barclaycard
Start today

Procedure Guide

For a smoother operation

Welcome to Barclaycard Business Payment Solutions

This procedure guide includes all the information your business needs to accept card payments. It forms part of the Terms and Conditions and your Additional Service Conditions.

Inside you'll find what you need to get started, along with information on some of the risks of accepting card payments – and how you can keep your business as safe as possible.

This guide is part of your Agreement with us

So please keep it in a safe place – and in easy reach of your employees (but not your customers).

It sets out a number of your responsibilities under the contracts with Barclaycard in order to illustrate to you how to meet these requirements, for a full list of your duties required under the contract please consult your terms and conditions.

Your Barclaycard merchant number

Whenever you get in touch with us, it's helpful to have your merchant number ready. If you rent a terminal from us, you will find the merchant number on the front screen. Alternatively, it will be on any Invoice/Statement we send you. Make a note of it below:

Let us know if your business changes

To make sure you receive the right services for your business, please call us on **0844 811 6666** if any of these changes take place:

- an alteration to the type of business or the goods or services you provide since you signed your Merchant Agreement
- you start to use other channels (e.g online or mail order)
- you change the name of your business
- you sell your business or change its legal entity (e.g if you change from a sole trader to a limited company)
- there's a significant change in the shareholding of your company
- you stop trading
- your business begins any insolvency procedure
- you change any of your business details, like your address or contact details

It's really important that you keep your contact details up to date, otherwise we can't get in touch when we need to.

Stay protected from fraudsters

We'll never email you asking for you to confirm any card payment or transaction details. If you do get an email asking for this that looks like it's from us, you shouldn't respond.

Instead you'll need to let us know so we can look into this for you. To do this:

- open a new email and attach the fake 'phishing' email – make sure you don't forward it, as this potentially loses important information
- then send your email to **internetsecurity@barclays.com**. Use this email address to report any of these instances

And be careful of third-party processing

If you're ever asked to buy card transactions or process another business' transactions, please call us on **0844 811 1981**. That's known as transaction laundering and would break the terms of your agreement.

Contents

Payment acceptance

We can help you to accept payments from your customers in various places and using a number of different payment methods. But to make things simple, we're going to explain the two main types of card payments:

- **Card Present (CP)** – this is when the cardholder is in front of you and has their card with them. You'll take the payment then and there by either taking a Chip and PIN payment, swiping the card or using contactless
- **Card Not Present (CNP)** – this is where the cardholder and their card are someplace else. Like if you're taking payments over the internet, by phone, by mail order or if it's a recurring transaction

We've explained which types of transactions you can take in your agreement with us – so tell us if you want to start taking any other types.

Accepting Card Present transactions

To accept Card Present transactions you'll need to use Barclaycard and card scheme approved processing equipment – either from us, from another supplier or your own. Just make sure your device can accept magnetic strip, Chip and PIN or signature and contactless payments.

Using Barclaycard processing equipment

As well as reading this guide, you'll need to make sure you and your staff read through the the 'Read me first' and 'Read me next' guides that came with your terminal. This includes important safety information about the equipment and how to use it – including keeping liquids away from it at all times. Take a look at **barclaycard.co.uk**

You'll also need to meet the Payment Card Industry Data Security Standard (PCI DSS), there's more on that on page 21.

If your device is damaged and needs to be repaired, please let us know so we can get this sorted for you Just bear in mind that if the damage is your fault, we might charge you to replace it.

Using your own processing equipment (or another supplier's)

If you don't use Barclaycard processing equipment, we'll need to test your processing equipment and approve it before you can take live transactions. Give us a call on **0844 811 6666**.

You'll also need to regularly carry out 'asset management'. That's where you record all stock and serial numbers, the location and the basic electronic and physical identification you use to authenticate your equipment.

It's up to you to make sure your supplier keeps to the PCI DSS and for making sure the equipment is up to industry standards. If you don't do this, you might end up breaking card scheme rules and have to pay fines as a result.

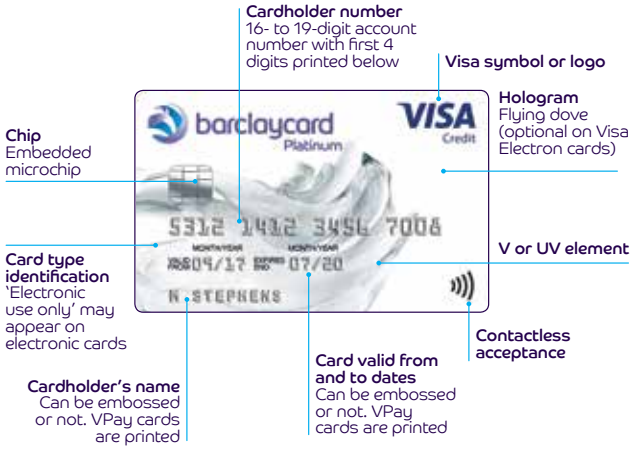
The different plastic card designs

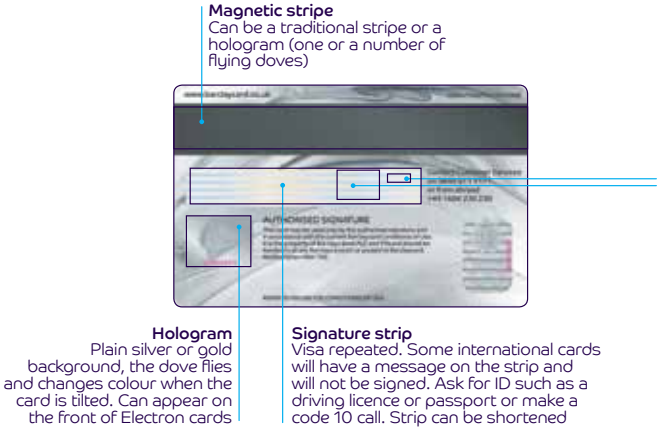
There are many different credit and debit card designs – but they all share some common features (like a card number, chip etc). It's important that you look for these to make sure you don't accept fraudulent cards.

Most of the time the cardholder will insert their card into the device themselves. But if you do handle the card you should complete visual checks yourself. Take a look over the page for some things to look out for.

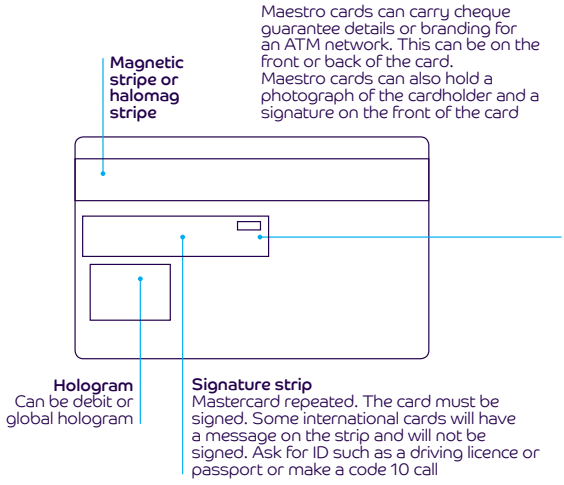
We've explained some of the common features of each card over the next few pages so you know what to look out for.

Visa

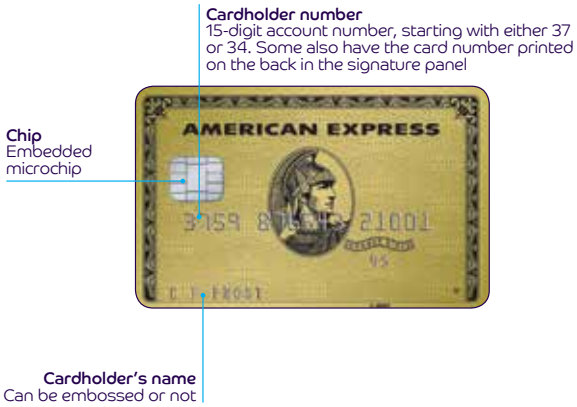




Mastercard



American Express



Don't accept a card outside the valid date range shown on the front.

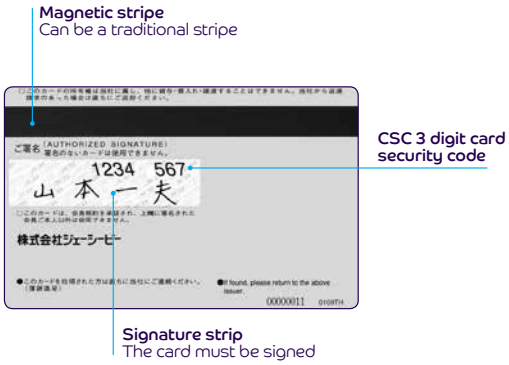
The four-digit CID number is on the front of the card, usually above the card number, either on the right or the left edge of the card.

The three-digit CSC is on the back of the card, usually above the card number, either on the right or the left edge of the card.

Some (but not all) American Express cards have a holographic image. This can be on the front or back of the card.

The card must be signed – and the signature must match the cardmember's signature on the charge record. The name must also be the same as the one that appears on the front of the card.

JCB



Accepting contactless payments

A contactless payment is processed using near field communications (NFC) technology. That's where the payment instructions are shared securely between a contactless card (or other device) and processing equipment that has contactless technology enabled. Contactless readers can be part of your processing equipment or they can be separate. And you can also carry out a contactless refund up to the current limit if you need to.

You can recognise contactless cards as they'll have this little symbol on them: 

Accepting American Express

If you have chosen to process American Express payments you will have a specific American Express merchant number as you will have entered into a separate contract with American Express Payment Services Limited. This doesn't change or replace the Agreement you have in place with Barclaycard. American Express will manage and operate your account and pay for the transactions you accept. Should you have any queries on how to handle American Express transactions, or billing, settlement, or general queries please contact American Express on **0800 032 7216**

Visual checks when accepting cards

Although most transactions are contactless or by Chip and PIN, if you do handle a card, please follow these quick visual checks:

- make sure the card is valid and in date
- check that no part of the card has been damaged or tampered with
- rub your thumb over the signature strip (it should be smooth and level with the surface of the card)
- if the cardholder needs to sign the transaction receipt, check that their signature matches the one on their card
- check that the spelling of their signature (if you can read it), matches with the name on their card
- check the hologram moves when you tilt the card back and forth – counterfeit cards use poor reproductions, so it should be easy to spot a fake at a glance

Accepting co-badged cards

Where you're presented with a co-badged card (a card that's aligned to more than one card scheme), you must allow the cardholder to choose which card scheme they'd like to pay through – providing you accept that scheme. There aren't many co-badged cards currently available in Europe, but this could change in the future. Our terminals support the acceptance of co-badged cards but if you have your own terminal or hire one from elsewhere you should contact your supplier to ensure that your terminal can support these cards and enable customer choice. In addition if your own terminal offers you the ability to prioritise a particular payment scheme, then you can do this providing it lets a co-badged cardholder override this with their chosen scheme.

