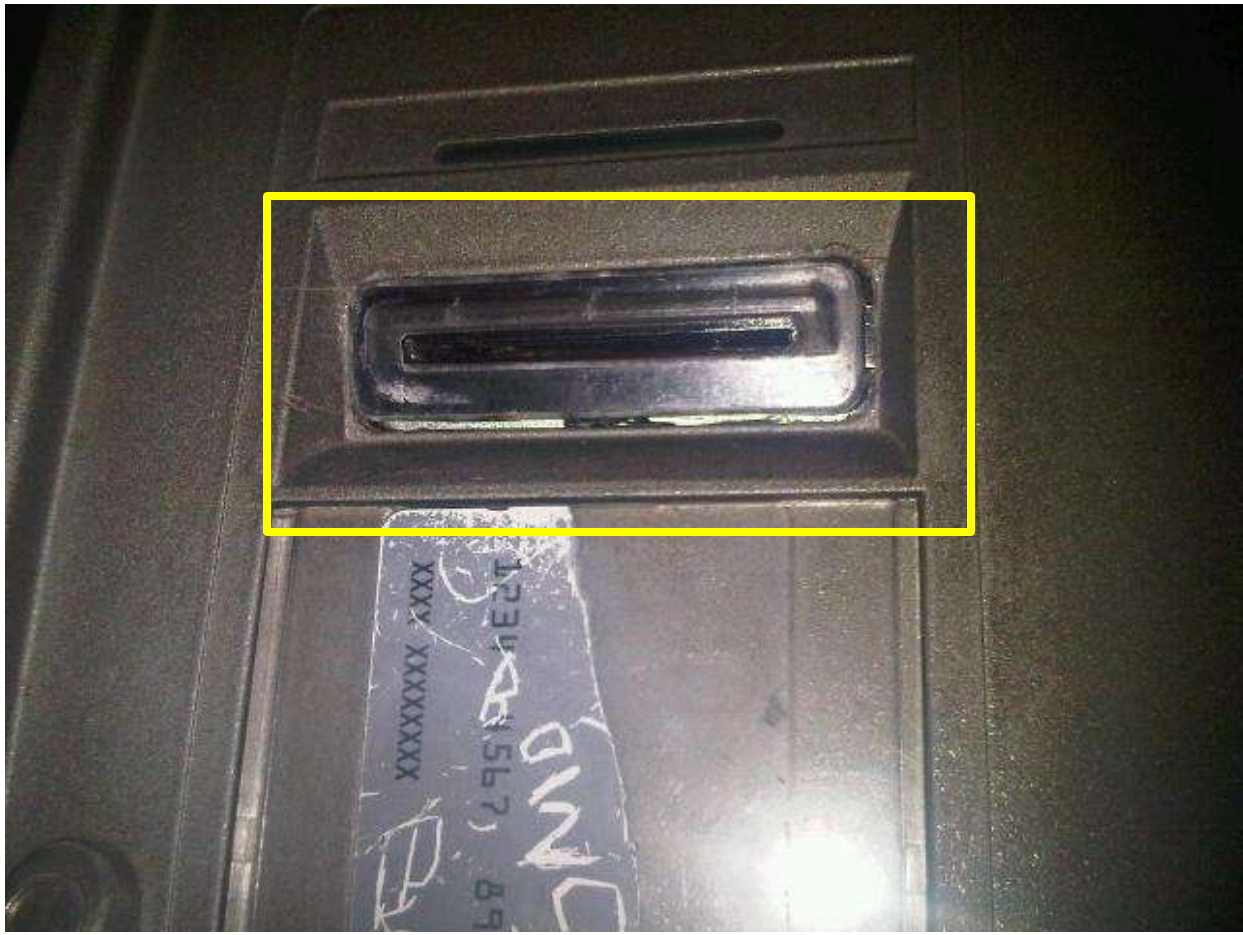
Skimming devices

A skimming device being ‘piggy-backed’ onto the card reader



Skimming devices

A smaller skimmer that looks just like a normal card entry slot and attached to the ATM rain cover.



Skimming devices

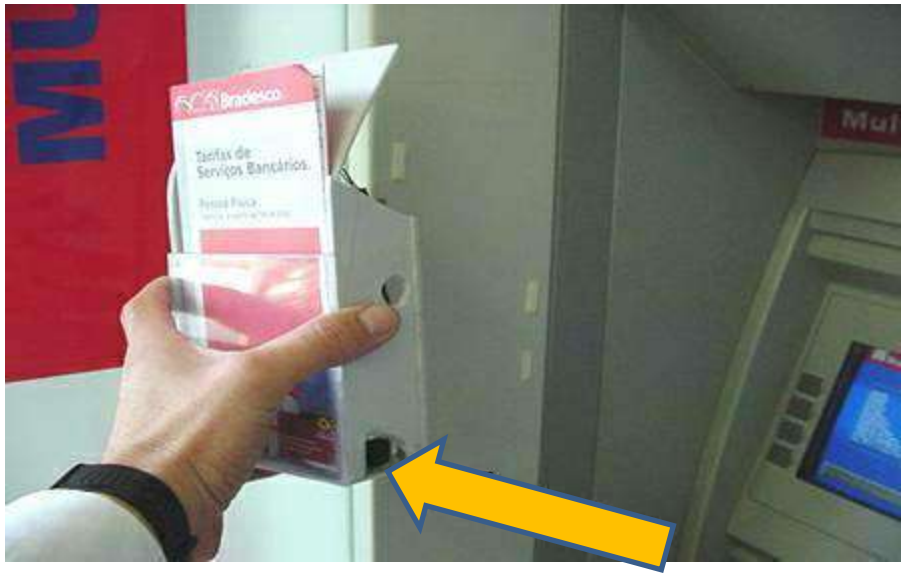
Here a skimming device has been installed on the ATMs card reader.

