



PIN Entry Device (PED) Security Guidelines for Retailers



Who are we?

The Irish Payment Services Organisation (IPSO) Limited is the representative body for the payments industry in Ireland. IPSO Card Services is a dedicated unit of IPSO which promotes safe card use and acceptance. IPSO Card Services provides information on payment card fraud and its prevention via its website www.SafeCard.ie and other relevant awareness campaigns.

The Garda Bureau of Fraud Investigation (GBFI) is a specialist agency that investigates fraud-related crime involving complex issues of criminal law or procedure. The GBFI investigates serious and complex cases of commercial fraud, cheque and credit card fraud, counterfeit currency, money laundering, computer crime and breaches of the Companies Acts and the Competition Act

The issue:

Criminals have found it possible to insert data capturing equipment into the devices used to input credit/debit card and PIN details at retail outlets. These devices are known as PIN Entry Devices (or **PEDs**).

The method involves the theft of PEDs from stores and retail outlets. These stolen PEDs are re-engineered and fitted with additional equipment inside. It should be noted that the criminals have overcome the security features of several different manufacturers. The compromised devices are then installed into a retail outlet, such as a supermarket or petrol station, (often with the assistance of a collusive member of staff) and card details and PINs captured from transactions. This data is transmitted to the criminals who then use it to create fake credit cards that are used abroad at non-Chip terminals.

What can you do to prevent this happening?

Great care is taken to ensure that the security of new PIN Entry Device (PED) products meets the highest industry standards. However, it is not sufficient to rely solely on this security to protect cardholders' details from being defrauded at merchant locations. Additional security can – and must – be provided by merchants to enhance the security provided by the terminal itself. You can achieve this by considering all the factors that can influence overall security and taking the necessary countermeasures detailed in this document to ensure a high level of security for cardholders using your merchant facility.

Review current security around your PEDs including:

- Ensure your PED estate is fully audited and recorded (i.e. collate a list of the serial numbers and any other identifying numbers for your outlet/s)
- Review condition and placement of internal CCTV systems to cover all till areas
- Regularly review those who have access to recording equipment (On occasions when PEDs have been stolen or replaced in the past, it was found that CCTV had been turned off or turned away from the area of criminal activity)
- When returning PEDs to your acquiring bank due to a break-down, ensure the return is properly recorded and that returns to the manufacturer are audited (Cases in other countries show that some returned PEDs have subsequently been found to have been tampered with and reused to commit crime)



- Consider how such a device might be placed at your premises. Staff may be approached and offered money or other rewards to facilitate the placing of corrupted PEDs at your outlets. Encourage staff to report anybody approaching them in this way
- Consider IT solutions that detect PED replacement on the system such as monitors which show if devices have been uninstalled for a period of time. For more information on the systems available, contact your acquiring bank or integrated terminal provider

What Action to Take:

1. PED Theft

If you discover that a PED has been stolen:

- Contact the Gardaí and report the theft
- Secure any CCTV images of the theft
- Retain any other evidence such as details of witnesses, staff or otherwise for the investigating officer
- Advise your acquiring bank or processor
- Follow all other procedures in line with your own company's policies

2. PED Compromise

If you believe that one or more of your PEDs have been compromised or tampered with:

- Remove the device and retain securely. Seal in a tamper proof bag if available
- Record the exact date and time the PED was disconnected from the system or 'powered down'
- Record the style, type, and colour of any connected leads, plugs, aerials etc., or take a photograph
- Contact Gardaí and your acquiring bank or processor immediately to report the incident
- Contact your company security and comply with any other company policy
- Secure any CCTV evidence and retain staff records