Card Not Present (CNP) transactions

Provided you have received written agreement from Cardnet you may accept a telephone or mail order from a cardholder who wishes to pay using a Visa, MasterCard, Maestro or Solo card.

You must not accept internationally issued Maestro cards for CNP transactions. Visa Electron cards can be accepted for CNP, as long as transactions are always authorised.

When accepting a CNP order, please take extra care to ensure you have permission to debit the card account and it is the genuine cardholder who placed the order as you are responsible for any transactions where the card and the cardholder are not present.

The following examples are all acceptable as CNP orders.

Mail orders – written authority from the cardholder, bearing the cardholder's signature in any form including:

- completed order forms
- facsimile transmissions.

If you conduct CNP transactions by mail, the cardholder's signature must appear on your order form. You must also keep the instruction for 18 months in case the transaction is disputed at a later date.

Telephone orders – authority from the cardholder by telephone.

When taking an order by telephone always record in writing all details of the transaction along with time and date of the conversation as you may be asked to produce this or the cardholder's authority for a CNP sale if the transaction is disputed at a later date.

For all orders received by mail, telephone or fax, goods must be delivered and it is advisable to keep documentary evidence of the delivery address for 18 months.

If you are unable to deliver the goods immediately, your authorisation is only valid for seven calendar days.

All mail/telephone order transaction records must be kept securely. Full details about how to store cardholder information can be found in Section 7, Security.

Other important fraud considerations

Remember – an authorisation code only indicates the availability of a cardholder's credit and that the card has not been blocked at the time of the transaction. It does not guarantee that the person using the card is the rightful cardholder.

Do not, under any circumstances, process transactions for any business other than your own. Some fraudsters offer commission to process transactions while they are awaiting their own credit card facilities or where they have not been successful in obtaining their own. If you process transactions on behalf of any other business/person you will be liable for any chargebacks and could put your own Cardnet facility at risk.

Fraud prevention

Transaction laundering

If you are approached with a proposal to buy card transactions, you must contact us immediately on **01268 567100**. This is a form of money laundering and is contrary to the terms of your Retailer Agreement.

Phishing emails

If you receive an email from somebody claiming to be a bank or an official business asking for transaction details of all cards recently accepted for payment, you must report this to Cardnet straight away on **01268 567100**. This is a fraud tactic to obtain card details. A bank or any other official business would never make contact in this way to request card information.

Fraud prevention programmes

Some businesses are more prone to fraud than others and you may be unfortunate enough to suffer a fraud attack, particularly if you offer goods that are attractive to fraudsters and can be easily, but illegally, resold.

It is your responsibility to protect your business from financial loss. it is also imperative that you and any staff that you employ follow the contents of this manual carefully at all times.

If you are concerned that you may be vulnerable to fraud attack, perhaps because of your business location or local intelligence, please contact the Cardnet Helpline and ask to speak to our Fraud Department who will be happy to help with guidance on best practice.

Please remember following the procedures contained in this manual is no guarantee that you will avoid incurring financial loss if you suffer a fraudulent transaction. You will remain ultimately responsible for any financial loss you incur as a result of any fraudulent transaction.

Further information on fraud prevention can also be found at **www.cardwatch.org.uk** as well as literature for staff awareness.

Collecting cardholder information for CNP transactions

When a cardholder is not present for the sale, you must obtain the following information in order to verify their identity and help validate the transaction:

- card number
- card expiry date
- card issue number, if present on the card
- cardholder name and initials as shown on the card
- the Card Security Code (CSC) (the three digit number on the signature strip on the back of the card, or on American Express cards the four-digit number on the front of the card)
- the address known to the cardholder's bank (for example where their card statements are sent to)
- contact telephone number (It is higher risk to accept a mobile telephone number).

This information will enable you to carry out the usual status check so that you can confirm whether the cardholder has sufficient funds to pay you. It also allows you to find out whether or not the card has been reported lost or stolen.

You will be asked to produce this information, except for the CSC, if the transaction is disputed at a later date.

Important

Under no circumstances can goods paid by mail or telephone be handed over the counter to, or collected by, the cardholder. See Section 7, Security, How to guard against fraud.