Choose the card categories you'd like to accept

You can choose the EU card categories you wish to accept within a scheme. Card categories are defined as consumer debit, consumer pre-paid, consumer credit and commercial. For example, you can decide to accept debit, prepaid and credit cards, but not commercial cards. Once you accept one consumer card within a particular category and card scheme, you will need to accept all cards within that same category and card scheme. For example, if you accept any Visa consumer credit card, you must accept all Visa consumer credit cards. This change only applies to cards issued in the EU. If you decide to accept any non-EU issued card within a scheme, then you must accept all card products within your chosen card scheme that are issued outside the EU. If you do choose to only accept certain types of cards, then you'll need to display this clearly at your point of sale and on your website.

Accepting different cards

Accepting cards with a chip

Most cards will come with a chip, but bear in mind that some cards might not.

- To make a payment, the cardholder should insert their card into the card reader
- If your terminal can't read the chip, you're allowed one level of 'fall-back' and can process the transaction by swiping the magnetic stripe through your device (more on that below)

You'll also need to get authorisation at the time of processing the transaction. This isn't a guarantee of payment but it does confirm that the cardholder has enough funds for the transaction – and checks that the card hasn't already been reported as lost or stolen.

If the genuine cardholder disputes the transaction (and you haven't completed the correct authorisation process), you may be liable for any chargeback.

Accepting cards without a chip

If a customer has a card without a chip, you'll need to swipe the card through the magnetic stripe reader on your device. You'll also need to get online authorisation so make sure your processing equipment has online access.

If your terminal can't read the magnetic stripe, ask the customer for another form of payment. If they don't have any, you can process this as 'a key entered transaction' (see page 8 for more info).

But be aware that this increases your chance of processing a fraudulent transaction and receiving a chargeback claim see page 19 for more on this.

To make a contactless payment

- Your customer needs to place their contactless card or device over the reader
- They don't need to enter their PIN unless it's for a high-value payment (HVP)
- Your reader will go online to check that funds are available
- The customer might be told to complete the transaction using Chip and PIN instead – this is just a security check
- And if the contactless payment fails, try again with a Chip and PIN or by swiping the card

Does your customer need a receipt? Your terminal only usually prints a merchant receipt for contactless payments. Take a look at your Terminal Operating Guide for info on how to print a copy for your customer.

Accepting high-value payments (HVP)

If we provide your payment acceptance terminals, your device will already be set up to receive HVPs. If your payment processing equipment is from another supplier, please check with them to get this set up. These are most likely to be made using a mobile phone and will need the customer to use a PIN or some other method to confirm that they're who they say they are.

Key entered transactions

If you can't swipe your customer's magnetic stripe card – you'll need to enter the transaction using the keys whilst your customer is in front of you (except for Maestro cards where, electronic key entry is only permitted for refund transactions). Make sure your equipment goes online so you can get the right authorisation.

There are also a few other steps you need to take:

- take an imprint of the card using your manual imprinter – this is to prove you saw the card and helps if the card issuer raises any chargeback claims
- fill in the voucher details in full and ask the cardholder to sign the paper voucher
- you'll automatically be credited for transactions made using the keys, so you don't need to send the paper voucher for processing – but do make sure you keep the vouchers and processing equipment receipts for 13 months. If you don't, you might be liable for chargebacks

Please note that the manual completion of a transaction does not provide sufficient proof of card presence in a fraud-related dispute. Unfortunately, you can't enter transactions using the keys for unembossed cards. So you might have to ask your customer for another way to pay.

Something not working? If the transaction fails, call for authorisation on **0844 822 2000**. If you're suspicious of the transaction, make sure you let us know it's a 'Code-10 call'. This may help protect you from chargebacks.

Verifying Card Present payments

Using Chip and PIN

Usually when there's a card with a chip, there's a PIN (Personal Identification Number). Your customer needs to enter this to confirm the transaction and your terminal will go online and seek authorisation.

A person with disabilities may not be able to enter a PIN – you should follow terminal prompts. Additionally, under the Disability Discrimination Act (1995), you must allow them to pay using a different method.

If the authorisation is declined, don't go ahead with the transaction – as we won't be able to help if there's a chargeback claim later on. Instead, ask your customer to pay another way (but not by swiping the card or by using the keys of the declined card).

Using a signature

If the terminal doesn't prompt the customer for a PIN, you can use their signature to confirm they're who they say they are – remember that a non-secure fee may be levied. If a customer cannot remember their PIN, the transaction should not be completed. Remember to carry out visual checks on the card.

Authorisations

Every Card Present transaction needs to be authorised at the time of the transaction. For hotels and and vehicle rental, please refer to the sector-specific sections.

Complete your authorisation either online through your processing equipment or by calling **0844 822 2000**.

Voice authorisation

Most of the time, your processing equipment will automatically communicate with the card issuer for an authorisation. But sometimes you might need to call for a voice authorisation. **Only accept an authorisation code from a confirmed Barclaycard source, do not accept a code from the cardholder**.

You should do this if:

- your device asks you to
- the transaction's more than your floor limit
- you're suspicious about the card or cardholder (see Code-10 procedure below)
- you have to use a fall-back voucher because of a fault with your Barclaycard equipment

By calling for voice authorisation, you're asking us to check that the cardholder has enough funds on their account and that the card hasn't been reported as lost or stolen. This is an Automated Voice Response service – you will need your Merchant ID, card number, expiry date, payment amount and currency to the nearest whole amount (for example, if the amount is £89.76, you should state 'ninety pounds'). **Just remember that a voice authorisation can't confirm the cardholder's identity or guarantee their payment**.

If you need to change the amount of the transaction after you've authorised it, cancel the original amount and get a new authorisation. This makes sure the right amount is taken from the cardholder's account.

Code-10 calls

If you or your staff are ever suspicious of the card or suspicious of the cardholder, it's important that you call for authorisation.

Call us on **0844 822 2000**. Remember, that a Code-10 call can only happen if the cardholder is present – so you can't call about mail, phone or online transactions.

When you call the Automated Voice Response service:

- provide your Merchant ID and when prompted on the transaction menu state Code 10 call
- you'll then need to give the card number, expiry date and issue number (if they have one). Next, you'll have to choose from the options given depending on the type of call you're making
- you'll then be connected to an operator – answer their questions with a yes or a no
- remember to keep the card and the goods out of reach from the customer
- and if you have surveillance equipment, make sure it's on and positioned at the point of sale equipment

If the operator asks you to keep the card, tell the customer politely and explain what happens next but never put yourself or any member of your staff at risk.

Referrals

Sometimes, the card issuer might ask for a referral before they approve the transaction. If this happens, your processing equipment will tell you to call for authorisation. Note that Visa does not support referrals.

In most cases you'll need to give the phone to the cardholder so they can answer some questions asked by their card issuer.

After we've spoken to the card issuer, we'll let you know what the decision is. You must have the final discussion with us. **Do not key any authorisation number given by the cardholder and do not allow the cardholder to key any data. If this happens, you may be liable for a chargeback and we are unable to defend your claim**.

Split sales

If the customer wants to split the payments across different cards, or a combination of a card, cash or cheque, it's called a split sale. These usually happen if the customer is making a high-value transaction and doesn't have enough credit on one card.

You should only accept a split sale if:

- the customer has their card with them in front of you (we'd strongly recommend not splitting sales for any phone, telephone or online transactions – as you're more at risk of chargeback claims)
- each transaction is authorised (no matter what floor limits you have)
- the cardholder clearly agrees to how much is being charged to each card and is given receipts

If the authorisation is declined, don't split the transaction into smaller amounts to try and authorise it. This could result in chargeback claims being made against you.

If multiple cardholders ask you to split one transaction (like at a restaurant)

- Just make sure you agree the amount that each cardholder will pay before you process each transaction
- Ask every cardholder to enter their PIN or give their signature
- And give each cardholder a copy of the transaction receipt (which might include any tips they've agreed to pay)

If one cardholder asks you to split a transaction across different cards

- Just make sure each card has the same cardholder name on and carry out visual checks
- And don't go ahead with the transaction if you're ever suspicious of it or the cardholder

If one cardholder asks you to split a transaction across a card and cheque

- Make sure the cheque and card have the same cardholder name

Exchanges

If your customer wants to exchange their items for something else, there are three different steps you can take. Just remember that you can only put a refund back on a card, you can't give the customer cash or a cheque.

- If they exchange a purchase for goods of the same value – you don't need to do anything (but it all depends on the individual procedures you have in place for your business)
- If they exchange a purchase for goods of lower value – you'll need to refund the customer the difference. Just make sure you do this on the same day and process the refund on the same card that they originally paid with. If they've lost that card, you can refund them to a different card. But if they've closed their account you'll need to refund the card number they used originally
- If they exchange a purchase for goods of higher value – carry out a sale for the difference in cost. You'll need to get authorisation, even if the amount is below your floor limit

Processing a fall-back paper voucher

It's unlikely – but if your Barclaycard processing equipment ever fails, you can use the manual imprinter we gave you to take certain payments. It goes without saying, but make sure you report any faults so we can get you back up and running. Call us on **0844 811 6666 option 1** or your supplier if you don't use equipment from us.

You should only use these fall-back paper vouchers in exceptional circumstances, like if your phone line or your device is faulty. You'll need to make sure you get voice authorisation for each transaction you make – but bear in mind that this won't guarantee a payment or that the cardholder is who they say they are. The card issuer can still raise a chargeback claim against you – even more so if you haven't followed the right processes. If something doesn't seem right about the transaction, please follow the 'Code-10' call process. You can't process unembossed cards with paper vouchers.

