



be prepared

A guide to preventing chargebacks on
card not present transactions

trade more securely

Trading over the phone, online or by mail order can be great for business but it's important to adopt the necessary processes to help safeguard your business against fraud-related chargebacks.

This guide contains useful information and tips to help you protect your business when accepting card not present transactions. It also explains what to do if you receive a chargeback and tells you what information we'll need from you to enable us to defend you against it.

What is a card not present transaction?

A card not present (CNP) transaction is where a purchase is made and the cardholder isn't present at the point-of-sale. These can be purchases made via the phone, internet or mail order.

As the card isn't present, the usual checks can't be carried out, which can lead to fraud. It's worth remembering that although a transaction may be authorised, this does not guarantee Payment – it simply confirms that the card hasn't been reported as lost or stolen and there is enough money in the account to make the Payment.

card not present chargebacks

A card not present chargeback happens when the genuine cardholder claims they didn't take part in or authorise a transaction.

A cardholder has 120 days from the date the transaction is processed to their account to dispute it with their card issuer as unauthorised or fraudulent.

We can attempt to defend the transaction if you can provide:

- evidence that a refund has been processed
- evidence that the customer has ordered goods from you previously that haven't been disputed
- a written and signed order form and the signature matches that of the cardholder. However, we can't guarantee that we'll be successful in defending you in these circumstances.



useful tips for spotting fraud

One of the best ways to prevent chargebacks is to keep an eye out for fraud. Consider the following points before taking a card not present Payment:

- is the sale too easy? Is the customer uninterested in the price or details of the goods?
- are the goods of high value or easily resaleable?
- is the sale excessively high in comparison with your usual orders? Is the customer ordering many different items?
- is the customer providing details of someone else's card claiming it's the card of a family member or friend?
- is the customer claiming to be paying for goods or services for a third party and that the other party or a taxi will collect the goods or partake of the services?
- does the address seem suspicious? Has the address been used before with different customer details?
- is the customer being prompted by a third party while on the phone?
- is the customer attempting to use more than one card in order to split the cost of the order? Do cards fail to authorise and does the customer keep providing details of alternative cards?

What to do if you're suspicious

If you feel suspicious, ask the cardholder to fax or post written authority to charge their card account together with identification that shows their name and address. You can then make sure the card account address matches the delivery address and also check the telephone code of the fax against the area code of the address.

Doing this won't guarantee against fraud, but a fraudster probably won't be able, or willing, to provide the documentation you ask for.

tips on receiving and delivering orders

These points may also help protect your business from fraud and chargebacks.

- Always use a reputable carrier who can provide proof of delivery.
- Be wary of urgent orders, particularly to an address where the recipient can't be identified as the cardholder – such as a doorman at a block of flats. A fraudster may have temporary access to a delivery address.
- Be cautious of customers who change the delivery address at the last minute.
- Be very cautious if the customer decides that they want to collect the goods. In this circumstance you should refund the original transaction and start a new one as an over the counter sale, making sure that you follow card present Chip & PIN procedures. And remember to check that the card number printed on the receipt matches the number on the card.
- Never release goods to a third party (such as a taxi driver or courier) who claims they were sent by the cardholder. Whenever the goods are released to someone other than the cardholder, the risk of a chargeback is increased.
- Question orders from overseas, especially if you only advertise in the UK.
- Question orders where the cost of delivery is high due to the location, especially if the goods could be purchased closer to the cardholder's address.
- Beware of large orders – especially if they're from new customers.
- Monitor orders by checking the value and volume of those for the same customer or card. Be especially aware of multiple orders, orders that increase in value over a short space of time and multiple orders using different cards.
- Beware of customers who want services such as holidays, event tickets and party functions at short notice.

reason codes and how they can be defended

If you do find you receive a chargeback, we may be able to defend you against it if you can provide us with the appropriate evidence. The card issuer will specify a reason code, which will identify what evidence is required.

Reason code Visa 83, MasterCard 37 or Maestro 37

These codes mean the cardholder denies participating in or authorising a transaction that's been processed to their account.

To defend you, we'll need evidence that the genuine cardholder has authorised the Payment and participated in the transaction. You'll need to send us any of the following:

- evidence that the cardholder, with the same name and address, has purchased goods or services from you previously that haven't been disputed
- details of the cardholder's authority or an order which bears the cardholder's signature and shows the correct details of the cardholder's card
- details of a refund processed to the cardholder's account (do not refund your customer after a chargeback notification).

* We can't guarantee that we'll be successful in defending a chargeback with this evidence.

Reason code Visa 75 or MasterCard 63

These codes mean that the cardholder doesn't recognise all or part of the transaction details.

To defend you, we'll need evidence of all details of the transaction to help the cardholder to recognise it. Any of the following would help:

- the name of the customer
- any other customer details
- details of the goods or services that have been provided
- the date the goods or services were provided
- your outlet name if it's different to what's on the customer's statement
- details of a refund processed to the cardholder's account (do not refund your customer after a chargeback notification).

Please be aware that if the cardholder still disputes the transaction after reviewing your reply, this will result in a fraud-related chargeback that can't be defended.

statement narrative

Sometimes chargebacks happen because the cardholder doesn't recognise the details on their statement, even though they made the transaction.

It's essential that the information that appears on the statement narrative (this is the information that appears on the cardholder statement) is accurate.

Our recommendations

We recommend that if your company operates using several trading names that each one has a separate merchant number. This will ensure that your customers statement details a business name they are more likely to recognise and connect back to the order placed.

