

ATM & EFTPOS PIN Security and Skimming Awareness Guide

A member education guide to assist in raising awareness of PIN security and card skimming



ATM & EFTPOS PIN Security and Skimming Awareness

About ATMs & EFTPOS

Automatic Teller Machines (ATMs) and Electronic Funds Transfer Point of Sale (EFTPOS) terminals are used around the world to make either currency available to members or to transact/make purchases electronically with convenience. You can now use an ATM or EFTPOS terminal at all types of locations; at a Credit Union, Building Society or Bank, shopping centres, convenience stores/petrol stations, pubs & clubs and airports. Not all ATMs are owned by Financial Institutions. Some are independently owned by the merchant, others are part of an independently owned network.

Community CPS Australia Ltd owns and operates its own ATMs branded as **rediATM**. These machines are part of the wider **rediATM** network across Australia. Members of course can generally also use a wide variety of different machines with different branding. The ATMs Community CPS own generally look like those below depending on whether they are a through-the-wall machine (below left) or an in-lobby type (below right):



ATM & EFTPOS PIN Security and Skimming Awareness

Secure use of an ATM or EFTPOS terminal

Here are some prudent actions that you can take when using an ATM.

- Choose ATMs that are in well-lit, public or highly populated areas.
- Remove the cash quickly and secure it out of public view as soon as practicable
- Be sure to remove your card
- Be attentive to your physical surrounds during and after an ATM transaction; and

Here are some tips for both ATM and EFTPOS terminal use:

- Make sure that there are no people standing close to you, while you are conducting a transaction.
- Be aware of attempts to distract you
- Cover your PIN number with your hand or purse/wallet when entering it on the keypad

What is Skimming?

Card Skimming is a method to fraudulently capture information contained in the magnetic stripe on the back of your ATM/EFTPOS card. It can occur at either an ATM or an EFTPOS terminal.

An ATM skimming device used to capture this information is often smaller than a standard pack of cards and is fastened close to or over the top of the ATM's factory-installed card reader.

It is generally used in conjunction with a pinhole camera device (either a mobile phone or other image capturing mechanism) that captures your PIN number when you type it in to the keypad on the ATM. This can be located above the keypad (eg: at the top of the screen area) or beside the machine – any location that can surreptitiously view the PIN number being typed on the keypad.

In some cases, the keypad can also be compromised by keypad overlays – which record the key strokes of your PIN. These are not common in Australia at present.

When you are using an EFTPOS terminal:

- Make sure you can always see your card
- Cover your pin
- Only swipe the card once

Skimming in this form has often occurred in taxis and at restaurants – where you handover your card to someone else to swipe. You need to ensure that you are able to perform the swipe yourself, or keep the card in sight at all times.

ATM & EFTPOS PIN Security and Skimming Awareness

What to look for on your ATM

1. Does the ATM look “normal” – are there any unusual additions, markings or changes in the regular appearance of the ATM
2. Are there any “marketing/pamphlet” holders placed around the ATM
3. Is there any evidence of tampering at the machine (eg: glue residue, exposed wires, double-sided tape remnants)

Let’s take a look at some pictures of ATMs with skimming devices

1. How the ATM appeared



3. Damage to front panel, which was revealed after the Card insertion cover was removed



2. The damaged Card reader



4. Mobile phone being used to capture PIN, which was concealed in the light cavity of the ATM



ATM & EFTPOS PIN Security and Skimming Awareness

1. ATM with pinhole camera device in housing above screen with card reader attachment over card slot



2. Close up of card reader attachment over card slot



3. Close up of pinhole camera housing



4. ATM after Pinhole camera device housing removed (ie: this is how the ATM should normally look)



5. Card slot after Card reader attachment removed (ie: this is how the ATM should normally look)



6. Skimming Devices removed and displayed



ATM & EFTPOS PIN Security and Skimming Awareness

Card Entry Slot Skimming Device



Fake façade in situ containing pin-hole camera and recording device.



Pin-hole camera

Multi-media player with transmission capabilities



Camera

mouth slot overlay



ATM & EFTPOS PIN Security and Skimming Awareness

What to do if you think your card has been skimmed?

If you believe your Community CPS card has been skimmed, or if you have suspicions about an ATM or EFTPOS terminal due to its appearance or how the transaction was conducted please contact:

Community CPS Member Contact Centre on 13 25 85 (during business hours) OR

Card Hotline – Redicard or Visa card 1800 224 004

If you see any suspicious persons loitering around an ATM:

- o Do not engage or confront the individuals
- o Move away from the ATM
- o Contact the police when it is safe to do so
- o Check your account as soon as possible and notify your financial institution of any anomalies

For more information regarding ATM and EFTPOS use please come in and see us at one of our Personal Financial Centres or go to our website at www.communitycps.com.au to learn more about how we help you to keep your money secure.

Remember; always cover your PIN entry with your hand, purse or wallet.