Here's what you need to do

1. Carry out all the normal card checks – you'll find these on page 7
2. Place the card face up on the imprinter ❶
3. Place the sales voucher ❷ face up over the card ❸ and use the imprinter ❹
4. Remove both from the imprinter and fill out the sales voucher with the following info (use a ballpoint pen and write as clearly as possible):
   - the date
   - the amount of each item
   - the transaction total (you must not split a sale – split sales are at your own risk and could be charged back)
   - details of what was bought. Please do not just write 'Goods' as this is not acceptable
5. If you're selling fuel, only fill out the 'For Merchant Use Only' boxes to record the vehicle registration number
6. Once everything's filled in, ask the cardholder to sign the sales voucher. You should hold the card and watch whilst they're doing this
7. Check that the signature matches the signature on their card and that the name is the same. You should also check the signature on the card hasn't been tampered with
8. Next, you'll need to get voice authorisation. Call **0844 822 2000** and ask for standard authorisation
9. You may need to follow some extra steps given by the operator you're speaking to, including passing the phone to the customer
10. **If the transaction isn't authorised** – no reason will be given, so you'll need to give the card back to the customer and ask them for another form of payment
11. **If the transaction is authorised** – write the authorisation code you're given on the sales voucher. Tear off the cardholder copy and give it to the customer, along with their goods. Remember only use the authorisation code given by ourselves, do not use any codes provided by the cardholder or a third party
12. **Keep the sales voucher in a safe place in case you need it.** Don't bank the voucher as your processing equipment will credit the amount to your bank account
13. Finally, once your device is up and running again, key in the transaction number. If you're using Barclaycard processing equipment, do this as a forced sale (select this from the Transaction Menu). This will prevent a second authorisation code from being given or the transaction being refused
14. If you can't enter the transaction using the keys, fill in the sales voucher and send it for processing (take a look at the 'Sales and refund vouchers' section). We'll accept the transaction as long as you've used the right authorisation and followed all the steps needed

And that's that. Remember, we can't accept altered vouchers. So if you make a mistake, destroy the sales voucher and start again. You should also never pin, staple, fold or damage vouchers as we might not be able to process them.

If you can't read a card

If you have chip-enabled processing equipment, you should usually have no problem reading the chip. But if you do – you're allowed one level of fall-back. Just bear in mind that sometimes the card issuer might refuse the transaction if you try to enter the details using the keys or magnetic stripe. If that happens, just follow the processing equipment prompts. That might involve speaking to our authorisation department. And only give the card back to the customer if you're not asked to keep it.

Whilst entering details using the keys or magnetic stripe can help you to process the transaction, it does mean you'll be skipping a number of very important security checks. Some fraudsters are aware of this and are taking advantage of the opportunities.

Important steps to keep your business safe

To protect your business from losses and reduce the risk of chargebacks, make sure you follow the below steps whenever your device can't process a transaction in the usual way.

- Enter the card number using the keys (more on this on page 8)
- Imprint a sales voucher and complete it in full (including details of the goods or services bought), write the words 'For verification only – this voucher is not for banking' on it and ask the customer to sign it (see page 10 for how to fill this in)

Card imprinter

Sales voucher

Banking procedures

It's as simple as this – to make sure you get paid for all transactions, follow the end-of-day banking procedure.

This means sending all transactions within two working days of being accepted. You can find more about this in your Terminal Operating Guide.

If you send a transaction later than two working days – the transaction might be rejected and charged back to you. And if that happens, we can't defend you from these chargebacks.

If your processing equipment isn't working, make sure you follow the steps on page 10 so you can still receive payment.

If you can't process a sales voucher, complete the three-part merchant voucher summary (MVS) and then send your bank copies of your sales and refund vouchers to the address referenced below. Just make sure that there are no more than 20 vouchers per MVS.

Sales and refund vouchers

When you use sale or refund vouchers, there'll be three copies:

- **a merchant copy** (on the top) – this is for you to keep
- **a bank processing copy** (the middle one) – you'll need to send this immediately so it can be processed within two working days
- **a cardholder copy** (the bottom one) – last but not least, give this to the cardholder for their records. Or if it's a phone or online order, post it to them
- make sure you don't bank the sales voucher as this will cause the transaction to go through twice. The voucher is just to show that the card was present and to prove the transaction was valid if there's any dispute
- keep a merchant copy of the receipt and the sales voucher – if you don't keep hold of these, you could suffer losses if there's a chargeback claim

A few exceptions

You can't process unembossed cards with paper vouchers:

And you can't take an imprint of any printed cards. So if your device can't read any of these cards, ask your customer for another form of payment as you won't be protected from chargebacks with an imprint.

How to complete your merchant voucher summary (MVS)

1. Write your merchant name and number on the MVS (this is usually on the top line of your imprinter plate), along with the paying-in date
2. List the value of each voucher on the back of the MVS in the boxes shown
3. Write the total number and value of both vouchers on the front
4. And then if possible, post these vouchers on the same day – or at least within the next two working days

Send your MVS to the below address for Processing:

MVP
51 Saffron Road
South Wigston
Leicester
LE18 4US

And that's that. As always, if you've got any questions about this just get in touch and give us a call on 0844 811 6666 (option 1)

How to spot and stop fraudulent Card Present transactions

We've mentioned it earlier in this guide, but it's worth repeating: taking Chip and PIN payments will help prevent you being charged back for any transactions the authorised cardholder claims they did not participate in.

If your customer doesn't have a chip-card, you're at higher risk of accepting a fraudulent transaction. So you always need to get authorisation and complete the below checks:

- keep hold of the card at all times (try and just touch the edges)
- keep the goods out of reach of the customer
- check the 'valid from' date. If the card is newly issued, be extra careful
- watch out if the customer hesitates with their signature – and make sure it matches the signature and name on their card
- stay alert – fraudsters might try to hurry or distract you when they're paying
- don't process transactions on anyone else's behalf. This would break your Merchant Agreement and could lead to chargebacks
- if your customer can't remember their PIN, make sure you ask for another form of payment

Contactless payments work a bit differently – as you don't need any verification (see page 8 for more on this).

Returning wanted or recovered cards

If we ever ask you to retain a customer's card and not return it to them, politely tell the customer what's happened. And then follow these steps:

- don't handle the card too much – you want to preserve fingerprints and other evidence, so try to hold it by the edges
- with the card facing you, cut off the bottom left hand corner only – keeping the signature strip, magnetic stripe, chip and hologram intact
- fill in the recovered-card form in your welcome pack – you'll need to keep the cut-off part of the slip in your files
- then send the top section of the form and both pieces of the card to: Recovered Card Services, Barclaycard Department RC, Northampton NN4 7SG
- If you're returning a Visa Electron card, you'll also need to include a copy of the processing equipment declined receipt

Need more recovered-card forms or have a question?
Call us on **0844 811 6666**.

Our returned card reward scheme

To say thanks for spotting and returning a wanted card, we might pay you a £50 reward. It's up to you whether to split the reward or pass it onto the staff member who actually recovered the card. Remember you are responsible for the tax treatment.

If the police want to keep a wanted card or sales voucher for investigation (like if a stolen card is presented), you'll need to keep certain details in case there are any further questions. Make sure you have a good copy of the sales voucher, as well as:

- the card number
- the expiry date
- the name embossed on the card
- the date the card was recovered
- the crime reference number
- details of the officer and police station dealing with the case

You can still claim the reward if the police take the card for evidence.

Accepting Card Not Present (CNP) transactions – by phone, online and mail order

Sometimes it's just not possible for the cardholder to be in front of you, like if you're taking payments online, over the phone or through mail order. **Whilst you can take Card Not Present transactions, it's important to understand that there are higher risks involved**.

When you accept these payments you'll need to get an authorisation and make a note of the following:

- the card number
- the card expiry date
- the cardholder's full name and address
- their postcode and phone number
- the delivery address and name of the person receiving the goods
- their signature (for mail order)
- the gross transaction amount (that means the total amount including postage, packaging, VAT etc)
- the card security code (CSC) (only for online transactions and mail order)

You must not store the card security code. This is part of the Payment Card Industry Security Standard.

If you'd like to accept online Maestro transactions, you'll need to enrol for Mastercard SecureCode™.

When dealing with CNP transactions, make sure you don't:

- give the goods to anyone who claims to be collecting them on the cardholder's behalf (like a taxi driver)
- let the cardholder pick up goods in person. If they pay online, or by mail order or phone (also known as MOTO) and come to collect the goods, you need to cancel the transaction and carry out a Card Present transaction instead

Authorisations

It's important to get an authorisation for all CNP transactions at the time the transaction takes place – either for the actual amount or as a pre-authorisation for the expected value (like a hotel or car hire bill). **Just remember that an authorisation only confirms there are enough funds in the account and that the card hasn't been reported as lost or stolen at that time.**

That means it doesn't guarantee payment or that the person paying is the genuine cardholder. So you're automatically more at risk of taking fraudulent transactions and seeing chargeback claims.

Shipping goods and providing services

The authorisation you need when shipping goods and providing services depends on the type of card you're using.

Visa transactions – can be authorised up to seven days before the transaction date (the day the goods are shipped or the services are provided).

This authorisation is still valid if the transaction is under 15% of the authorised amount, as long as the extra amount represents shipping costs.

Mastercard transactions – need an authorisation on the day the cardholder places the order. When the goods or services are ready to be delivered, you should then process the transaction (which can't be more than the original authorisation amount). Please note that a Mastercard final authorisation is only valid for 7 days, a preauthorisation is valid for 30 days for Mastercard and 7 days for Maestro.

Recurring transactions
If a cardholder gives you permission (in writing or electronically) to bill their account for goods or services you'll deliver over time, that's called a recurring transaction. Some common examples of this are subscriptions and memberships – as long as there are less than 365 days in between transactions.

You can't set up a recurring transaction for a Maestro card. When setting one up for other cards, make sure you include all the relevant card details, including the expiry date, as card issuers might decline a card if there isn't an expiry date or it's not valid.

To cancel a recurring transaction
The customer can get in touch with you directly or with their card issuer. If they don't speak to you directly, you may not know anything's been cancelled until the payment fails.

Accepting payments online

To accept payments online you can either use a Barclaycard payment gateway, which you integrate into your website, or you can use another Payment Service Provider (PSP).

Website information

It's important that your customers understand how to make payments and any restrictions that are in place. So make sure you clearly display this information on your website:

- your company name, registered office address, phone number and email address
- your company registration number and VAT number
- a full and clear description all the goods and services, including the price and all extra costs like taxes and delivery costs
- information on the type of transaction security you provide
- your privacy statement
- your transaction currency
- the merchant outlet country at the time of giving payment options
- the scheme logos of the cards you accept
- your delivery policy
- any export restrictions (it must be clear to cardholders where you are located)

Transaction receipts

You need to give your customers a transaction receipt as part of an order confirmation notice at the time of the purchase. This receipt has to include:

- an instruction to print or keep the receipt for future reference
- your company name, address and phone number for customers to contact
- your website address
- the total cost of the purchase and the currency it's made in
- the transaction date and type (e.g. whether it was a sale or a refund)
- the name of the purchaser
- an authorisation code
- a complete description of all the goods and services bought
- clear information on your Terms and Conditions, cancellation, returns and refund policy (if there are restrictions)
- the exact date any free trial period ends (if applicable)

Just make sure you only include the last four digits of the card number. And don't include the expiry date for Mastercard transactions.

