Fraud Protection Guidelines for Merchants

EFTPOS Terminals

Merchants in Australia have been warned to be on alert after recent fraud activities targeting EFTPOS terminals. The purpose of these guidelines is to provide you with a list of issues to be aware of and advice to help prevent fraud at the EFTPOS terminals on your premises.

Fraud activity at EFTPOS terminals

EFTPOS terminals should be treated as securely as cash registers. Why? An EFTPOS terminal that has been fraudulently tampered with can lead to significant losses. Criminals tamper with EFTPOS terminals so that they can gather card account information; the information they capture is used to produce counterfeit cards to obtain cash at a later time. Criminals can also get PINs from the tampered EFTPOS terminal or through other means, such as a hidden camera***. Important:***

- Criminals steal EFTPOS terminals, tamper with them, and then either return them to the same premises or place them elsewhere;
- Criminals tamper with EFTPOS terminals while they are still on the premises.

Vigilance against such activities is essential.

High Risk Issues

Merchants should be particularly vigilant where:

- There is one staff member working on the premises alone
- The business is in an isolated or remote location
- The business is left unattended or closed for a period during the day
- Particular EFTPOS terminals are not attended or supervised from time to time
- Wireless EFTPOS terminals are in use (as it can be harder to keep track of these terminals at all times).

Suggestions for protecting your EFTPOS terminals

- Keep a list of all EFTPOS terminals on your premises, detailing:
  - the make, model and serial number;
  - where each EFTPOS terminal is kept on your premises;
  - any stickers on the EFTPOS terminal and where they are placed; and
  - the type of cables connected to the EFTPOS terminal.
- ***Daily***, check the serial number underneath the EFTPOS terminal against the serial number you have recorded on your list and/or that is displayed electronically on the EFTPOS terminal (if applicable). These MUST match.
- ***Daily***, check for any evidence of tampering:
  - Do all the details recorded on your list still match your EFTPOS terminals?
  - Have any stickers been removed or replaced?
  - Does any part of the cabling look different?
  - Are any additional or unknown items of electronic equipment connected to the EFTPOS terminal?
- ***Daily***, check that the merchant name on the receipts being issued by the EFTPOS terminal is the correct one.
- Lock the EFTPOS terminal in its position with, for example, a cable lock. Remove and secure the EFTPOS terminal when it is not in use (if practical).
- Regularly conduct an inventory check on your EFTPOS terminals. Report missing or stolen terminals to your provider.
- Always verify the credentials of service staff or “official” visitors to your premises. Do not allow unannounced service visits or inspections.

- If an EFTPOS terminal is being connected (e.g. a new terminal or after overnight securing) make sure this is done by authorised personnel, preferably by two staff members.
- Only buy terminals that have been approved by the Australian Payments Clearing Association and are listed on its website (www.apca.com.au). Always buy from a legitimate distributor or vendor and be wary of refurbished terminals.
- Dispose of old EFTPOS terminals securely – return old terminals to your acquirer or to the original terminal vendor.

Suggestions for protecting EFTPOS terminal connections

- Ensure that the point at which your EFTPOS terminal connects to the network is not easily accessible to the general public. This will make it more difficult for criminals to simply "plug in" and activate a replacement EFTPOS terminal.
- Have a warning notification or an alarm alert activate when an EFTPOS terminal is removed or replaced in the network.
- Include in your procedures that when an EFTPOS terminal is connected or reconnected, authorisation must be given before it can "go live".

Suggestions for protecting against staff risk

Criminals may attempt to trick, bribe or threaten your staff into 'looking the other way'. What can you do?

- Do not allow staff access to CCTV equipment.
- Do background checks of new staff.
- Allow only senior staff to replace terminals and perform the checks detailed above OR preferably have two staff members undertake these activities together.
- Randomly check that your staff members are complying with these guidelines.

Protecting against risk of PIN capture

Criminals may attempt to obtain details of PINs from customers, for example by using concealed pinhole cameras. What can you do?

- Check false ceilings above where the EFTPOS terminal is kept.
- Check boxes (e.g. boxes with leaflets or charity boxes) near the EFTPOS terminal.
- Be aware of anything different in the area around the EFTPOS terminal – it may be hiding a small camera.
- Make sure your surveillance camera adequately covers the area where an EFTPOS terminal is kept but is not able to record the PIN as it is entered by a customer.

Report and disconnect suspicious terminals

If you suspect that an EFTPOS terminal has been tampered with, or you notice anything suspicious:

- disconnect the terminal immediately and contact your EFTPOS services provider; and
- keep the EFTPOS terminal in a secure place so that any evidence (e.g. fingerprints) will be preserved.

Staff education

- Ensure staff members are aware of, and trained in, the need to follow these guidelines.
- Consider introducing rewards for staff members that detect any fraudulent activity on your premises.