Group Security

ATM Card Skimming and PIN capturing Awareness Guide

Prepared by Simon Grubisic-
Protective Security Advisor

SECURITY IS EVERYONE'S RESPONSIBILITY

What is ATM Card Skimming and PIN Capturing?

- ATM Card Skimming is a method used by criminals to capture data from the magnetic stripe on the back of an ATM card.
- The devices used are smaller than a deck of cards and are often fastened in close proximity to or over the top of an ATM's factory-installed card reader.
- Pin Capturing refers to a method of strategically attaching cameras and various other imaging devices to ATMs; in order to fraudulently capture the ATM user's PIN.

SECURITY IS EVERYONE'S RESPONSIBILITY

Where to spot a card skimming or pin capturing device on an ATM?

Region 1. Light diffuser area

Region 2. Speaker area

Region 3. ATM side fascia

Region 4. Card reader entry slot

Region 5. ATM keyboard area

SECURITY IS EVERYONE'S RESPONSIBILITY

What do skimming devices look like?

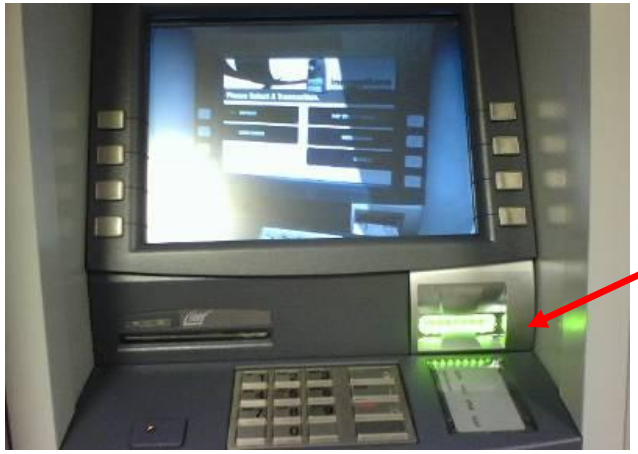
Can you tell if this ATM machine has a skimming device fitted to the card reader?

...

SECURITY IS EVERYONE'S RESPONSIBILITY

What do skimming devices look like?

Spot the difference…Can you tell now?



- **Top photo shows an unadulterated ATM fascia. The flashing lead through entry indicator is easily observed.**

Note: Most skim devices when fitted will obscure the flashing entry indicator this should be a vital clue as to any suspect tampering.

Spot the difference in the next photo.

- **A skim device has been placed in or near the card reader slot. Although the device has been given the appearance of being a standard part of the terminal it is in fact and additional fitted piece & clearly is different from the above photo.**

Note: No flashing lead through light can be seen.

The shape of the bezel is clearly different.

SECURITY IS EVERYONE'S RESPONSIBILITY

What do skimming devices look like?

Here we have another example of the skimming device being piggy-backed onto the card reader

SECURITY IS EVERYONE'S RESPONSIBILITY

What do skimming devices look like?

Here we have another example of a skimming device installed within this piece of ATM fascia. This was a replacement unit found on an ATM.

SECURITY IS EVERYONE'S RESPONSIBILITY

What do skimming devices look like?

