Group Security

ATM Card Skimming and PIN Capturing Customer Awareness Guide
What is ATM Card Skimming and PIN Capturing?

- ATM Skimming and Personal Identification Number ("PIN") Capturing is a world-wide problem.
- Skimming is a method used by criminals to capture data from the magnetic strip on the back of an ATM card.
- The devices used are smaller than a deck of cards and are fastened in close proximity to, or over the top of, the 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.
- Once captured, the electronic data is encoded onto fraudulent cards and the captured PINs are used to withdraw money from customers’ accounts.
Where to spot Card Skimming or PIN Capturing devices 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
What do skimming devices look like?

Can you tell if this ATM machine has a skimming device fitted to the card reader?
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 skimming devices when fitted will obscure the flashing entry indicator. This should be a vital clue to any suspect tampering.

  *Spot the difference in the next photo.*

• A skimming 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 an additional fitted piece and is clearly different from the above photo. 

  **Note:** No flashing lead-through light can be seen and the shape of the bezel is clearly different.
What do skimming devices look like?

Here we have an example of the skimming device being piggy-backed onto the card reader.
What do skimming devices look like?

Another example of a skimming device installed on the card reader of this ATM.
What do skimming devices look like?

Take a closer look..
What do skimming devices look like?

Here is an example of where a hole has been made in the ATM fascia to insert a skimming device. The fascia plate has then been replaced to conceal the entry point.
What do PIN capturing devices look like?

In this case an ATM fascia plate (located above the screen) has a PIN capturing device fitted to the top of the ATM. It is very difficult to establish.
What do PIN capturing devices look like?

Let's remove the ATM fascia plate for a closer look.
What do PIN capturing devices look like?

Here you can clearly see the PIN capturing device installed on the inner side of the fascia plate.
What do PIN capturing devices look like?

Here we have an another example of an additional fascia piece fitted to the speaker area directly above the screen.
What do PIN capturing devices look like?

In this situation a brochure holder has been placed on the side ATM fascia wall.
What do PIN capturing devices look like?

Upon closer inspection of the brochure holder, you can clearly see it has a pin hole camera installed on the bottom side. This is used to capture images of the keypad and customers inputting their PINs.
The last area of focus is the ATM keyboard fascia. A skimmer plate can be placed over the top of the existing keyboard as a method of PIN capturing.
What do PIN capturing devices look like?

This is an example of what an ATM keyboard skimmer plate can look like.
Facts on ATM skimming attacks

- Skimming devices are normally affixed to ATMs during periods of low traffic, e.g. early morning/late evening.

- Length of time skimming devices can be affixed can vary, but normally are no more than for 24 hours.

- Successful skimming requires both a card skimmer (card reader) and camera (PIN capturing device) to be fitted to the ATM in order to steal card data as PINs are not recorded on the cards themselves.

- Criminals may stay nearby to observe proceedings and remove equipment at short notice in order to later download information. In some cases this data may be transmitted wirelessly to other devices located nearby.
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.
- Familiarise yourself with the look and feel of the ATM fascia on the machines you commonly use. Pay particular attention to all of the touch and action points (e.g. keypad, customer card entry slot, lighting diffusers).
- Always use your hand to shield your PIN when entering it at the ATM.
What can you do to mitigate the risk of a skimming attack?

- Inspect all areas of the fascia. Look at the card reader entry slot & regions immediately above the ATM screen and keyboard area for anything unusual.
- Report any unusual appearance immediately to Branch Staff (if the ATM is located at a branch). For non-branch ATMs contact the Police immediately.

👍 By being vigilant you can help reduce the risk of ATM skimming!