You'll need to keep a record of the cardholder's name and address in case there are any questions in the future. It's also your responsibility to check the card when the goods are delivered to see if the card number and expiry date are the same as the one presented. And to also check that the signatures match.

If your customer is picking up their order, you'll need to cancel the original transaction and start a new Card Present transaction. Take a look earlier in this guide for how those work.

Using a PSP to accept online payments

If you don't use a Barclaycard payment gateway, we can accept your online payments through an accredited Payment Service Provider (PSP). You just need to make sure that the PSP meets the minimum security guidelines in this guide and that they offer the communication links needed.

It's up to you to make sure your PSP follows the Payment Card Industry Data Security Standard (PCI DSS) to help keep your business and your customer's card data as safe as possible. There's more on the PCI DSS and how to comply with it on page 21. If your PSP offer it, we'd also recommend you use their fraud management service too.

The services your chosen PSP offers and the charges they apply are part of the agreement between you and them, and are separate from our agreement with you.

Using your own software to accept online payments

If you'd prefer, you can also use your own equipment or software to accept online payments.

Just bear in mind that it's your job to make sure we can approve the equipment or software, and that it keeps to the necessary card scheme rules. You'll also need to make sure your PSP keeps to the PCI DSS and the Payment Application Data Security Standard (PA–DSS).

Using our payment gateway to accept online payments

Our online service lets you take quick and secure payments online. And business is open all hours, as you can take these payments 24 hours a day, all year long.

You have two options to choose from:

- using our Hosted Payment Pages (HPP)
- or hosting your own

If you choose our HPP, you can rest assured that these pages will meet the PCI DSS. And you won't see any sensitive card data either.

If you host your own pages, you can take more control over the process. But you'll need to integrate with our Application Programme Interface (API), so you can collect cardholder details and communicate directly with our gateway. If you want to do this, we'll give you a guide on how to get started.

If you don't use a Barclays-owned submission product, you'll need to correctly flag every transaction by using the correct level of APACS software. You should then maintain the level of software in line with the APACS standards.

If you don't, you'll be liable for any fines or penalties from the card schemes.

Requirements if you don't use a Hosted Payment Page (HPP)

Keeping your card data secure

Whether you use our payment gateway, your own software or someone else's, you'll need to have certain security measures in place. If you don't use a Hosted Payment Page (HPP), you'll have even more responsibility to make sure your customer's data is as safe and secure as possible.

Take a look at our guide to the PCI DSS and other security standards on page 21.

Accepting Mail Order and Telephone Order (MOTO) payments

Before we talk you through how to take MOTO payments, we need to point out that you only accept them if you and the card issuer are from the same country in the UK, Ireland or France.

Taking telephone orders

1. First, keep a record of the cardholder's name and address in case there are any questions in the future
2. Check the card on collection and delivery to make sure the card number and expiry date match the ones quoted
3. Ask the customer for their signature and make sure this matches the one on their card
4. If they're collecting the order, you'll need to cancel the original Card Not Present transaction and start a new one as Card Present transaction
5. Finally, you should give the customer a transaction receipt. We recommend that this only includes the last four digits of the customer's card number and doesn't include the expiry date for Mastercard transactions

Just remember, if you key in a transaction after a phone order, you won't be able to guarantee that the customer is the genuine cardholder and so you could be at risk of chargebacks.

Although you need to get authorisation, as this is a Card Not Present transaction it will only guarantee that there are enough funds in the account at that moment in time and that the card hasn't been reported as lost or stolen. It won't guarantee payment.

How to spot and stop fraudulent Card Not Present transactions

You do need to take extra care with Card Not Present transactions and to understand that there are greater risks. For example, without a cardholder and card in front of you, you won't be able to complete any of the usual visual checks. So it puts you at greater risks of accepting fraudulent transactions and chargebacks.

If most of your payments are online, over the phone or by mail order, you need to use an online or MOTO solution. That's because you won't be able to accept online transactions using your face-to-face Chip and PIN processing equipment.

A few important things to remember

- Authorisation only confirms that there are enough funds at that moment in time on the card to pay for the goods and that the card hasn't been reported as lost or stolen at that time. It doesn't guarantee payment
- You can use internet authentication (such as Verified by Visa or Mastercard, or Maestro SecureCode), which is the same as entering a PIN. Please refer to pages 27 to 34 for more information on Internet Authentication.
- Always make sure that goods are sent to the person named on the card and that you don't give them to anyone else
- **If the cardholder comes to collect their goods you'll need to cancel the original transaction and process a new Card Present transaction instead**

With these greater risks in mind, you should ask yourself the following questions before you accept any MOTO transactions. If the answer's yes, it could be a fraudulent transaction.

- Are the goods high value or easily resold?
- Is the transaction out of character compared to your usual orders or this particular customer's past orders?
- Is your customer ordering many different items?
- Does the delivery address seem suspicious, or has it been used before with different customer details?
- Is the customer being prompted by someone else whilst on the phone?
- Are they trying to use more than one card to split the cost?
- Does the customer lack basic knowledge of their account, or have a problem remembering their home address or phone number?
- Has there been previous declines with the card details provided?
- Have items been removed to lower the transaction value and gain authorisation?
- Have you been provided with several cards after initial cards have been declined?

Tools for monitoring fraud

You can use the following security checks to help you watch out for fraud. They won't be able to fully prevent fraud or stop you from being liable for chargebacks, but they are best practice and recommended by the card schemes.

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

These services can help reduce Card Not Present fraud by asking the cardholder for a small amount of extra information.

- CSC is a condition of the card schemes and asks for the last three numbers on the signature strip or the three digits in the white box next to the signature panel. Make sure you don't store the CSC after the transaction's been authorised
- AVS asks for the first five numbers of the cardholder's full statement address and for the numbers in their postcode.

Internet authentication (3D Secure)

Internet authentication services (Verified by Visa and Mastercard SecureCode) all use 3D Secure protocol to authenticate card users by asking them to log in with a password.

Depending on their card issuer, cardholders will register for this service – but Maestro transactions can only be authenticated through Mastercard SecureCode. Take a look at page 29 for more on this.

Fraud screening

Using rule-based tools can help reduce the risk of fraud to your business. It can let you cross check the name, address, phone numbers, card details, email address and IP address with past and daily records.

We know that fraudsters can use similar details elsewhere – for example using different card numbers but the same name and address, or the same IP address. So constantly cross checking this type of information will help you to spot this.

Make sure you reject any suspicious transactions (also called velocity checking) and then check further before accepting the order or request.

Using our payment gateway will give you extra fraud screening tools, as well as the ones above. Or you can use a number of different providers for tools like these.

To find out more about what's on offer, give us a call on **0844 811 6666**.

Extra security checks for online transactions

As well as all of the above checks, there are some extra steps you can take to try and keep your online transactions as safe as possible. Use our checklist below:

- check for sequential card numbers
- review orders going to and coming from the same customer – with the same name, address and card number
- review or refuse all or new orders going to a different delivery address other than the registered card address
- review or refuse duplicate purchases
- review or refuse the order if the postcode doesn't match
- refuse the order if the CSC doesn't match
- and refuse new orders that have an invalid expiry date

You should also:

- use the 'chargeback data' you receive to highlight possible problem names, addresses and IP addresses
- always make sure that you reply quickly to 'request for information letters' as you may be able to prevent the chargeback. Failure to reply opens up additional risk of chargeback
- use internet authentication (3D Secure) and CSC/AVS for added security

There's more on this and how you can make your staff more fraud-aware at **barclaycard.co.uk/paymentacceptance**

Refunds

If you sell products or services to customers without face-to-face contact, Distance Selling Regulations (DSRs) and e-commerce Regulations (ECRs) will apply. That's because if customers buy over the phone or online, they won't have had chance to examine or discuss the goods or services in person before they buy.

You're legally required to keep to these regulations
The aim is to make sure there's a minimum level of consumer protection across the European Union (EU), although other EU countries might put the regulations into practice differently. If you don't stick to these regulations, the courts can take action against you.

Make sure you include these regulations in your online or MOTO returns policy – find out more about them at **dshub.tradingstandards.gov.uk**

To make a MOTO or e-commerce refund

- Make sure the refund is processed to the card that was originally used and that it doesn't go over the original sale amount
- If the card or account originally used is closed, you can use another one
- If the customer doesn't have another card, you can credit the refund to the customer's bank account in line with your own procedure (as long as the credit isn't any winnings from gaming)

Other services

Dynamic currency conversion (DCC)

If your business takes payments from non-UK cards, your processing equipment can be configured for DCC. This makes it easier for Visa and Mastercard cardholders to pay in their home currency. And gives them a competitive exchange rate for purchases too.

The cardholder will be asked whether they want to pay using the currency of the card or their local currency. To make things straightforward, the transaction will stay in whichever currency the customer chooses from start to finish. That way, you both know how much the purchase costs at the time of sale.

Every time you send an authorisation request, you need to use the conversion rate for that date. If you're sending more than one request for the same transaction, use the rate that applies on the day of the final authorisation request. Remember that you're responsible for any rates that you've told your customer about.

A cardholder can opt out of Dynamic Currency Conversion transaction - it's their choice. If they opt out the transaction will be processed in sterling.

Chargeback and retrieval requests

A chargeback usually takes place when a cardholder disputes a transaction shown on their statement or you process a transaction outside the terms of your Merchant Agreement. They can cost your business money – that's why it's so important to understand what they are and how to protect your business from potential losses if they do happen.

Some of the most common reasons for chargebacks are:

- if the cardholder doesn't recognise the transaction (e.g. if they believe their card's been used fraudulently)
- if you've processed the transaction outside of your Merchant Agreement (for example, if you didn't get the right authorisation) or if you didn't follow the instructions in this procedure guide
- if the Card Not Present transaction was fraudulent (take a look at page 17 for more information on how to avoid these)
- if you didn't respond in time to a request for a copy of the transaction (a retrieval request)
- because the card wasn't valid when the transaction was made (this can happen if the transaction's made before the 'valid from' date or after the 'expiry date')
- if the sale amount (for one transaction or for a split sale) is more than your floor limit and you didn't ask for authorisation
- if you accepted a card that should have been verified by the PIN, but your processing equipment wasn't able to do this – if this happens, you're legally responsible for any fraudulent transactions and chargebacks
- if the goods or services were faulty, not as described or not received
- if the transaction was processed on the behalf of someone else. This is called laundering and breaks your Merchant Agreement
- a refund not received by the cardholder
- the use of an authorisation code that was not produced by Barclaycard

Tips to prevent chargebacks

You can help prevent chargebacks by following this guide and sticking to your agreement with us. For a quick reference, you'll find some handy tips below that will help protect your business.

