HICAPS

PREVENTING HICAPS TERMINAL TAMPERING

The methods used by criminals to gain unauthorised access to merchant terminals to conduct fraudulent activities are becoming more sophisticated.

You can protect your HICAPS terminal and reduce the financial and business risks associated with fraud by being aware of commonly used tampering techniques.

WHAT IS EFTPOS TERMINAL TAMPERING?

Terminal tampering occurs when criminals gain unauthorised access to a HICAPS terminal to commit fraud.

Examples include:

- Stealing terminals to learn how to modify the terminal without it being detected.
- Replacing external components, such as cables, to install listening or skimming devices to capture card data.
- Installing card reader devices into functioning terminals while at a merchant's premises, enabling card data to be captured and collected at a later stage.
- Installing internal devices that enable a cardholder's PIN to be captured.
- Placing miniature cameras on or near terminals to record cardholders' entering a PIN or merchants entering terminal passwords.
- Hacking into business ISP (internet service provider) networks.

WHERE IS TERMINAL TAMPERING LIKELY TO OCCUR?

Terminal tampering can occur anytime and anywhere with criminals targeting:

- Areas of a merchant's premises that are frequently unattended.
- Areas of a merchant's premises where only one staff member is likely to be present at any one time.
- Businesses located in remote or isolated regions.
- Areas which are closed for a period during the day.
- Areas which use mobile/wireless devices.

HOW TO MINIMISE TERMINAL TAMPERING

You can use simple steps to help protect your business from terminal tampering by:

- Maintaining a list of the terminals that includes the type, make, model and serial number. This list and terminals should be checked on a daily basis.
- Checking that serial numbers on the terminals match the serial numbers displayed on the terminal screen.
- Checking for signs of terminal and component tampering.
- Checking that stickers and other visual identifiers are unchanged.
- Ensuring all HICAPS equipment can't be accessed easily by the general public.
- Conducting probity checks before employing new staff.
- Prohibiting unauthorised people from accessing terminals and any CCTV equipment.
- Training your staff about the risks associated with terminal tampering.

WHAT TO DO IF YOU SUSPECT YOUR TERMINAL HAS BEEN TAMPERED

- Disconnect and remove the terminal immediately.
- Contact the HICAPS Help Desk on **1300 650 852** (Monday to Saturday, 8am -10pm AEDT) for a replacement terminal.

WHAT TO DO IF YOUR TERMINAL HAS BEEN STOLEN

- Contact the HICAPS Help Desk on **1300 650 852** (Monday to Saturday, 8am -10pm AEDT) to report the theft and request a replacement terminal.

MORE INFORMATION

Several industry forums and groups provide useful information to merchants on how to minimise merchant terminal fraud.

Visit the following websites:

- www.pcisecuritystandards.org
- www.apca.com.au
- www.visa.com.au
- www.mastercard.com.au

You may also contact the HICAPS Help Desk on **1300 650 852** (Monday to Saturday, 8am -10pm AEDT) or go to **nab.com.au/merchantfraud**