SAFEGUARD AGAINST SKIMMING

APCA
Australian
Payments
Clearing
Association

EVERY DAY,

Australians make more than 10 million retail purchases using debit and credit cards at in-store terminals. Accepting card payments is safe, convenient and essential to the smooth operation of your business.

However, card fraud is a global problem and card skimming at in-store terminals also occurs in Australia. Without the right safeguards in place, any business that uses terminals is potentially at risk. The impact of skimming is significant – it can lead to loss of money, loss of customers and undermine the reputation and credibility of your business. It is vital that you know how to prevent and detect skimming so you can protect your customers and your business from this type of fraud.

This information forms part of APCA's merchant education program to increase awareness on how to safeguard your terminals against skimming. It should be used and distributed in conjunction with the "Safeguard Against Skimming" videos.

"When it comes to fighting fraud, everyone needs to lend a hand. Financial institutions can supply secure systems and processing, but merchants can also protect themselves and their customers by stopping fraud as it happens. This program shows how."

Chris Hamilton
CEO of the Australian Payments Clearing Association (APCA)

"I urge you to take stock of the information in this brochure and follow the steps to protect your businesses. Together with your efforts we can make it harder for organised crime to find a foothold."

John Lawler, APM
CEO of the Australian Crime Commission (ACC)

HOW DO I SAFEGUARD AGAINST SKIMMING?

You can reduce the risk of skimming in your store by taking a few simple steps.

1. DAILY CHECKS

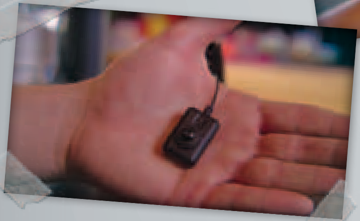
Take careful note of the little things that are unique to your terminal and the area around your terminal. At the start of every shift, check that your terminal:

LOOKS THE SAME AS BEFORE AND HAS NO DAMAGE

HAS THE SAME TYPE AND NUMBER OF CABLES

HAS THE CORRECT SERIAL NUMBER

PRINTS RECEIPTS WITH THE RIGHT BUSINESS NAME AND ADDRESS



IS CLEAR OF ANY HIDDEN CAMERA

If you notice anything different or suspicious, take action. **Tell your supervisor immediately.**

2. TAKE ACTION

During your shift, be constantly aware of your terminal and how it is being handled. **Do not leave your terminal unattended – protect it like you would cash.** If you must leave the immediate area:

- make sure you put the terminal out of sight and reach of customers
- lock the terminal away, if possible.

If you see anyone acting strangely near the terminals or security cameras in your store:

- do not approach the person
- watch them closely without putting yourself in danger
- tell your supervisor as soon as it is safe to do so – your supervisor will contact the police.

Importantly, you can help safeguard against skimming by **telling your supervisor immediately** if:

- you notice anything different or suspicious during your daily checks
- a visitor arrives to service or replace a terminal or security camera
- your terminal is missing
- you see anyone acting strangely or committing a crime.

IMPORTANT INFORMATION FOR SUPERVISORS*

1. KNOW YOUR TERMINALS

It is essential that you and your staff are completely familiar with the terminals in your store so that you can **spot any changes quickly and take action.** Any change to a terminal is an important sign that skimming may have occurred.

It is strongly recommended that you:

- record the following information about your terminals:
  - brand, model and serial number
  - where a particular terminal is kept in your store
  - a description of all cables connected to the terminal
  - details of any security stickers and where they are placed on the terminal
- give your staff forms to help them complete their daily checks – your service provider can help you with this
- ensure your staff check their terminal at the start of each shift and that you personally check every terminal in your store regularly (e.g. monthly).

2. SECURE YOUR TERMINALS

Ensure you **provide a secure place – preferably out of sight and reach of customers** – for staff to put the terminal if they need to leave the area. An unattended terminal is an easy target for criminals – protect it like you would cash.

3. BEWARE OF HIDDEN CAMERAS

Be mindful that **criminals may use cameras** to record customers' PINs, so:

- do not put objects that might hide a pinhole camera near any terminal
- check false ceilings for pinhole cameras
- ensure that your security cameras adequately cover the terminal area – but are not able to record the PIN entered by a customer.

4. ACT ON ANYTHING SUSPICIOUS

If any of your staff notice changes to a terminal or suspect a camera may have been used to record PINs:

- double check all information
- disconnect and remove the terminal
- store the terminal somewhere secure
- contact your service provider.

Report any missing terminals to your service provider immediately. Contact police if you are made aware of any criminal activity in your store.

5. VERIFY SERVICE VISITS

Your staff should direct all visits by technicians and other service contractors to you.

Service visits should always be arranged in advance. **All visitors should be asked to present their security identification (ID).** If the visit was not booked, or the ID does not match arrangements, call your service provider.

6. KNOW YOUR STAFF

Criminals are known to bribe or intimidate staff into helping them with skimming. To protect your staff and your business:

- inform staff how to respond if they are approached by anyone suspicious
- watch for any unusual behaviour among your staff
- do background checks on new staff.

7. PROVIDE STAFF TRAINING

Ensure your staff are informed and aware of how they can safeguard against skimming:

- show them the 'Safeguard Against Skimming' video
- give them a copy of this brochure
- use the posters and stickers provided in this package
- regularly check that they are following the practices recommended in this brochure and the videos.

* See also the video 'Safeguard Against Skimming – More Information.'

WHAT IS SKIMMING?

Card skimming is a crime. Using sophisticated skimming techniques, criminals steal or skim data from a customer's card as it is swiped through the terminal. More experienced criminals will try to get the customer's PIN at the same time. Once they have this information, it is used in various ways to take money from the customer's account. Most often, criminals use the stolen data to make fake cards and withdraw funds at ATMs.

HOW ARE CARDS SKIMMED?

In-store terminals do not save customers' card or PIN details. To skim cards in your store, criminals need to steal your terminal, make changes to it and put it back, or swap your terminal with one they have already modified. Either way, they need to get access to your terminal.

To do this, criminals may:

- pretend to be a technician that has come to service your terminal
- distract you or make a disturbance so that attention is taken away from the terminal
- look for a terminal that has been left unattended or is not locked down.

Often criminals will modify terminals to skim cards and capture customers' PINs. However, criminals may also try to steal PINs by other means including:

- hiding a pinhole camera in a box or other item close to the terminal
- placing a pinhole camera behind a hole in the ceiling or walls
- using a security camera in your store to record customers entering their PIN.

FOR MORE INFORMATION

If you have further questions on card skimming contact your service provider: the financial institution or payment company that supports your terminals.

Your service provider can also arrange for additional copies of the "Safeguard Against Skimming" training videos and other related materials.

APCA
Australian
Payments
Clearing
Association

ABN 12 055 136 519
Level 6,14 Martin Place
Sydney NSW 2000 AUSTRALIA

Supported by:

ACC
AUSTRALIAN CRIME COMMISSION

AFP
AUSTRALIAN FEDERAL POLICE

NSW Police Force

275821 APCA 001_WEB 05/12