

You may have heard recently in the media about recent fraud activity regarding Terminal Manipulation fraud. My message this week comes from *Abacus Fraud & Financial Crimes who answer some questions you might have regarding this new fraud trend.

What is it?

Terminal manipulation is a form of card skimming whereby an EFTPOS terminal is compromised by criminals to record card data and PIN numbers. This information is later used to commit fraud on your members account.

What has happened so far?

The first instances of terminal manipulation were identified in October 2009 in WA, where that high profile scam saw around \$2.5 million lost due to a skimming operation through Western Australian McDonalds outlets. In other cases terminals were removed from merchant outlets and replaced with compromised ones. In other cases the terminals had skimming devices inserted when still in the store. Since this time, a large number of further instances have been identified across Australia. It's estimated that losses from this fraud already exceed \$5million.

Mutual sector⁺ losses have been minimal.

What's being done to combat it?

Acquirers are working closely with their merchants to ensure their EFTPOS terminals are secure and compliant to industry and scheme standards. This includes full audits of their terminal fleets, physically securing terminals and ensuring staff are adequately trained in respect to terminal security. This is being given their upmost attention.

Why are we receiving reports of new incidents?

These are not new incidents of terminal manipulation. Though there have been a number of alerts issued recently, these relate to compromises that occurred in September and October of 2009. Only now, as the compromised data is being used for fraud, are they being identified. This is how the majority of card skimming incidents are detected.

To date, six people have been arrested and charged in relation to these matters.

What can I do?

The best thing is to be diligent about keeping your PIN private and to be aware of what funds are in your accounts, and to check your statements carefully.

Some useful tips for your card safety include:

- Regularly change your Personal Identification Number (PIN);
- Following an EFTPOS transaction check store receipts for any irregularities i.e. the store name, details, and location should all match the store from which you made your purchase;
- Regularly check your account statements;
- Be aware of the amount of funds you have in your account;
- Do not write your PIN anywhere;
- Cover your PIN when entering it into a terminal;
- Where possible and if it is available to you, use chip technology;
- If you have concerns contact your credit union or building society immediately.

What is my liability?

Under the EFT Code of Conduct, cardholders are not liable for fraudulent transactions if they did not contribute to the loss or disclose their PIN.

Abacus is aware of our members' concerns about losses experienced by them due to circumstances beyond their control. We are currently working with the relevant stakeholders to make our members' concerns known, and will be working to encourage regulators and APCA to review the fraud liability issue in circumstances where acquirers have failed to implement industry agreed risk mitigates.

If you have concerns or any questions, please contact Holiday Coast Credit Union Risk & Compliance Department at ubelong.com.au for more information.

* Abacus is the industry body representing the Australian mutual sector, comprising credit unions, mutual building societies and friendly societies.

+ The mutual sector has combined assets of some \$75 billion, offering Australians a competitive alternative to banks and access to a range of savings products. Unlike banks, profits are not paid to external shareholders, but put back into better products and services for the over 5.5 million members (customers) and their communities.