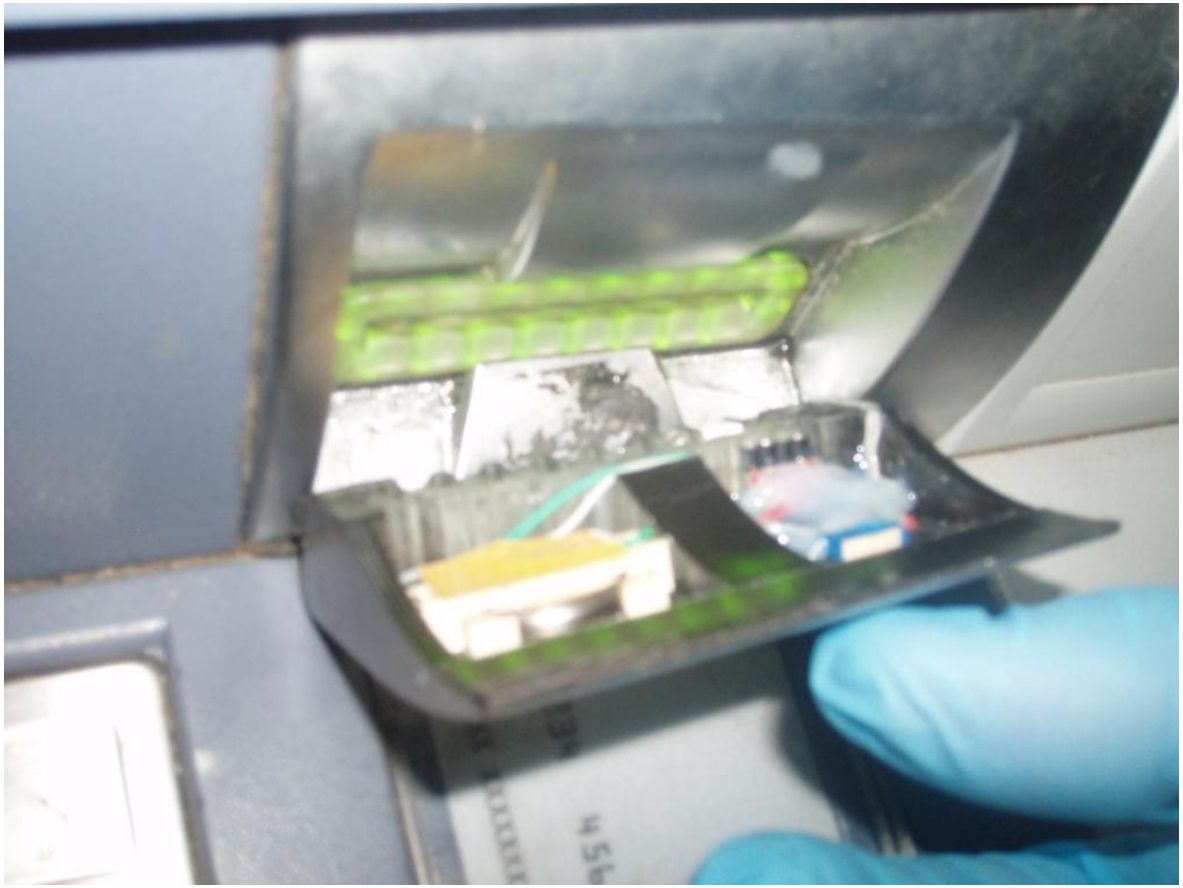
Another example of a skimming device installed on the card reader of this ATM. Hard to tell its there isn't it?

...

SECURITY IS EVERYONE'S RESPONSIBILITY

What do skimming devices look like?

Take a closer look..



SECURITY IS EVERYONE'S RESPONSIBILITY

What do skimming devices look like?

Removal of a skimming device from card reader slot, the device was fitted over the card reader throat.

SECURITY IS EVERYONE'S RESPONSIBILITY

What do PIN capturing devices look like?

Can you tell if this ATM fascia piece (located above the screen) has a PIN capturing device installed within- You cannot really tell can you?

...

SECURITY IS EVERYONE'S RESPONSIBILITY

What do PIN capturing devices look like?

Lets remove the ATM fascia piece for a closer look.

SECURITY IS EVERYONE'S RESPONSIBILITY

What do PIN capturing devices look like?

Here you can clearly see the PIN capturing device installed on the inner side of the fascia piece.

SECURITY IS EVERYONE'S RESPONSIBILITY

What do PIN capturing devices look like?

Another example of a PIN capturing device installed on the inner side of the light diffuser fascia piece (above the ATM screen). Can you see the camera?

SECURITY IS EVERYONE'S RESPONSIBILITY

What do PIN capturing devices look like?

Lets have a look on the inner side. A mobile phone camera was used as a PIN capturing device, with the information being transmitted via a wireless device.

SECURITY IS EVERYONE'S RESPONSIBILITY

What do PIN capturing devices look like?

Here we have an additional fascia piece fitted to the speaker area directly above the screen- can you see this additional piece?

...

SECURITY IS EVERYONE'S RESPONSIBILITY

What do PIN capturing devices look like?

How about now?

Removal of fitted device from fascia- the additional part can now be clearly seen.

SECURITY IS EVERYONE'S RESPONSIBILITY

What do PIN capturing devices look like?

Here we have a piece of merchandising placed on the side ATM fascia wall. Can you spot a PIN capturing device?

...

SECURITY IS EVERYONE'S RESPONSIBILITY

What do PIN capturing devices look like?

