

Card-not-Present (CNP) Transactions

fraud prevention guidelines for CNP retailers

IF IN DOUBT, CHECK IT OUT



telephone



Internet



mail order

© APACS (Administration) Ltd 2002

CW/037/002

05/02

Association for Payment Clearing Services

Mercury House, Triton Court

14 Finsbury Square

London, EC2A 1LQ

Telephone 020 7711 6356

Fax 020 7628 0927

E-mail cardwatch@apacs.org.uk

www.cardwatch.org.uk

www.apacs.org.uk



important note

These guidelines are produced by the Association for Payment Clearing Services (APACS) on behalf of its Members and in consultation with the British Retail Consortium.

For more copies of these guidelines and any operational queries relating to CNP transactions, please refer in the first instance to your acquiring bank (either directly or via your head office).

introduction

Card-not-present (CNP) transactions are those where neither the card nor its holder are present at the point of sale, e.g. orders by mail, telephone, fax or the Internet.

Some banks may require you to have a separate agreement for accepting these transactions.

These types of transactions are becoming increasingly popular with customers – unfortunately, they are also appealing to criminals. Because you have no opportunity to physically check the card or the identity of the cardholder, there is always some risk.

The fact that a transaction is authorised and an authorisation code is issued does not guarantee payment – it simply means that the card has not been reported lost or stolen and that there are sufficient funds in the account at the time of authorisation. It does not guarantee that the address given to you by the cardholder is correct. If the sale is fraudulent, the full amount may be charged back to you.

These guidelines, which incorporate new security measures, provide general advice in preventing this type of fraud and in assessing the risk involved in undertaking such transactions. However, they do not replace your own bank's operating instructions. Before you accept any CNP orders, make sure you are familiar with the procedures given to you by your bank (either direct or via your head office). If you have no written instructions, ask your bank or head office for a copy.

Here is a general guide to situations most at risk:

- retailers who don't take CNP transactions very often.
- purchases involving bulk buys or random items.
- purchases of highly desirable consumer goods or articles which are easily resold.
- transactions on cards issued overseas or where delivery is to an overseas address. Ask the cardholder to tell you the name of the bank issuing the card, and if it is not familiar to you, it may be an overseas bank. Contact the authorisation centre to see if they can validate the issuer details.
- where the delivery address is different from the cardholder's statement address.

This list is not exhaustive. However, if your transactions are in any of the above categories you might want to consider some of the extra security checks suggested in these guidelines.

new security measures

There are two new security measures to help fight CNP fraud which are available for retailers who use the automated electronic authorisation process. The aim is to provide retailers with additional information upon which they can assess whether to proceed with the transaction. The first is the **Card Security Code (CSC)**, which is a three digit number in reverse italics on the signature strip on the back of the card, printed directly after the card number, which can either be in full or the last four digits only (note that in the case of American Express cards, this code is a four digit number printed on the **front** of the card).

The other measure is the **Address Verification Service (AVS)** which allows you to check the numerical part of the cardholder's statement address and post code with the card issuing bank. At present these measures are only available for UK issued cards.

For more information about these systems, please contact your acquiring bank.

initial customer contact

If you are using an electronic terminal to complete a CNP transaction, you must obtain the following details from the cardholder whether the transaction is being made by Internet, phone or mail order:

- the card account number.
- the cardholder's name as it appears on the card.
- the card expiry date as it appears on the card.
- the cardholder's address for delivery of goods.
- the card issue number and card start date (if present).
- a contact phone number (preferably not a mobile number).
- the name of the bank, building society or other institution that issued the card.

If you are using the new automated electronic system these additional details should be obtained:

- the Card Security Code (CSC) as found on the card's signature strip.
- the cardholder's statement address, where different from the delivery address.

For telephone orders:

- record the time and date of your conversation.

For mail or fax orders:

- obtain a signature on the order form.

Always retain a copy of the written order, any proof of delivery and keep a note of the telephone conversation so that these can be checked in the event of any query.

Does your bank require you to record any other information?
If so add those points to the checklist.



authorisation

The fact that a transaction is authorised and a code is issued does not guarantee payment – it simply means that the card has not been reported lost or stolen and that there are sufficient funds available at the time of authorisation. It does not guarantee that the address given to you by the cardholder is correct or that the genuine cardholder actually placed the order.

Always call for voice authorisation (if your terminal has not itself sought authorisation) if:

- the sale equals or exceeds any CNP floor limit you may have. Remember, this is often lower than your normal floor limit.
- the card is the subject of a warning notice or is on a hot card file.

You should always call for authorisation if you are suspicious in any way.

Make sure that you check if your bank has a special telephone number for CNP transactions and if not:

- ensure that you tell the authorisation centre straight away that this is a CNP transaction.
- never allow a repeat delivery of goods without going through the authorisation procedure again.

security

For security and fraud prevention reasons you must not under any circumstances store Card Security Code (CSC) data. The code must be obtained each time a transaction is authorised.

other checks

There are other checks which you can make before delivery of the goods which may help to reduce the risk of serving a criminal and incurring a chargeback. Some suggestions include:

- For Switch card transactions a manual address and name check facility is available. Contact your acquiring bank for details.
- For business customers not known to you, if possible check their details in your local business directory or register.
- Personal customer address details can be checked in the Electoral Register; in the telephone directory; or from BT's CD ROM Phone Disc if you do not utilise the AVS check through the card issuer.
- Don't necessarily rely on the phone number you were given by the customer. Get the phone number for the cardholder's address through directory enquiries if possible, and phone the customer back on that number to confirm the order. Use the '1471' call back facility if available to verify the caller's phone number (and be wary if the caller's number has been suppressed). Consider a 'caller display' service.
- Check your records to see if you have had a number of transactions in a short period of time from a company or person with whom you have not had any previous dealings.
- Check if the delivery address has been used before with **different** card details.
- Be wary if the contact phone number is a mobile number (starting 07) – if so, ask for a land line phone number, if available, and use this to check the customer's name and address. Remember that criminals committing CNP fraud often use mobile phone numbers.