- **Use Chip and PIN enabled processing equipment** and take these payments wherever possible. That's because the chip makes it more difficult for fraudsters to copy the card and the PIN makes it harder for them to use a lost or stolen card. Most cards have a 4-digit PIN, although Diners Club cards can have 4 or 6-digit PIN
- **Make sure all transactions are correctly processed** depending on the card type
- Only accept cards that you've agreed to process – as some cards have several functions
- **Don't accept mail, phone or online transactions unless you understand the risks** of these. If you see an increase in these types of transactions, get in touch so we can make sure you have the right agreement in place

- **Follow your instincts** – if something about a card, the person using it or the transaction itself doesn't seem right, make a code-10 call to our authorisation team (for Card Present transactions only)
- **Keep copies of all transaction records**, keep receipts for six months and copies of transactions for another seven months – you might need to provide them if there's a chargeback claim
- **Display a limited returns policy on your receipts** and at the point of sale so customers understand this

As long as you process contactless transactions in line with card scheme regulations and follow this guide, we'll also give you the same level of protection as Chip and PIN payments.

Want to talk about chargebacks?

We have a dedicated Chargeback Education Team on hand to give you advice on how you can reduce the risk of your transactions being charged back. Get in touch by calling **0844 755 0094** or email **chargebackteamportfolio.managers@barclaycard.co.uk**

Retrieval requests and how to respond

A retrieval request or request for information (RFI) is when a customer wants to see a copy of the transaction details. This is usually because they don't recognise the transaction, or if they need more details for their records (e.g. for an expenses claim or tax return).

This can also happen if the description on their statement doesn't match the name of your company – and they're worried the charge might be from someone else. If you seem to be getting a lot of retrieval requests, check what information you're showing to the customer. You can change the description by calling us on **0844 811 6666**.

If you carry out a lot of online or MOTO transactions, you'll need to include a contact number (or website or email if online) rather than a location within the statement description. For example, 'The E Shop London' should be shown as 'The E Shop, **01207 123 4568**'. This is a requirement for Visa and Mastercard – and used so customers can contact you directly rather than contacting their card issuer.

Here's how you respond to retrieval requests:

- for all online transactions, you need to include the website address or email address
- make sure you send us a clear and legible copy of the transaction details within the time requested (usually 14 days) – if you don't, the transaction will be charged back to you
- you'll need to send all relevant documents to support the transaction, this could be your Terms and Conditions, the authorisation codes and dates and times
- you can send this by fax or post (or another method depending on our instructions).

As you're just providing us with more information, there won't be any immediate loss to your business – unless it results in a chargeback.

Timescales for chargebacks

As most chargebacks happen because the customer disputes a transaction on their statement – it can be up to one month after the transaction before a customer checks their statement and gets in touch with their card issuer.

Here's an example of how the chargeback process can happen:

- the customer receives their statement and disputes the transaction – they claim their card or card details was used by someone else
- depending on card scheme rules and transaction type, the card issuer may ask the customer to complete and sign a disclaimer (this is a legal document where they declare they didn't make the transaction)
- once they have this back, the card issuer lets us know that there's been a dispute. There are strict time limits for them telling us this – we'll automatically protect you if the correct documents aren't supplied or these timelines aren't met
- we'll then let you know a chargeback's been raised – either by post, fax or another method we've agreed
- the card issuer has up to 120 days from the processing date to issue a chargeback. For Chargebacks relating to goods or services not provided, we work out the time limit from the expected date of goods/services.
- if it's likely that you'll have extra information about the transaction that can help us defend it, we'll give you 14 days to supply us with it
- if it's not likely that you can defend the dispute (e.g. if you didn't get authorisation), we'll take the transaction amount from your nominated bank account
- if you disagree, you'll need to write to us in 14 days to tell us. If your reply is unclear or we can't read it, we may not be able to defend you from the chargeback

We're here to help

Our Chargeback Portfolio Managers can give you advice on how to deal with chargebacks. For free advice, have your contact details and Barclaycard merchant number to hand and:

- call us on **0844 755 0094** (9am to 5pm, Monday to Friday, excluding Bank Holidays)
- or email **chargebackteamportfolio.managers@barclaycard.co.uk** and we'll get back to you in 48 hours

Payment security

To help keep your customers' data as safe and secure as possible, it's important that you keep to the Payment Card Industry Data Security Standard (PCI DSS). It's a set of guidelines to make sure payment information is stored securely by your company and anyone else who stores, transmits or processes the cardholder's payment information on your behalf. Remember that cardholder data should not be stored unless absolutely necessary to meet the needs of your business.

Sticking to this standard also forms part of your agreement with us. If you don't, you can be charged non-compliance fees, penalties and charges from card schemes – not to mention the impact it will have to your customers, and your business' reputation.

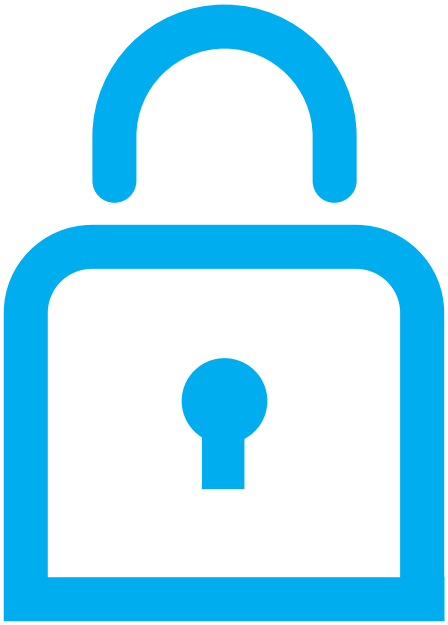
What information needs to be stored securely?

You'll need to make sure any information that's necessary to process card transactions is stored securely.

We call this 'cardholder data' and it includes:

- **any information used to authenticate a card payment, including:**
  - the card number
  - the expiry date
  - the issue number
  - passwords or pass phrases
  - and any other unique information supplied as part of the card payment
- **any information that could identify individual cardholders and their purchase**

  That means:
  - their name
  - their address
  - description of the purchase
  - the purchase amount
  - and other details of the card payment



What information shouldn't be stored?

Make sure the Primary Account Number (PAN) is rendered unreadable and that the data stored excludes sensitive data, which is:

- full magnetic stripe data
- the card verification value (CVV/CAV2/CVC2/CVV2/CID) which is stored within the magnetic stripe and chip
- the PIN or PIN blocks contained within the magnetic stripe

What do I need to do to be compliant with the PCI DSS?

There are 12 requirements within the PCI DSS which you must meet if you are to become compliant. These are best summarised by the six key goals of the Standard below:

1. Build and maintain a secure network and systems
2. Protect cardholder data
3. Maintain a vulnerability management programme
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

Take a look at the full details of the 12 requirements and what they mean on the Payment Card Industry Security Standards Council (PCI SSC) page at: **www.pcisecuritystandards.org**

Meeting these requirements will mean you're compliant with the PCI DSS and are running a more secure business for the peace of mind of you and your customers.

How to show you meet the PCI DSS

We need you to show us that you're meeting the PCI DSS every year. We also might ask you to pass vulnerability scans every three months to keep to the standard.

If you don't meet the PCI DSS, you could be legally responsible for paying any charges and penalties to us and the card schemes.

The actions you need to take to keep to the standard and how you let us know you're following them depends on your merchant level and the type and volume of card transactions that we process on your behalf, which we've explained below. We might also get in touch to tell you to take extra security measures for a set period of time.

Merchant Level	Definition	Actions needed to keep to the Standard
1	If you process over 6 million Visa or Mastercard transactions a year[1]	The Barclaycard Payment Security team will support you in achieving and proving your compliance with the PCI DSS each year. You'll have to: • ensure an on-site security assessment is completed every 12 months (or after a significant change to your cardholder data environment) by a PCI SSC accredited Qualified Security Assessor (QSA) or your own Internal Security Assessor (ISA), who is recognised by the PCI SSC • ensure network vulnerability scans are successfully completed every three months (or after a significant change to your cardholder data environment) • complete penetration testing every 12 months (or after a significant change to your cardholder data environment) of your internal and external networks • maintain an up to date Security Policy which is known to all employees
2	If you process 1 to 6 million Visa or Mastercard transactions a year	The Barclaycard Payment Security team will support you in achieving and proving your compliance with the PCI DSS each year. You'll have to: • either complete a Self-Assessment Questionnaire (SAQ) via your Internal Security Assessor (accredited by the PCI SSC) or run an on-site security assessment through a PCI SSC accredited Qualified Security Assessor (QSA) every 12 months (or after a significant change to your cardholder data environment) • ensure network vulnerability scans are successfully completed every three months (or after a significant change to your cardholder data environment) • Complete penetration testing every 12 months of your internal and external networks (or after a significant change to your cardholder data environment) • Maintain an up to date Security Policy which is known to all employees
3	If you process 20,000 to 1 million VISA or Mastercard online transaction a year	You'll need to use our Data Security Manager (DSM) online service to confirm your compliance via a self-assessment method. • You'll receive your DSM Welcome Pack no earlier than two weeks after your merchant account is opened with Barclaycard. This will include your user credentials and details of the monthly Data Security Fee • You'll need to follow the step-by-step instructions provided to complete your profile and the designated Self-Assessment Questionnaire (SAQ) every 12 months (or after a significant change to your cardholder data environment) to prove your compliance with the Standard. Alternatively, if you use another PCI DSS Assessor, you'll need to upload either your completed SAQ or your signed Attestation of Compliance (AOC) to the portal in order for your compliant status to be recognised by Barclaycard • If you're advised your business requires quarterly vulnerability scans, you can use DSM to fulfil this requirement for you or you can employ a PCI SSC recognised Approved Scanning Vendor (ASV) to complete this for you and submit your 'pass' reports to DSM every three months
4	If you only process online transactions and process fewer than 20,000 Visa or Mastercard transactions a year Or if you don't process online transactions and process up to 1 million Visa or Mastercard transactions a year	

A few notes:

1. If you operate in more than one country or region and meet the Level 1 criteria in any Visa country or region, you'll be considered a global Level 1 merchant. There might be an exception to global merchants if there isn't any common infrastructure and if Visa data isn't collected across borders. In these cases, we'll validate you according to regional levels.
2. If you're a Level 1 or Level 2 merchant who uses an ISA, you'll need to ensure that the ISA maintains their PCI SSC accreditation on an annual basis.

From time to time, we may audit the type and volume of your card transactions, which could change your merchant level. If this happens we'll let you know and you'll then have to make sure you comply to the PCI DSS according to your new level.

Using approved Qualified Security Assessors (QSA) and Approved Scanning Vendors (ASV)

If you need to have on-site security assessments or vulnerability scans, you must use a QSA or ASV who has been approved by the PCI SSC.

