

## Transactions with your chip and PIN terminal

Chip and PIN has been highly successful in reducing certain types of fraud but criminals will always try to target shops and business in order to obtain card details and PINs to commit fraud.

To help all card-accepting businesses better protect themselves and their customers APACS has developed this advice guide to help minimise the chances of being targeted.

### Why do criminals target cards, card details and PINs?

Fraudsters try to capture card details and PINs in order to produce fake magnetic stripe cards, which can then potentially be used in shops or cash machines that haven't upgraded to chip and PIN – mainly overseas.



### Threats

Listed below are some of the main forms of attack in the shop environment:

#### Electronic Attacks

These are attacks on the chip and PIN terminal or the software used to process card details and include attempts by criminals to place illegal, data-capturing devices, bugging equipment or software in chip and PIN terminals or installing pinhole cameras, focused on a keypad, that record customers' PINs.

#### Substitution Attack

Fraudsters attempt to remove parts or all of the chip and PIN terminal and substitute them with doctored or bogus devices that capture card data or PINs. Criminals may attempt to install fake equipment by posing as bogus service engineers.

#### Theft

Criminals may try to steal chip and PIN terminals with the aim of: gaining access to any stored data held in the device; learning about their inherent security features; or attempting to doctor the device prior to re-installing it in a shop environment.

#### Members of Staff

Criminals may target businesses by applying for jobs or coercing existing shop staff into helping them so they can access chip and PIN terminals, install pinhole cameras or skim cards through the use of handheld card readers.

# Advice to help keep chip and PIN equipment safe and secure

Chip and PIN terminals need to meet specific levels of security that are set by Visa, MasterCard and APACS. On top of this it is essential that the location where they are being used is physically secure and that the devices are safely looked after. The following advice can help keep chip and PIN equipment safe and secure:

## Physical security of equipment

- The physical location of the chip and PIN terminal and security of its parts should be considered. Can it be removed easily; are the separate parts physically protected to prevent tampering or theft? \*
- Chip and PIN terminals should always be placed in a location that allows the customer to use them in a way that prevents other customers from seeing the PIN. Where practical, terminals should include PIN shielding.
- Secure cradles should be used to minimise opportunities for criminals stealing the terminal. \*
- CCTV should be used to cover the till area. Cameras must be fixed so that a customer's PIN cannot be identified. Access to CCTV footage should be restricted to authorised staff and measures in place to ensure that it is not possible to interfere with the recordings. \*\*
- Routines should be implemented to check the condition of chip and PIN equipment on a regular basis to ensure that it has not been tampered with. Checks should include an inspection of the cabling to ensure that nothing has been added.
- Only authorised personnel should be allowed access to chip and PIN equipment so always ask for identification and be very suspicious of any engineers turning up without prior arrangement.
- A process that oversees any changes to chip and PIN equipment - with appropriate audit trails - should be in place, especially where external suppliers provide maintenance checks.

\* Care must be taken to balance these security needs with the requirements of the Disability Discrimination Act 1995

\*\* See also the Information Commissioner's CCTV Code of Practice ([www.ico.gov.uk](http://www.ico.gov.uk))

## Managing chip and PIN equipment

Chip and PIN terminals are valuable assets and should be treated as you would the cash in a till. They should also be subject to good management routines:

- Retailers should devise an inventory to record the serial numbers of their terminals and the location where they are installed (including replacements and spares).
- Regular checks should be carried out to ensure that these devices are where they should be and that any changes are authorised and noted in an asset management record.
- Shop managers should also have systems in place to review inventories and asset management records on a regular basis and have procedures in place when any inaccuracies are spotted.
- Where equipment consists of several different components, each part should authenticate itself to the terminal – this may take the form of a regular 'heart beat' check. Any unusual events (such as missing heartbeats) should be flagged for supervisor attention.

## Staff security

A standardised recruitment and vetting procedure, including criminal record checks, should be adopted that covers all employees (full, part time, temporary and contract).

- Employee application processes should include checking an applicant's work history and work record, as far as is allowed by law.
- A documented security policy should be developed that is available to all staff and, where possible, responsibility for security matters should be allocated to a manager who can act as a single point-of-contact for all staff.
- Security training should be carried out to remind staff of their responsibilities at least annually (and more regularly where staff turnover is high). This training should be an integral part of the induction of new staff.
- Staff should be made aware of all the potential ways that criminals target card data and encouraged to report any issues or concerns they may have.
- Any security-related activities involving chip and PIN equipment should be carried out under the supervision of more than one employee or manager.
- Staff access to sensitive data should be managed accordingly. This includes staff who have no operational responsibility but have physical access to buildings (e.g. staff not directly employed by your organisation - such as cleaning and maintenance staff.)
- Staff who are approached or coerced by criminals into acting fraudulently should contact the police immediately.
- When employees leave the employment of an organisation it is important to ensure that all of their access rights and security related entitlements are revoked. In particular ensure that all keys are returned and that any physical access codes are changed so that they cannot subsequently enter secured areas.