Upon closer inspection of the merchandising unit, you can clearly see the pin hole camera installed on the bottom side, capturing an image of the keypad and subsequently, the customers PIN

SECURITY IS EVERYONE'S RESPONSIBILITY

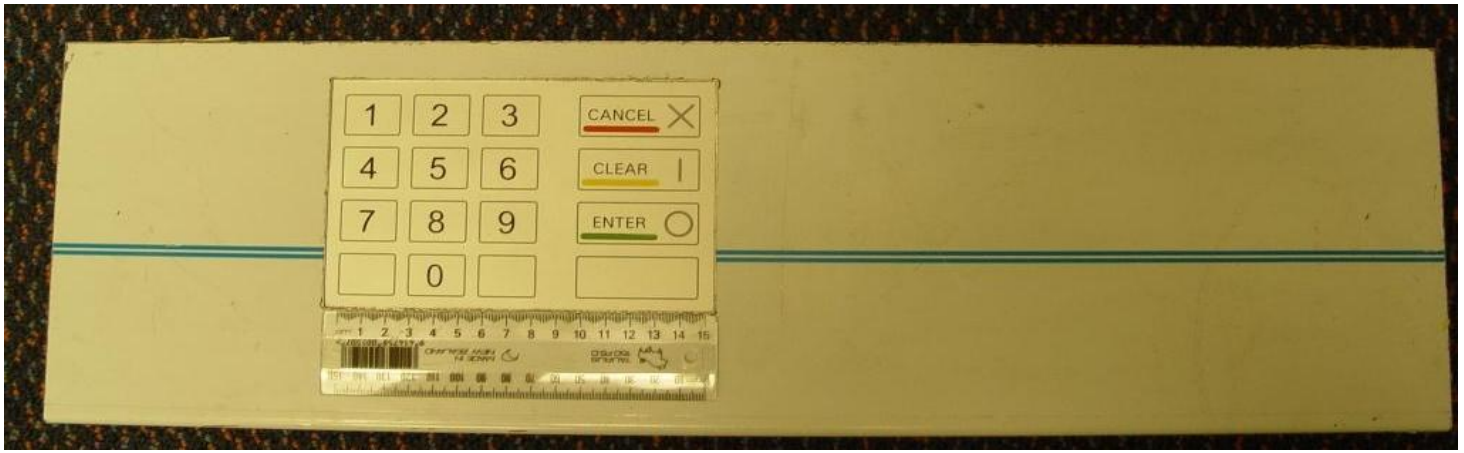
What do PIN capturing devices look like?

The last area of focus is the ATM keyboard fascia. Offenders are known to place the skimmer plate on top of the existing keyboard.

SECURITY IS EVERYONE'S RESPONSIBILITY

What do PIN capturing devices look like?

This is an example of what an ATM keyboard skimmer plate can look like.



SECURITY IS EVERYONE'S RESPONSIBILITY

Facts on ATM skimming attacks

- Criminals tend to attach skimming devices either late at night or early in the morning, and during periods of low traffic.
- Skimming devices are usually attached for a few hours only.
- Criminals install equipment on at least 2 regions of an ATM to steal both the ATM card number and the PIN.
- Criminals then sit nearby receiving the information transmitted wirelessly via the devices (installed on the ATM).

SECURITY IS EVERYONE'S RESPONSIBILITY

What can you do to mitigate the risk of a skimming attack?

- Get to know the appearance of your ATM.
- Inspect the front of the ATM for unusual or non standard appearance. Scratches, marks, adhesive or tape residues could be indicators of tampering. The inspection should be part of your morning external check and afternoon closing procedure. Where possible, inspections should also be conducted during trading hours.
- Familiarise yourself with the look and feel of your ATM fascia. Particularly pay attention to all of the touch and action points. (e.g. keypad, customer card entry slot, lighting diffusers)

SECURITY IS EVERYONE'S RESPONSIBILITY

What can you do to mitigate the risk of a skimming attack?

- **Inspect all areas of the fascia. Look at card reader entry slot & regions immediately above the consumer display and keyboard area for anything unusual.**
- **Report any unusual appearance immediately through to the Group Emergency Hotline on 1800 643 410 and keep watch over any suspect device until the Police or CBA Security arrive.**

By being vigilant you can play a part in reducing the risk of a skim attack!