If a cardholder wishes to collect the goods, then they must attend your premises in person and produce their card. Any Sales Voucher already prepared must be destroyed and an over the counter transaction processed. If you have already completed a CNP order you must either cancel the transaction or perform a refund. If you perform a refund, please let the cardholder know that the original transaction, a refund and the over the counter transaction will all appear on their card statement.

If authorisation was obtained for the original transaction, or your terminal indicates that manual authorisation is required, you must telephone the Authorisation Centre.

The Address Verification Service (AVS) and Card Security Code (CSC)

Since the introduction of chip and PIN fraudsters have increased their activity in Card Not Present transactions.

As you are responsible for any transactions where the card and the cardholder are not present, as well as collecting the Card Security Code (CSC), we recommend you complete these transactions using the Address Verification Service.

How to guard against fraud

Over the counter transactions

Please make sure that all staff accepting payment by card on your behalf have read and understood the following guidelines which aim to reduce the possibility of fraud.

These suggestions could help you to prevent fraudulent transactions that could result in a chargeback to you.

- Upgrade your equipment to be chip and PIN-capable.
- Be extra vigilant if you are presented with a card that does not carry a chip as these are less secure and more likely to be used to perpetrate fraud.
- Ask yourself does the cardholder appear nervous/agitated/hurried?
- Is the cardholder making indiscriminate purchases?
- The cardholder makes an order substantially greater than your usual sale, for example, your average transaction is £40, but this transaction is for £400.
- The cardholder insists upon taking the goods immediately, for example, they are not interested in free delivery, alteration or if the goods are difficult to carry.
- The cardholder takes an unusual amount of time to sign the voucher and refers to the signature on the back of the card.
- The cardholder takes the card from a pocket instead of a wallet.
- The cardholder repeatedly returns to make additional orders in a short period of time causing an unusual/sudden increase in the number and average sales transactions value over a one to three-day period.
- The sale is at an unusual time of day for your business.
- The cardholder tells you that he/she has been having problems with his/her card for payment where multiple transactions are subsequently declined but eventually an authorisation is obtained for a lower amount. (Most genuine cardholders know how much available credit they have.)
- A fraudster may present more than one card, often to find a card that will be successfully authorised. If this happens, take particular care and also look out for cards presented, issued by the same bank, where the card numbers are sequential or very similar. When in doubt, make a 'Code 10' call to the Authorisation Centre.
- Most floor limits are now zero. However, if you have an electronic terminal with a floor limit and you wish to reduce exposure to fraud, you may request a reduction to your terminal floor limit. Not only will this reduce fraud but it may also reduce chargebacks due to invalid cards. Please contact your terminal supplier to arrange this reduction.
- You should be on guard when chip and PIN cards are presented and the PIN is blocked or the incorrect PIN is entered. You should check that this is the genuine cardholder because you are at risk if you accept a signature in these circumstances.

Remember: If the appearance of the card being presented or the behaviour of the person presenting the card raises suspicion, you must call the Authorisation Centre on **01268 822 822** and state "This is a Code 10 call" and follow the operator's instructions.

There are a number of extra checks you can make to help make sure you are dealing with a genuine cardholder including:

- Use Verified by Visa and MasterCard SecureCode for E-commerce transactions. See Section 4, Accepting transactions.
- For business cardholders not known to you, check their details in your local business directory or Internet search engine.
- Private cardholders' addresses not known to you can be checked against the Electoral Register, telephone directory, from a BT CD-ROM phone disk or Internet map searches.
- Obtain a telephone number for the cardholder's address through 118 Directory Enquiry Service, if possible, and telephone the cardholder back on that number to confirm the order. (Not necessarily straightaway.)
- Be aware if the cardholder is suggesting unusual arrangements such as going back for another card number if the one given is refused.
- Check your records to see if you have had a number of transactions over a short period of time from a company or individual with whom you have not had any previous dealings.
- Also check to see if there are any unusual features or consecutive sequences in the card numbers given over a period. (Usually fraudsters will offer card numbers that are the same except for the last four digits. This could mean that a batch of cards has been stolen.)
- Be especially wary if the delivery or cardholder's address given is overseas and products purchased are readily available in that locality.

Also be particularly wary of:

- demands for next day delivery
- alterations of delivery address at short notice
- phone calls on the day of delivery asking what time the goods are due to be delivered
- mulli-tiered addresses for example, units, flats.

