



ATM Security

ATM Card Skimming and PIN
Capturing Awareness

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 data is then transmitted wirelessly to criminals waiting nearby.
- The devices are attached over the top of an ATM's factory installed card reader slot.
- PIN capturing is attaching a camera in a certain position in order to capture the ATM user's PIN number.

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



Light diffuser area

Card reader slot

ATM keyboard pad

What do skimming devices look like?

Can you tell the difference?



This photo indicates an ATM which has not been tampered with. The flashing light on the card reader slot is easy to observe.

Note: Majority of skimming devices once fitted will obscure the flashing light on the card reader slot.



This photo indicates an ATM that has a skimming device placed over the card slot. The device appears to be a standard card reader slot.

Note: No flashing light can be seen.

What do skimming devices look like?

Can you tell the difference?



This photo indicates an ATM which has not been tampered with.

Note: This type of ATM has no distinct features like new ATMs do i.e. no flashing light.



This photo indicates an ATM that has a skimming device placed over the card slot reader. The device appears to be a standard card reader slot.

What do skimming devices look like?

An example of a card skimming device can be seen below. The device was fitted over the card reader.



This photo indicates an ATM skimming device which was placed over a card slot reader.

Note: This type of ATM has no distinct features like new ATM's i.e. no flashing light. Look for a sticky substance, adhesive or tape residue left around the card slot reader.

What do PIN capturing devices look like?



A closer look at the ATM fascia piece.



An inside view of the ATM fascia piece with the PIN capturing device installed.

What do PIN capturing devices look like?

The removal of the fitted device from the fascia can be seen below - the additional part can now be clearly seen.



How to identify a skimming device?

- Get to know the appearance of the ATM and familiarise yourself with the look and feel of the ATM fascia. Pay attention to all of the touch and action points (i.e. keypad, card reader slot, lighting diffusers and fascia).
- Inspect the front of the ATM for unusual or non-standard appearances. Scratches, marks, adhesive, tape residues or holes could indicate that the ATM has been tampered with.

You can protect yourself against a skimming attack?

Yes you can!

- If you do not feel safe using an ATM or think that it has been tampered with, **do not use it.**
- Be wary and alert of people loitering around an ATM. If there are people acting suspiciously, **do not use it.**
- Be suspicious of an ATM if it has a physical sign on it advising you to use another ATM.
- Protect your PIN, when using an ATM ensure that you cover the keypad with your hand when entering your PIN.



Report suspicious activity to SUNCORP

- Report any unusual appearances immediately to Suncorp Bank on 13 11 55.
- **Do not** approach any suspicious people hanging around the ATM under any circumstances.