

ATM Card Skimming & PIN capturing – Customer Awareness Guide



Determined to be different

Group Security
Commonwealth Bank of Australia
November 2009

What is ATM card skimming?

ATM Skimming 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



What is PIN capturing?

Personal Identification Number ("PIN") capturing is a world-wide problem

PIN capturing refers to a method of strategically attaching cameras and various other imaging devices to ATMs to fraudulently capture PIN numbers

Once captured, the electronic data is encoded onto fraudulent cards and the captured PINs are used to withdraw money from customers' accounts



Spotting devices on an ATM



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



Skimming devices



Could you tell if this ATM had a skimming device fitted to the card reader?

Skimming devices: spot the difference



- Normal fascia

An unadulterated ATM fascia. The flashing lead-through entry indicator can be easily seen.

Note: Most skimming devices will obscure the flashing entry indicator. This detail serves as a vital clue in identifying suspect tampering.



- Skimmer device attached 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 - clearly different from the photo on the left.

Note: No flashing lead-through light can be seen & the shape of the bezel is clearly different.

Skimming devices



An example of a skimming device being 'piggy-backed' onto the card reader

Skimming devices



Another example of a skimming device being installed on the ATM's card reader

....Now take a closer look



Skimming devices



An example of where a hole was made in the fascia to insert a skimming device. The fascia plate was then replaced to conceal the entry point

PIN capturing devices



The ATM fascia plate (highlighted in yellow) has a PIN capturing device fitted to the top of the ATM – typically, these devices are difficult for the untrained eye to detect

PIN capturing devices

Closed



Open



The PIN capturing device has been installed on the inner side of the fascia plate

PIN capturing devices



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

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

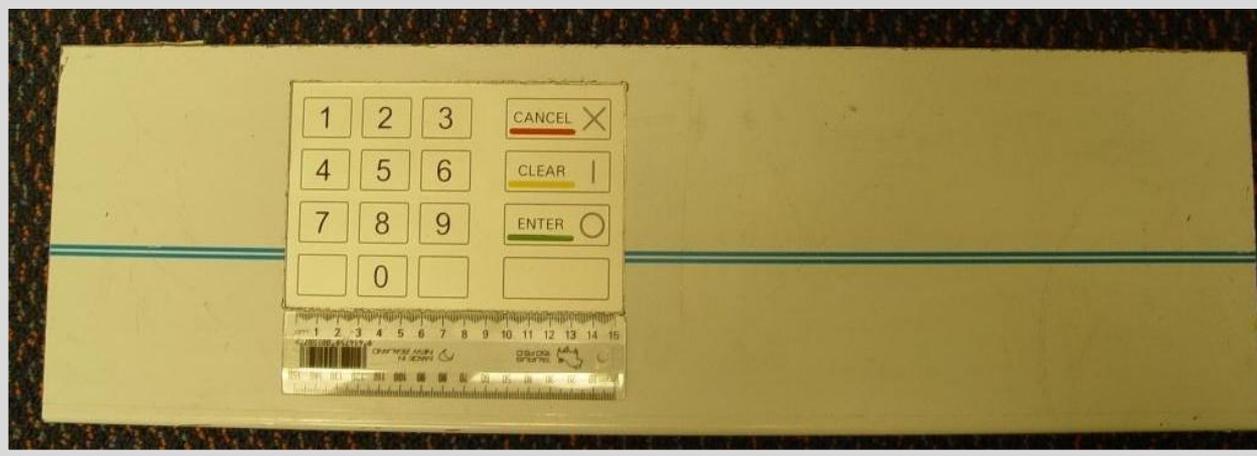


PIN capturing devices – keyboard fascia



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



1

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



2

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



3

- 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



4

- Criminals may stay nearby to observe proceedings & remove equipment at short notice in order to later download information.
- This data may be transmitted wirelessly to other devices located nearby



How can you reduce the risk?

- 1 Familiarise yourself with the appearance of your ATM
- 2 Inspect the ATM for unusual or non-standard appearance
- 3 Familiarise yourself with the look/feel of the ATM fascia on the machines
- 4 Always use your hand to shield your PIN when entering it
- 5 Inspect all areas of the fascia
- 6 Is there anything unusual? (card reader, area immediately above the screen)
- 7 Report any unusual appearance immediately to branch staff or Police

By being vigilant, you can reduce the risk of skimming