Take a look at the current list of approved organisations at:

- **www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors**
- **www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors**

Data compromises

If cardholder data is ever lost, stolen or revealed, or you think it might be, you need to get in touch with us as soon as possible. You also need to let us know if any unauthorised person had access to this.

What happens if data is compromised?

As well as telling us about any data compromises, you'll also need to employ an industry-approved Payment Forensics Investigator (PFI) to carry out a forensic investigation at your company. They'll review the whole end-to-end process of how you handle cardholder data and give you a report on their findings, with recommendations on actions you need to take.

There are a few other things that will happen after we've seen the Forensic Investigation Report:

- we may reclassify you as a Level 1 merchant and ask you to keep to the PCI DSS guidelines for this merchant type
- if the compromised data is stolen or used fraudulently you may have to pay fines to the card scheme and cover any losses to the card issuer. If your business isn't keeping to the PCI DSS, you might then have to pay additional card scheme fines

Take a look at the list of PFIs on the PCI SCC site:
www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators

Other organisations that store, transmit or process your cardholder data

The PCI DSS applies to every part of your business and any companies you're linked with. That means it's your responsibility to make sure any organisations that store, transmit or process cardholder data on your behalf also follow the Standard each year. The standard applies to both manual and electronic methods of processing and storing cardholder data.

A few examples of these organisations are:

- resellers
- till vendors
- EPOS vendors
- software application providers
- payment service providers
- payment processing bureaus
- data storage providers
- web-hosting providers
- shopping cart providers
- software vendors

You'll need to tell us about any organisations that handle your cardholder data and make sure they're registered on the Visa website: **www.visaeurope.com/media/images/visa%20europe%20merchant%20agent%20list%20october%202016%20-73-33499.pdf**

What could happen if I'm not compliant with the PCI DSS?

If customer cardholder data which you or your third parties have handled is compromised, stolen or used fraudulently, you could be liable for:

- substantial financial penalties for Account Data Compromise (ADC)
- potentially high costs for forensic investigations, issuer losses and business recovery
- reputational damage
- non-compliance charges for being in breach of the terms of your Merchant Agreement
- suspension of your acquiring facilities until compliance with the PCI DSS is evidenced

How to protect cardholder data

As well as keeping to the PCI DSS, you'll need to follow other requirements to keep your cardholder data as safe as possible.

If you're using thermal paper to process transactions, make sure that they don't fade when stored. You can stop this from happening by:

- keeping them away from direct sunlight and wrapping transaction copies in paper or storing them in envelopes
- storing them in a cool, dark and dry environment – away from heaters
- keeping them at an even temperature and humidity. Ideally this would be 20 – 23 degrees and 45 – 55% humidity
- not storing them in PVC wallets

You can get hold of prepaid envelopes by calling us on **0844 811 6666**.

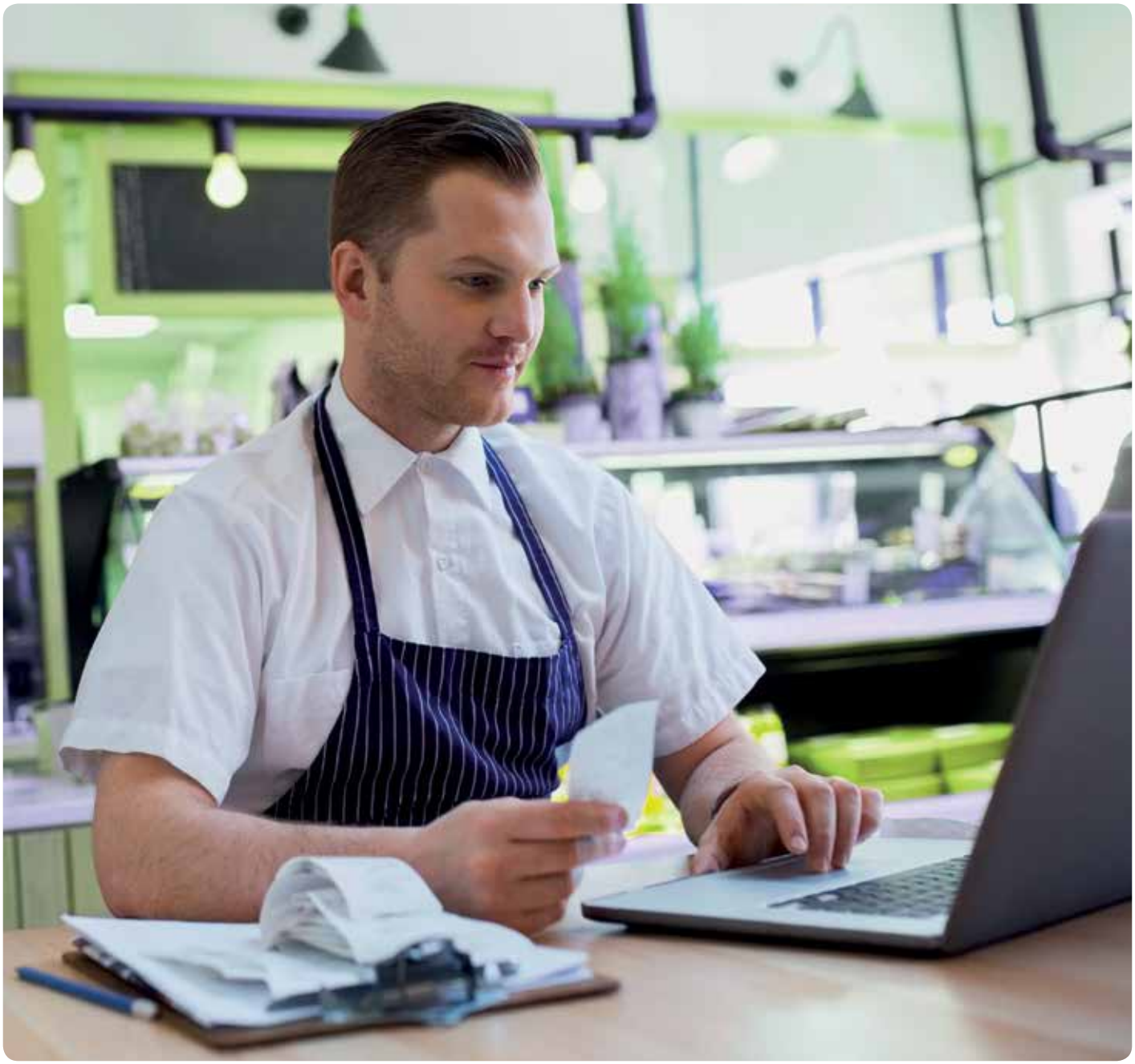
Storing your records

It's important to keep original copies of transactions in an accessible place for at least six months. We'd also recommend that you keep copies of transactions for seven months after that, although these can be on microfilm or similar media.

You should store the transactions by transaction date rather than by cardholder name or number. That's because we might not always be able to give you the cardholder name if there's a retrieval request.

You also need to keep all copy vouchers and till rolls in a secure place to keep to PCI DSS requirements.

Have a question about the PCI DSS?
Give us a call on **0844 811 0089**.



Understanding your statement

Your monthly statement doesn't just tell you about your transactions and the amount you owe – it's also your VAT invoice.

If you're a single outlet, or you've asked us to send separate statements to each outlet, you'll receive:

- a merchant invoice and statement
- and transaction payment advice

If you've asked us to send statements to your head office instead, they'll receive:

- a merchant invoice and statement
- transaction payment advice
- and advice on service charge details

Your outlets usually won't receive anything.

A closer look at your statement

You'll see page numbers in the top right-hand corner. There are three main headings: transactions and other charges, statement of account, and total amount due.

Inside your statement you'll also find:

Transactions payment advice

This gives you itemised details of payments made to you with the dates we processed the transactions, and the payment reference.

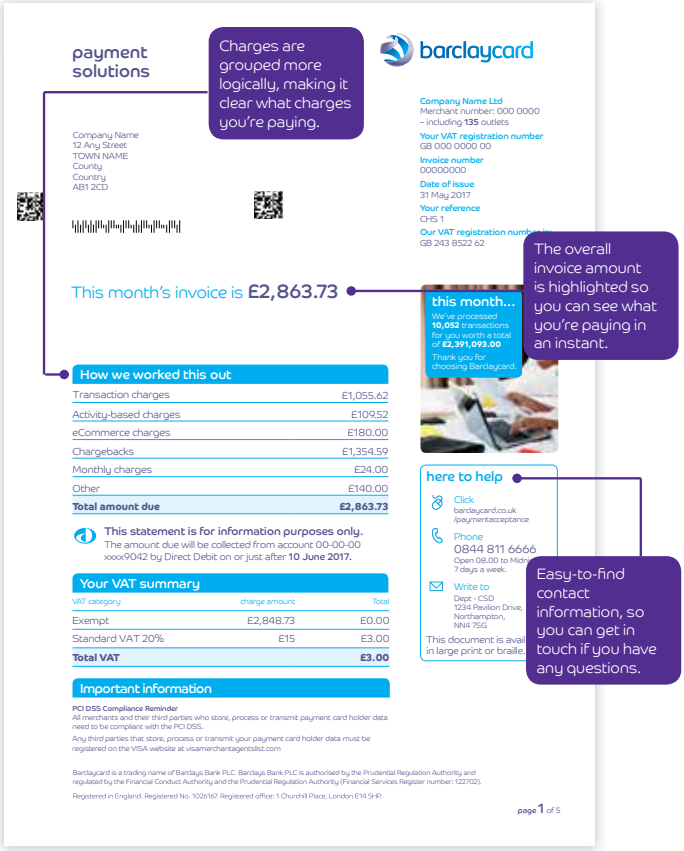
Periodic settlement

If you've chosen to be paid periodically (e.g. weekly or twice weekly), remember that the total payments figure might not match the transaction charges on page 1 of your statement. That's because they cover different accounting periods. Payment for any dates not showing will appear on your next statement.

Advice on the details of the service charge

This shows a breakdown of the invoice for each outlet and includes a customer reference. It shows processing equipment rental charges and the total charge. But only your chain head office will receive this.

Statement example



Questions about your invoice or statement?

Have your outlet or chain head office number to hand and call us on **0844 811 6666**.

Remember to check that all transactions have been processed and they show on both your merchant and bank statements. You'll also need to regularly check your monthly service charge statement against your bank statement to see that they match. If you don't, you could be legally responsible for any chargebacks for presenting transactions late.

Detailed transaction reports

We also offer detailed transaction reports, which provide a breakdown of all your transactions including our charges and the Interchange we've paid on your behalf for each card transaction. These reports are free of charge and available on request either on an ad hoc or more regular basis if required.