Skimming devices

Photo shows a PIN capturing device fitted to the top of the ATM. These devices are usually difficult detect

PIN capturing devices

A **brochure holder has been** placed on the side of the ATM fascia wall.

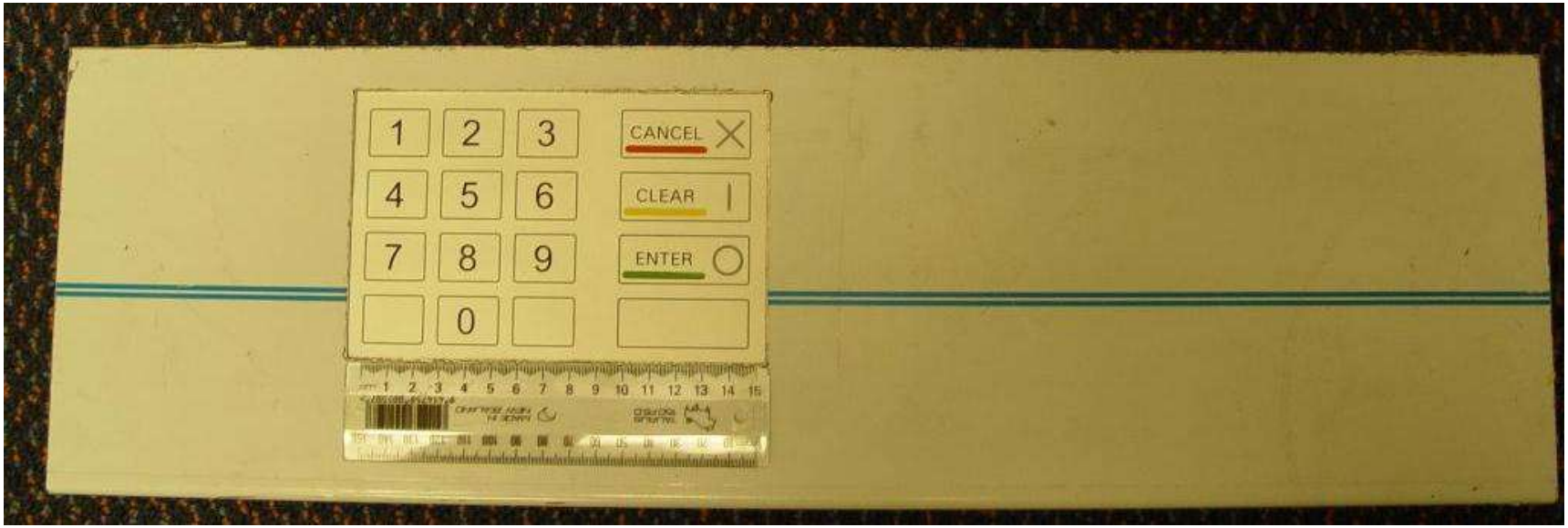


Take a closer look at the **brochure holder –a pin-hole** Camera has been installed. This is done to capture images of the keypad and customers inputting their PIN.

PIN capturing devices –keyboard fascia

A skimmer plate can be placed over the top of the existing keyboard as a method of PIN capturing.

PIN capturing devices



An example of what an ATM skimmer plate can look like.

Facts on skimming devices

Skimming devices are normally attached to ATMs during quiet periods, e.g. early morning / late evening

Length of time skimming devices are attached can vary, but normally no longer than 24 hours.

•Successful skimming requires both a card skimmer (card reader) & camera (PIN capturing device) to be fitted to the ATM in order to steal card data

Criminals may loiter nearby to observe customers & remove equipment after machine use.

Downloaded information can be transmitted wirelessly to other devices.

How can you reduce the risk?

Familiarise yourself with the look & feel of the ATM fascia on machines

Inspect the ATM & all areas of its fascia for unusual or non-standard appearance

Is there anything unusual (card reader, area above the screen)?

Report any unusual appearance immediately to Police or the nearest CBA branch

Always use your hand to shield your PIN when entering itBe vigilant! You can reduce the risk of skimming.

Be vigilant!
You can reduce the risk of skimming.

Thank You

DhanlaxmiBank
established 1927