

# Group security

ATM Card Skimming & PIN Capturing  
Customer Awareness Guide

# 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 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

# 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



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

# Skimming devices: the difference



An unadulterated ATM fascia. The flashing lead-through entry indicator is easily observed.  
**Note:** Most skimming devices will obscure the flashing entry indicator. This should be a vital clue to any suspect tampering.



A skimming device placed 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 the skimming device being piggy-backed onto the card reader

# Skimming devices



Another example of a skimming device installed on the card reader of this ATM

# Skimming devices



Take a closer look

# Skimming devices



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

# PIN capturing devices



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

# PIN capturing devices



Let's remove the ATM fascia plate for a closer look

# PIN capturing devices



Here you can see the PIN capturing device installed on the inner side of the fascia plate

# PIN capturing devices



Here we have an another example of an additional fascia piece fitted to the speaker area directly above the screen

# PIN capturing devices



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

# PIN capturing devices



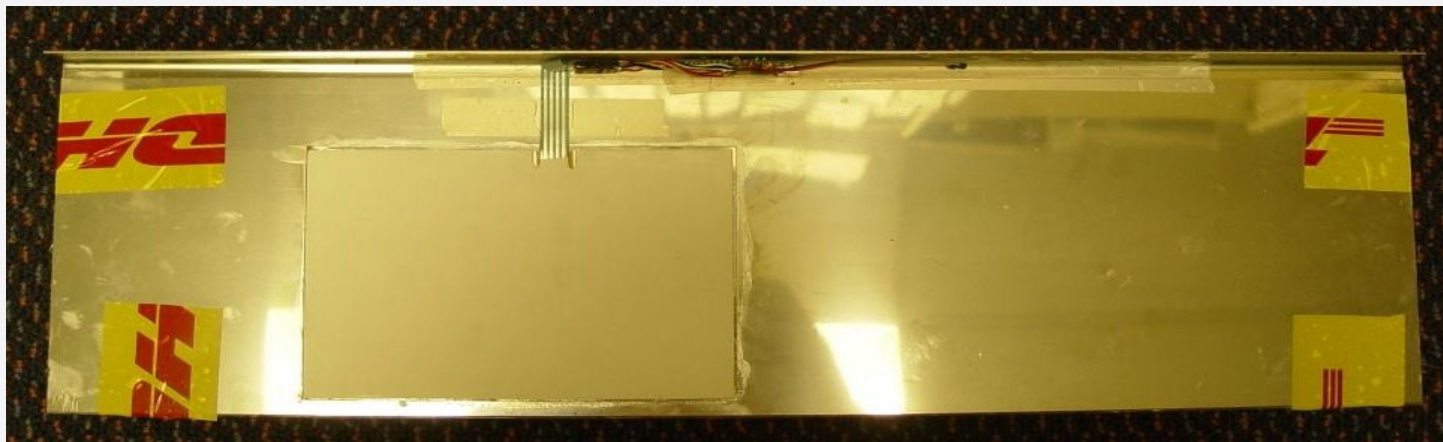
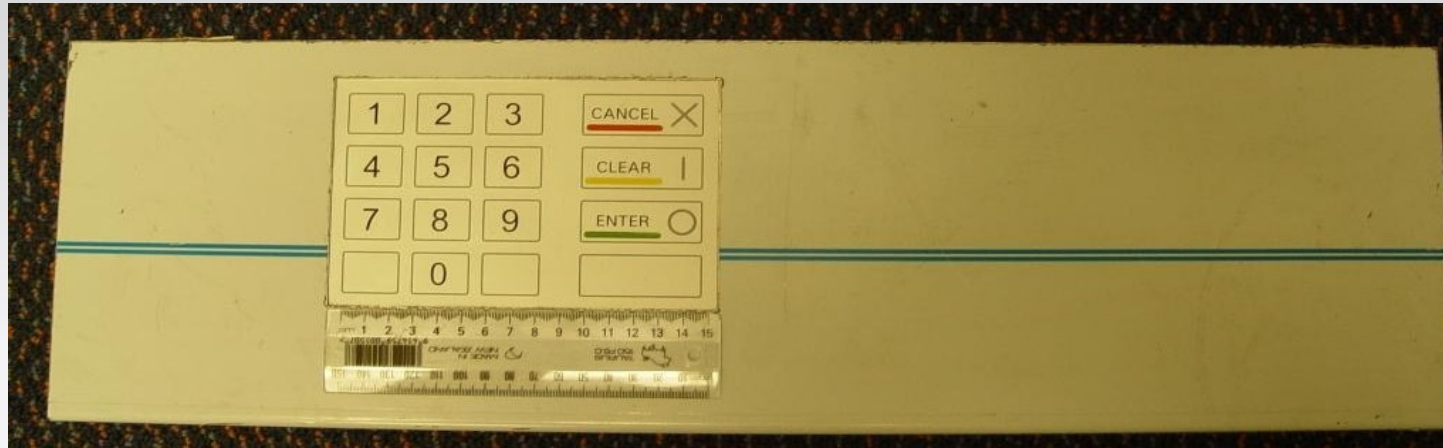
Upon closer inspection of the brochure holder, you can see a pin hole camera installed. This is used to capture images of the keypad and customers inputting their PINs

# PIN capturing devices



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.

# PIN capturing devices



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) & camera (PIN capturing device) to be fitted to the ATM in order to steal card data

# Facts on ATM skimming attacks

- ▶ Criminals may stay nearby to observe proceedings & 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

# Mitigating risk

- ▶ 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

# Mitigating risk

- ▶ Inspect all areas of the fascia
- ▶ Look at the card reader entry slot & regions immediately above the ATM screen & 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!**