

# CARD NOT PRESENT (CNP) TRANSACTIONS



## CNP transactions include payments via mail-order, telephone and the Internet

There are potential fraud risks when accepting CNP payments. Since the card is not present, you cannot verify the cardholder, i.e. neither a PIN nor a signature can be obtained. Some of your questions about CNP transactions are answered below.

### Does authorisation mean a payment is guaranteed?

No. An authorisation confirms that a) the card has not been reported lost or stolen at the time of the transaction and b) that there are sufficient funds in the account to cover the transaction value.

### How can I check that the cardholder is genuine?

- Request a landline phone number and check the name and address details against those in the phone book.
- You can request a Card Security Code (CSC) from the cardholder and confirm it is correct via your processor. This helps to confirm that the person using the card details has the genuine card with them.
- 3D Secure is an option for internet use.

### Below are a few of the tell-tale signs of a fraudster at work in a CNP environment. Watch out for these:

- Is a high value sale being conducted too easily?
- Is the customer disinterested in the overall price or exact details of the goods?
- Is it a new customer, purchasing multiple high-value goods?
- Is the customer reluctant to give a landline phone number?
- Is the customer being prompted by a third party whilst on the phone?
- Is the customer attempting to use more than one card in order to split the value of the sale?
- Does the customer seem to have a problem remembering their home address or phone number?

Answering “yes” to one or more of the questions above during a CNP sale does not mean that the customer is a fraudster but it should encourage you and your staff to consider carrying out further checks before proceeding with the transaction.



### IF YOU ARE SUSPICIOUS OF A CARD OR A CUSTOMER, CARRY OUT A CODE 10 CALL TO YOUR CARD PROCESSOR WHO WILL ASK YOU TO REQUEST SPECIFIC INFORMATION FROM THE CARDHOLDER TO ENSURE THEY ARE GENUINE

Do not hand the card back. Call the authorisation centre and let the operator know you are suspicious by simply saying that you are making a Code 10 call. The bank won't mind if it's a false alarm - it is better to be cautious than to let a card criminal deceive you and your employer. Above all, never put your colleagues, customers or property at risk.



Bank of Ireland



Elavon  
MERCHANT SERVICES

GE Money

HALIFAX

MBNA  
EUROPE

National Irish Bank

permanent tsb

Ulster Bank

For more information on simple, yet effective, fraud prevention advice visit [www.SafeCard.ie](http://www.SafeCard.ie)