What do you need to do?

If you want to receive these reports, then please let us know by emailing your merchant name and address, Merchant ID and contact details to **transactionreport@barclaycard.co.uk**

Exceptional procedures

Passing charges to customers

No surcharge can be added to a payment made using a personal debit or credit card. You can ask your customers to pay a surcharge if they pay with a commercial card. But – it's important to really consider whether you want to do this or not.

If you do, you're at risk of being uncompetitive and upsetting customers who end up paying more than those who pay another way.

If you decide to apply a surcharge, you'll need to meet the below conditions.

1. Under the terms of the Price Indications (Method of Payment) Regulations 1991, you must clearly display the commercial card surcharge at the entrance of your premises and at the point of sale. If you sell fuel, the regulations are in the Price Making (Petrol) (Amendment) Order 1990
2. If you take online or MOTO payments, you'll need to tell your customers about the surcharge before they place the order. You'll also need to make sure that any catalogues, advertisements and the order form carry the exact details of the surcharge
3. The amount of the surcharge (that you add to your normal cash price), can't be more than the amount of the merchant service charge that you pay us

The rules governing surcharging are covered in the Consumer Rights (Payment Surcharges) Regulations 2012 – this has been updated by PSD2 to ban surcharging on all bar commercial cards.

It's up to you to make sure that these surcharges are only used if allowed by law, even when the cardholder isn't present. It is also your responsibility to make sure you apply the correct tax treatment to the additional charge.

If you'd like copies of any of the regulations we've mentioned above, contact your local Trading Standards Office.

Minimum charging

You can't set any minimum limit on credit and debit card transactions. You need to treat purchases by card in exactly the same way as cash purchases – except if you apply a surcharge.

Internet authentication

How to successfully authenticate customers

When your customers pay online, you can use internet authentication services to confirm their identity and reduce the chances of accepting a fraudulent transaction.

We offer the following card scheme authentication services, which we'll explain over the next few pages:

- Verified by Visa (for Visa transactions)
- SecureCode (for Mastercard and Maestro transactions)

Although using these services can help protect you against fraud chargebacks, there are different rules for different card schemes, card types and regions. Partial or attempted authentication transactions might not be protected in the same way.

To use an internet authentication service you need to:

- have a valid internet merchant relationship with us
- be registered with us
- and have the authentication software included in your chosen payment solution. Unless you specifically ask us for an alternative, we'll assume that you want to use authentication for all card schemes that support internet authentication

Once that's all sorted you have a few options. You can either use our payment gateway (that's already set up with 3D Secure or you can set this up yourself), or you can find or develop your own 3D Secure software solution. If you choose the latter, you'll need to make sure the software is approved by all card schemes we support and that the 3D Secure solution meets protocol level 1.0.2.

The different types of authentication

The card schemes use three types of authentication, which we've explained below. As each one works differently, you'll be liable in different ways.

Full authentication

This is where the card issuer, cardholder and you (the merchant) all correctly process an authentication transaction. The cardholder successfully authenticates themselves (through a browser pop-up or in-line window) with their card issuer. This is called 'Full authentication' for Visa and 'Full UCAF' for Mastercard.

The card issuer will provide an IAV (issuer authentication value) to show that the authentication took place, which acts as your proof.

Attempted authentication

This happens when the cardholder isn't registered for authentication, but you're providing an authentication request. If this happens, an IAV (also called an 'attempt') will be provided to show you that you successfully tried to authenticate the cardholder.

Visa, Mastercard and Maestro all define an attempted authentication as when you support authentication and can confirm that everything's been done correctly.

Passive authentication

This happens when an issuer presents a 3D Secure window but decides not to prompt the cardholder to authenticate the transaction. The cardholder then goes back to the merchant site without authenticating the transaction. If this happens, you'll still be covered by the full 3D Secure benefits.

The main authentication benefit – transferring liability

In the past, online transactions carried a higher risk than standard Card Present transactions. That's because you couldn't complete any visual checks or confirm the genuine cardholder was using their card – meaning chargebacks were more likely.

That's where cardholder authentication comes in.

This proves that valid cardholder details were used at the time of the transaction – helping to prevent chargebacks and shifting the liability from you, to the card issuer. (As long as you keep to the 3D Secure protocol.)

It's essential to reduce the risk of fraud as much as possible. That's why you should use internet authentication alongside the other fraud checks you should have in place – not instead of them.

Levels of protection

Cardholder authentication protects you against specific types of chargeback. Who's liable for this really depends on the card issuer and the type of authentication gained.

For Visa, Mastercard and Maestro there is full worldwide cover for fully authenticated transactions and successfully attempted authentication.

Displaying the Verified by Visa and SecureCode™ logos

To show customers that you use cardholder authentication, the card schemes require you to display the logos on your payment pages. So if they're not added automatically to your payment page, you should add them yourself. You'll be able to get these once you apply for 3D Secure.

If at any stage you decide not to take part in these schemes, you'll need to remove the logos (if they're not removed automatically).

Using our 3D Secure solution

Your responsibilities

We control the authentication process within the Hosted Payment Page (HPP) and will make sure there's as little disruption to your current transaction processing as possible.

But it's still your responsibility to:

- correctly integrate the HPP in line with the instructions you receive when you sign up
- read and understand how the HPP handles authenticated transactions (we've explained this earlier on in the guide)
- set up any 3D Secure fraud detection settings in your back office

Our responsibilities

It's our job to:

- register you with each card scheme we support
- provide you with the relevant integration guides
- control the processing of authentication transactions
- keep to the relevant card scheme policies
- process transactions according to your 3D Secure fraud detection settings
- maintain a full audit trail and provide transaction evidence to the card issuer if there's a chargeback where we believe authentication was correctly carried out and that the liability should be with them. (This doesn't include retrieval requests)
- make sure the correct authentication values are attached to both the authorisation and clearing message (where appropriate)
- maintain authentication transaction records on your behalf and use these to provide evidence that the transaction was authenticated if there's a chargeback. It's our responsibility to make sure the correct IAV (CAVV, AAV), ECI, and XID (for Visa) value is attached to both the authorisation and settlement transaction

Message values

When you use cardholder authentication, new message values will be created to show the level of security used, plus the result of the authentication. We'll make sure the HPP processes all the new message values correctly.

Sometimes, authentication might not be possible (e.g. if the in-line window doesn't appear). If that happens, you'll need to decide if you still want to process the transaction. You can set this on the HPP – see the HPP integration guide for how to do this.

If it's a Visa transaction you'll need to refuse it – your payment gateway provider may do this for you automatically, or provide you with settings to manage this.

Using your own authentication solution

If you're not using our authentication solution, you're then responsible for the whole authentication process and need to make sure you keep to the integration and implementation requirements.

And if you're using another product to carry out internet authentication, you need to make sure it supports the requirements shown in this section.

Your responsibilities

You need to:

- sign up for authentication, giving details of your chosen payment solution, and say that you only want to be registered for the service
- make sure we've approved your chosen payment solution to process internet authentication transactions
- correctly build and put into practice your authentication and payment solution in line with the latest 3D Secure procedure and APACS standards
- get our full approval for you to use the APACS standards at the necessary level
- make sure that the authentication responses returned by your authentication solution are correctly passed to your payment solution so they can be included in the authorisation message
- make sure that the IAV (CAVV for Visa and AAV for SecureCode) is correctly passed in the authorisation message
- make sure that any other data is passed in the authorisation message
- make sure any extra data is passed in the clearing message
- manage the process around the cardholder pop-up or in-line window (e.g. size and time outs)
- manage the process if an error happens on the pop-up or in-line window (if the cardholder cancels)
- secure the authentication merchant information that's used to register you with the card schemes
- make sure the BIN cache for each scheme (if being used) is updated at least every 24 hours
- maintain full audit records of authentication transactions (including BIN cache updates)
- give us evidence of authentication (e.g. your 3D Secure logs) if we ever need to defend a chargeback. If this happens, you'll need to send us this information within 14 days

Our responsibilities

If you do all of the above, we'll make sure we:

- register you with each card scheme we support
- give you any authentication merchant information that's registered with the card schemes
- accept authorisation and clearing messages from your chosen payment solution that include authentication data
- provide transaction evidence to the card issuer if there's a chargeback where we believe authentication was correctly carried out and that the liability should be with them
- let you know about any scheme or procedures updates

Transaction records

It's important that you keep and store full authentication records. That way you'll be able to give evidence if there's ever a chargeback claim or a retrieval request. If you don't have this, you'll be at risk of being liable for the transaction and we won't be able to defend it.

Here's a guide to what type of evidence you'll need to provide:

Card issuer pop-up or in-line window

You need to provide your online customers with a pop-up or in-line window in their browser so they can authenticate themselves. You can choose whichever you like, but we'd recommend going with an in-line window, since there could be problems with pop-ups being blocked. The card issuer will create the content and carry out the authentication, but you have to take care of the rest.

You'll need to:

- make sure you give customers a reasonable amount of time to authenticate themselves before the window times out. You should set this time in line with your website and risk policy
- display an error message if your customer does time out – and control the size and conditions of this
- make sure your website can handle error responses (e.g. if your customer closes, cancels or can't view the window)
- use a balance of informative and non-specific information so you don't encourage potential fraud

	Visa	Mastercard
Full authentication / full UCAF	• ECI value = 5 CAVV • Supply this in a readable format, PAReq/PARes XID	• ECI value = 2 AAV • Supply this in a readable format, PAReq/PARes
Attempted authorisation / merchant UCAF	• ECI value = 6 attempts CAVV • Supply this in a readable format, VEReq/VERes OR PAReq/PARes XID	• ECI value = 1 AAV • Supply this in a readable format, VEReq/VERes OR PAReq/PARes

Does your solution support BIN cache? If so, you'll also need to give CRReq/CRRes.

Your authentication merchant information

We'll give you specific data so you can take part in online authentication and will register you with each card scheme. We'll only give this information to you – and won't be able to release it to any payment providers acting on your behalf.

You'll need to carefully code these details into your authentication solution and pass them on each authentication request. Make sure everything's correct, as the information might be different for each scheme. If you don't – the authentication request might fail.

Once you've entered this information, you shouldn't change it unless we tell you to. If you lose the information or think it may be compromised, tell us immediately. We'll then issue you with new details and re-register you with each card scheme – which could take up to 10 working days.

Message values

When you use online authentication, new message values will be created to show the level of security used, plus the result of the authentication. You'll need to make sure you fully understand the responses sent to your authentication solution by the card schemes and then pass it to your payment solution in the authorisation and clearing messages.