We strongly recommend that any merchant who accepts card not present transactions via the telephone or by mail order, makes sure that their contact telephone number appears on the second line of the statement narrative. If you're processing Payments through the internet, we suggest that the website address shows in this field.

If the cardholder can resolve any uncertainty directly with you as a company, this may prevent the customer raising a chargeback with their card issuer, saving you time and money.

However, we do understand that some businesses don't want their company name to appear on their customer's statements, due to the nature of their business, or for privacy. If this is the case, please make sure that your customer is clear what name they should expect to see on their statement.

How to change your details

If you'd like to change your statement narrative details, simply call us on **0844 811 6666.***

Card Security Code and Address Verification Service

The Card Security Code (CSC) and the Address Verification Service (AVS) were developed by the UK card industry to help businesses fight card not present fraud.

If both the CSC and AVS checks are verified, you can be more confident that, not only is the cardholder using a valid card, they're also a valid user. If the cardholder can't provide a CSC or the one provided doesn't match, we advise that you don't continue with the sale.

How do they work?

CSC and AVS both work by electronically checking the security code on the reverse of the card and making sure that the address details given to you match the information held by the company that issued the card.

CSC

The CSC only appears on the genuine card – it can't be taken from till receipts.

When you enter the CSC that the person making the transaction has given you into your terminal while processing the transaction, it's sent to the Card Issuing Company as part of the authorisation request.

The card issuing company will check the information you provide against their own records and send a response indicating whether the data has been checked and if so whether it matched their records.

AVS

You can enter the numbers of the postcode you've been given into your terminal (up to five digits), for example:

- postcode: NN16 3SH
- numbers to be entered = 163.

You can also enter numbers from the rest of the address into your terminal (up to five digits), for example:

- address:
Flat 5a
Redfield House
29 High Street
- numbers to be entered = 529.

If the cardholder's address contains more than five digits, only the first five should be used. The address details that the customer must use are those to where their card statement is sent, not those to where the goods are to be delivered, as this may be different.

If the address doesn't have a number, for example it simply contains a house name, such as "Rose Cottage", you should only enter the numbers in the postcode.

Important points to remember

The company that issued the card is responsible for carrying out the CSC and AVS checks and the subsequent responses. We won't be able to advise on the reasons for any decisions given.

You should never store the CSC or AVS data in any circumstances. This information needs to be obtained from the cardholder for each transaction.

If you're setting up a recurring transaction where you're using the same card details on a regular basis, you'll only need to take CSC or AVS information when setting up the Payments.

Please note, it's your decision whether or not to proceed with the sale after you've received a response from the Card Issuing Company. And while these services are designed to give valuable additional checks to our merchants, they're not an absolute guarantee of Payment and you may still incur chargebacks.

trade safely online with ePDQ

ePDQ

ePDQ is a secure online service available from Barclaycard Payment Acceptance for card Payment authorisation and settlement. Featuring in-built velocity checking, with parameters you can determine, it enables you to set the fraud screening options – and accept and process card transactions from your website 24 hours a day, 365 days a year.

ePDQ-lite

ePDQ-lite, also from Barclaycard Payment Acceptance, is the virtual PDQ – an online card Payment authorisation and settlement service that can be accessed from any PC and can provide your company with quick, easy and secure transaction processing, wherever your customers are.

ePDQ-lite has been designed to support your business in processing card not present transactions, including those made by mail order or by telephone. It carries out the CSC/AVS checking and also other fraud screening checks as standard.

3D Secure Authentication

3D Secure Authentication shifts the liability for fraud from the merchant to the Card Issuer, providing the correct responses are received.

This tool does not shift the liability for chargebacks unless they are due to fraud, so chargebacks are still valid for reasons such as non-delivery of goods, duplicated processing or no authorisation.

Want to know more?

For further information, just call our Customer Contact Centre on **0844 811 6666*** or visit our website **www.barclaycard.co.uk/business/accepting-payments**

You can also find out more about ePDQ by calling our helpline on **0844 822 2099.***

need further help?

This guide is just one in the series we've developed to help you better understand what chargebacks are, why they occur and what you can do to reduce their impact on your business. More detailed guides are available.


Other guides available include:

- **"strength through knowledge"** – Your introduction to chargebacks and retrievals
- **"don't lose out"** – A guide to preventing chargebacks on card present transactions
- A series of sector specific guides on best practice for avoiding chargebacks, including codes and defences, for:
 - **Airline**
 - **Car rental**
 - **Hotel**
 - **Card not present gaming.**

Together we can help your business build stronger defences.

Contact our dedicated Chargeback team on
01604 614 012*

[www.barclaycard.co.uk/business/
existing-customers/chargebacks](http://www.barclaycard.co.uk/business/existing-customers/chargebacks)



Please ensure that all card data is protected in accordance with the Payment Card Industry Data Security Standard (PCI DSS). For further information see: www.barclaycard.co.uk/pcidss or www.pcisecuritystandards.org

This document is available in large print, Braille and audio by calling **0844 811 6666**.*

*Calls may be monitored and/or recorded to maintain high levels of security and quality of service. Calls to 0844 numbers will cost no more than 5.5p per minute, minimum call charge 6p (current at December 2011). The price on non-BT phone lines may be different.

Barclaycard is a trading name of Barclays Bank PLC. Barclays Bank PLC is authorised and regulated by the Financial Services Authority. Registered in England. Registered No. 1026167.
Registered Office: 1 Churchill Place, London E14 5HP.
BCD111605BROB3. Updated: 12/11. 23714BD