Danger signals

If any of the following happen, we recommend you make extra checks. This list does not cover every eventuality – some fraudsters spend a long time building up credibility and then request an extremely large order that is 'too good to be true'.

- Is the sale almost too easy? Is the caller disinterested in the prices/precise details of the goods, particularly if it is a new customer? Is the stock ordered of high value or easily resold merchandise?
- Is the sale excessive in comparison with your usual orders? Is the cardholder ordering lots of different items? Does the spending pattern fit your average customer?
- Is the customer giving you a third party's card number, claiming to be acting on behalf of a 'client'?
- Does the caller match the card? Do not accept orders from someone quoting someone else's card details for example, woman using husband's card or a business using a personal card. It may well be a genuine call, but it pays to check.

- Never split an order to avoid authorisation, or at the suggestion of the cardholder – for instance, if they offer two card numbers to cover one order.
- Is the caller suggesting any unusual arrangements? For example, "if the card number I've given you doesn't have sufficient funds let me know and I'll give you another number."
- Is the caller being prompted by a third party whilst on the telephone?
- Does the caller seem to have a problem remembering their home address or telephone number or do they sound as if they are referring to their notes?
- Does the cardholder seem to lack knowledge of their account?
- Is the card-issuing bank/building society based overseas?

Please remember you remain ultimately responsible should a transaction be confirmed as invalid or fraudulent, even if the AVS and CSC data matches and an authorisation code is given.

Delivery warning signals

Here are some danger signs to look out for when arranging delivery of goods.

- Goods should not be released to third parties such as 'friends' of the cardholder, taxi drivers, chauffeurs, couriers or messengers. (However, third party delivery of relatively low value goods such as flowers is appropriate.)
- Insist that goods may only be delivered to the cardholder's permanent address. If you agree to send goods to a different address, take extra care and always keep a written record of the delivery address with your copy of the transaction details.
- Don't send goods to hotels or other temporary accommodation. Only send goods by registered post or a reputable courier and insist on a signed and dated delivery note.
- Be wary of sending goods abroad that may be readily available in the buyer's local market.

Couriers should be instructed:

- To make sure the goods are delivered to the specified address and not given to someone who 'just happens to be waiting outside'.
- To return with the goods if they are unable to effect delivery to the agreed person/address.
- Not to deliver to an address which is obviously vacant.
- To obtain signed proof of delivery, preferably the cardholder's signature.

Counterfeit cards

Chip and PIN cards have reduced this type of fraud as most cases of counterfeit fraud involve 'skimming' or 'cloning'. This is where the genuine data in the magnetic stripe on one card is electronically copied onto another card without the legitimate cardholder's knowledge. This type of fraud can be identified by checking that the card number printed on the voucher is the same as that embossed on the front of the card. If these numbers differ, call the Authorisation Centre immediately on **01268 822 822** stating "This is a Code 10 authorisation".

To help avoid receiving chargebacks as a result of counterfeit fraud and disputed key entered transactions, follow the 'Failed Card Swipe' Procedure, see Section 9, Exceptions.

Card Not Present (CNP) fraud

Card Not Present fraud occurs when fraudulently obtained card details are used to order goods by telephone, mail order or electronically such as over the Internet.

If the goods that you sell can be easily resold such as computers, TV and hi-fi equipment, you may be especially vulnerable to being targeted by fraudsters using fraudulent or stolen cards. You should be particularly suspicious of unusually high value or bulk purchase transactions from new customers.

The Card Security Code (CSC) and Address Verification Service (AVS) will help you decide whether to progress with a transaction. See Section 4, Accepting transactions, Card Not Present transactions. (Please do not use the Code 10 authorisation facility to undertake address checks.)

Important

Under no circumstances can goods purchased by mail or telephone be handed over the counter to, or collected by, the cardholder.

If a cardholder wishes to collect the goods, then they must attend your premises in person and produce their card. Any Sales Voucher already prepared must be destroyed and an over the counter transaction processed. If you have already completed a CNP order you must either cancel the transaction or perform a refund. If you perform a refund, please let the cardholder know that the original transaction, a refund and the over the counter transaction will all appear on their card statement.