REMEMBER – IF IN DOUBT, CHECK IT OUT

delivery arrangements

Goods ordered by CNP transactions are usually delivered. But if the cardholder comes to collect the goods, they should be asked to produce the card used in the transaction. Such sales become 'cardholder present' and require a new voucher with the card details signed and checked in the usual manner, and any electronically processed transaction reversed. For how to reverse transactions, please refer to your own bank's instructions.

It is recommended that goods are not released to taxi drivers, chauffeurs, messengers or to any third parties such as 'friends' of the cardholder, as this type of delivery is considered high risk.

Be particularly wary of:

- the customer who demands next day delivery and shows no regard for any additional costs involved.
- alterations of delivery address at short notice.
- phone calls on the day of delivery asking what time the goods are due to be delivered.

You will help to reduce the risk if you:

- insist that goods are only delivered to the cardholder's permanent address. If you do agree to send goods to a different address, take extra care and always keep a detailed proof of delivery with your copy of the transaction details.
- try to avoid sending goods to hotels/guest houses. The incidence of fraud involving delivery to such places is extremely high, so be sure you are satisfied with all factors in the transaction.
- only send goods by registered or recorded post or by a reputable security carrier, and insist on a signed and dated delivery note.

Couriers should be instructed to:

- return with the goods, if unable to deliver them to the agreed address.
- always deliver goods into the specified address, or to someone who says they live at the address, ie. opens the door, and do not give goods to someone who just happens to be waiting outside.
- not deliver goods to an address that is obviously vacant.
- get signed proof of delivery.

If you have your own delivery service or trusted courier, consider introducing a procedure whereby the driver is issued with an imprinter and vouchers; is trained in acceptance procedures; and is instructed to hand over the goods only when the card is produced and the cardholder signs the voucher. If you tell the caller that this is your procedure, a criminal is likely to abort the call. Remember that not all types of cards can be used with a paper voucher.

Note that purchasing cards, which are issued to individuals in companies to make purchases on behalf of that company, may have special arrangements associated with the collection and delivery of goods. The acceptance of such cards is a matter for agreement with your bank.

documentation

Retain:

- all transaction details.
- documentary proof of delivery, wherever possible, with the cardholder's signature, for the period stipulated by your bank (directly or through your head office).

finally – some things to watch out for..

- Is the sale almost too easy? Is the customer disinterested in the prices or precise details of the goods, particularly if it is a new customer? Is the stock ordered all high value or easily re-sold merchandise?
- Is the sale excessive in comparison with your usual orders? Is the customer ordering lots of different items? Does it fit your 'average' customer?
- Do not accept orders from customers giving you a third party's card number, claiming to be acting on behalf of a 'client'.
- Be wary of someone quoting someone else's card details, e.g. a woman using her husband's card or a business using a personal card. It may well be a genuine call, but it pays to double check.
- Be wary if the customer offers two card numbers to cover one order – it could be a ruse to split the order to avoid authorisation. Never try to avoid authorisation yourself by splitting an order.
- Does the customer seem to lack knowledge of their account? e.g. '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 customer being prompted by a third party whilst on the telephone? Does the customer seem to have a problem remembering their home address or phone number? Does the customer sound as if they are referring to notes?

If you are successful in deterring a criminal, and you have any details from the aborted transaction, contact your bank and let them know. You may also wish to contact the police to advise them of any potential or actual fraud. You may help to prevent the criminal from trying the same trick with another retailer.

CNP checklist



telephone



Internet



mail order

during the initial customer contact you should obtain the

card account number
name as it appears on the card
card expiry date
cardholder's address for delivery of goods
card issue number and start date (if present)
phone number
name of the card issuer
card security code (CSC)
address verification details (AVS) if applicable
cardholder's statement address and postcode, where different from the delivery address

Time & date

Is there a signature on the form?

seek authorisation when

the amount is equal to or above the agreed CNP floor limit
the card is on a hot file or warning list
the purchase is of currency/travellers cheques/open airline tickets/gift vouchers (obtain Card Security Code (CSC) every time an authorisation is requested)

if you are suspicious... make other checks

use the local business directory or electoral register
use directory enquiries or 'call back' (1471) to phone the customer to confirm order
check if there have recently been frequent transactions from a previously unknown company or person
be cautious if the cardholder uses the same address as in previous transactions but uses different card details
get a permanent phone number, not a mobile

delivery

if the cardholder collects, it becomes a cardholder present transaction
no third parties should collect goods, only the cardholder themselves
using a permanent address for delivery purposes reduces the risk of fraud
use registered post or a reputable carrier for delivery
get a signed record of delivery
deliver into the address, do not hand over the goods outside
do not deliver to a vacant address
delivery driver should obtain an imprint of the card and signature
avoid next day delivery