

Fraud Watch

ATM Skimming Incidents on the rise!

Travelling to Sydney? Need to use an ATM? Be aware that unprecedented levels of ATM skimming incidents have occurred.

Over the past 3 months there have been 47 confirmed instances of skimming devices being fitted to ATMs over the East coast of Australia - 45 of these were in Sydney.

What is an ATM skimming device?

An ATM skimming device is a unit that criminals attach to the front of an ATM over the card reader slot, often with a camera also fitted somewhere on or near the ATM. This device reads the mag stripe information on the card ("skimming" the information) and the camera records the customer entering their PIN. Occasionally a false keypad is also fitted.

Usually the ATM appears to work in the normal fashion and the money is dispensed. Some time later the devices are removed, the information downloaded, cards created and then accounts are raided.

Cards skimmed from just one ATM in Sydney recently led to over \$400,000 of funds being stolen from accounts.

How to avoid ATM skimming

- > *If using any ATM, make sure you cover the key pad when entering your PIN.*
- > *Be particularly aware if a passerby stops to assist you when you are using the ATM. These 'helpful' people are often part of the criminal enterprise.*
- > *If you think an ATM looks unsafe or a little different - do NOT use it!*

NSW Police have set up a dedicated ATM Crime Task Force who are working closely with our colleagues in the east as well as the Abacus Fraud & Financial Crimes section.

If you require any further advice please contact Police Credit Union immediately on 1300 131 844 during business hours or 1300 247 489 after hours.

12 March 2009