The key value is the issuer authentication value (IAV), which will come from your card issuer and shouldn't be changed. Visa call this the CAVV and for Mastercard it's the AAV. Your payment solution needs to check that you've attached the correct e-commerce indicator (ECI) to the authorisation and clearing message.

Here's a guide to the different ECI values each card scheme uses:

Card scheme	ECI value	Message
Visa	5	Authentication's successful.
	6	Authentication was attempted but the cardholder's not registered.
	7	Authentication's not successful or not attempted (standard e-commerce transaction).
Mastercard and Maestro	2	Authentication's successful. Full UCAF.
	1	Authentication was attempted but the cardholder's not registered. Merchant UCAF.
	0	Authentication's not successful or not attempted (standard online transaction).

Take a look at your authentication software integration guide for details on how to map these values into your payment solution.

You need to make sure your payment solution supports the correct APACS level so it can communicate with our acquiring system. Just call us if you need this information.

BIN cache

The BIN (Bank Identification Number) cache is a store of BIN ranges that can be held locally on your server. If you want to use this, you'll need to contact each scheme directly through a 3D Secure request (CRReq/CRRes) to download the latest version at least every 24 hours.

You can check the BIN cache before contacting the scheme directory to check whether the cardholder's taking part in that scheme. This can help to reduce the number of messages you need to generate.

Keeping to the card scheme rules

It's important that you understand any responsibilities you may have when taking part in cardholder authentication. This will vary according to whatever payment product you use.

If authentication fails or there's a mistake

If your customer is registered for authentication, they'll usually have no trouble authenticating themselves. But mistakes can happen and sometimes cards could be used fraudulently. If those things happen, you'll get one of these scenarios:

1. Failed authentication – that's where the customer has entered a wrong password (they may have up to three attempts)
2. A mistake during authentication – that's where:
   a. the cardholder cancels or closes the pop-up or in-line window
   b. the pop-up or window times out
   c. the content may be corrupt because the issuer made a mistake
   d. or the customer's browser blocks the pop-up

   How you deal with these, depends on the card scheme you're using.

How to respond if authentication fails

Card scheme	What message will you receive in the PARes message?	What should you do?	Message
Visa, Mastercard and Maestro	'N' response.	Refuse the transaction and don't process it. If you choose to continue and attempt authorisation you will be liable for the transaction.	If you are using a Barclaycard gateway, our e-commerce solution will automatically either refuse or continue with the transaction depending on how the response is returned and in line with scheme rules. If you are not, please check the instructions for your Payment Gateway to understand how your system handles outcomes of the 3D Secure process.

Passing authentication values

You need to make sure you keep to our Barclaycard e-commerce solution v1.0.2. And you need to pass the authentication results in your authorisation and clearing message – this should include the APACS standard that supports this.

Just get in touch for information on which standard is used. But if you use our integrated 3D Secure solution, you won't have to do this.

You'll need to be able to receive and pass:

- issuer authentication value (IAV) – CAVV for Visa, AAV for SecureCode
- ECI values
- XID (for Visa)
- 3D Secure procedure messages

You shouldn't change these values in any way.

The CAVV or AAV could be incorrectly passed if:

- the payment solution you're using doesn't support these values
- there's a problem with your integration to the hosted authentication service or payment software

And the ECI values could be incorrectly passed if:

- there's a problem with your integration hosted authentication service and/or payment software
- you've registered to take part but haven't asked to go live yet
- you've accidentally hard-coded every ECI value to a set limit (e.g. ECI for standard or e-commerce)

It's important that you do everything you can to avoid these mistakes. Because if you fail to pass the IAV, or incorrectly pass the ECI, you'll be liable for the transaction. And if you deliberately falsify any authentication value, we might end your authentication and merchant agreements with us.

Please see the integration instructions for your payment gateway to check whether you need to process or pass the authentication values in your authorisation requests.

Error conditions

It shouldn't happen often – but if there's ever an error when using cardholder authentication, you'll need to be prepared for the below situations.

Scheme directory server unavailable

This happens if you can't connect to the relevant scheme directory. If this is the case, you'll see an error message, which you'll need to handle appropriately.

If the directory server isn't available, this is considered a 'break' in the authentication process as a success or failure message couldn't be supplied. Who becomes liable for this depends on the card schemes.

- For Visa – you can continue with the transaction, but as this is non-authenticated you'll need to pass an ECI 7. And you won't be protected from chargebacks
- For Mastercard and Maestro – you can continue with this transaction and pass ECI 6, as the transaction is deemed to qualify as 'attempted authentication'

Hosted authentication not available

If you can't authenticate transactions because the hosted authentication service isn't available, this is also classed as a 'break' – but there's a different outcome.

You can continue with the transaction, but as it's not authenticated you'll need to pass an ECI 7 for Visa or ECI 0 for Mastercard. Bear in mind that you won't be protected from any chargebacks.

Please check the instructions for your Payment Gateway to understand how your system handles outcomes of the 3D Secure process.

Cardholder browser doesn't display the pop-up

If the customer's browser blocks the pop-up, this is also classed as a 'break' in the authentication request. As with the other scenarios above, you can carry on with the transaction – but if it's a Visa transaction, you won't benefit from any chargeback protection.

That's why we'd recommend you use an in-line window, so this doesn't happen.

Your own authentication software not available

If you can't authenticate transactions because your authentication service isn't available, this is also classed as a 'break' – but there's a different outcome.

You can continue with the transaction, but as it's not authenticated you'll need to pass an ECI 7 for Visa or ECI 0 for Mastercard. Bear in mind that you won't be protected from any chargebacks.

Chargeback reason codes

Each different card scheme uses a different reason code to charge a transaction back. If you're using any automated risk tools, you should make sure you cater to each scheme reason code if it applies.

One of the main reasons the authentication schemes are in place is to stop chargebacks from happening.

The card issuers are adding edits to help make sure you're not charged back for a transaction if it's been authenticated properly.

You'll be liable for the transaction for any chargeback reason codes that we haven't included in this guide.

Visa

75	Transaction not recognised – when the cardholder tells you that they do not recognise an item on their card statement.
83	Fraud card absent environment – the card was not present and a transaction was processed without the cardholder's permission, or a fake (card) account number was used.

Mastercard and Maestro

37	No cardholder authorisation – the cardholder denies responsibility for the transaction or the acquirer lacks evidence of a cardholder's authentication (in other words, a signature).
63	Cardholder does not recognise – potential fraud. When a cardholder claims he or she does not recognise a card-not-present transaction (such as an e-commerce transaction). If after being presented with new information, the cardholder says that they did not authorise the transaction. You may be asked to provide supporting information to us to defend a transaction (see section on Retrieval requests on page 20). Protection against this reason code may help to avoid a chargeback following the request.

Storing cardholder credentials

Your customers' card details should be just as important to you as they are to them. So if you give your customers the opportunity to store their credentials with you for future payments, you must comply with the latest stored credential requirements.

Stored credential

A stored credential, also known as credential on file (COF), is information stored by you to process future purchases for a cardholder. A credential is not considered a stored credential when the merchant stores the credential to complete a single transaction or a single purchase for a cardholder.

For example, when a cardholder provides a payment credential to a hotel to cover future reservations and charges as part of the cardholder's membership profile, it is considered a stored credential. However, when the cardholder provides the payment credential to a hotel to cover charges related to a specific reservation only, it is not a stored credential.

It is important to know:

- there are requirements for flagging stored credential transactions
- stored credential transactions will not contain a CSC as this cannot be stored. Issuers will not be allowed to decline transactions solely based on the absence of this data
- you are required to comply with the stored credential cardholder disclosure requirements
- the industry practices where you might store card details are called Merchant Initiated transactions
- credentials might also be stored for the purposes of a Cardholder Initiated transaction. For example, a 'one click' type transaction where the cardholder has stored their details for future purchases on a merchant site

Disclosure requirements

When entering into a cardholder agreement, all requirements related to the specific transaction type listed below must be clearly displayed at the time that the cardholder gives their consent and must be displayed separately from the general purchase terms and conditions.

When capturing a stored credential for the first time you must establish an agreement with the cardholder that contains all of the following:

- a truncated version of the stored credential (for example, the last four digits of the account number), as it may be updated from time to time
- how the cardholder will be notified of any changes to the agreement
- how the stored credential will be used
- the expiration date of the agreement, if applicable

In addition, before processing an instalment, recurring or unscheduled credential-on-file transaction, you must obtain the cardholder's express informed consent to an agreement that contains all of the following:

- the transaction amount (including all associated taxes and charges) or a description of how the transaction amount will be determined
- the transaction currency
- where surcharging is permitted, acknowledgement of any surcharge assessed and the associated disclosures
- cancellation and refund policies
- location of the merchant outlet
- for instalment transactions, both:
  - total purchase price
  - terms of future payments, including the dates, amounts, and currency
- for recurring transactions, the fixed dates or intervals on which the transactions will be processed
- for unscheduled credential-on-file transactions, the event that will prompt the transaction (for example, if the cardholder's balance falls below a certain amount)

You must retain the cardholder's agreement for the duration of the agreement and provide it upon request.

Transaction processing requirements

When capturing a stored credential for the first time you must submit an authorisation request for the amount due. If payment is not required, submit account verification. If this is not approved, do not store the credential.

For a cardholder initiated stored credential transaction you must also validate the cardholder's identity (for example: with a login ID and password) before processing each transaction.

For an instalment, if an authorisation request for a subsequent payment is declined you must notify the cardholder in writing and allow them at least seven days to pay by other means. You must not process an initial instalment until the merchandise or services have been provided to the cardholder and must not process individual instalments in intervals of less than seven calendar days.

Cancellation procedure

You must provide a simple cancellation procedure and, if the cardholder's order was initially accepted online, at least an online cancellation procedure.

Do not complete a transaction:

- beyond the duration expressly agreed by the cardholder
- if the cardholder requests a change of payment method
- if the cardholder cancels according to the agreed cancellation policy
- if it receives a decline response

For an instalment, if the cardholder cancels within the terms of the cancellation policy, you must provide to them with a cancellation or refund confirmation in writing and a credit receipt for the amount specified in the cancellation policy.

Sector-specific trading – Vehicle rental companies

Best practice guide for reducing chargebacks

There are certain types of chargebacks that happen most often for vehicle-rental providers. So to help reduce these and the cost to your business, you'll find some best practice tips over the next few pages.

Authorise every transaction

It's important to do this, just remember that authorisation doesn't guarantee payment. It only confirms that the card hasn't been reported as lost or stolen and that there are enough funds available to make the transaction.

You'll still be legally responsible if the cardholder later states they didn't make a Card Not Present transaction.

There's a greater risk of chargebacks if you take Card Not Present transactions. So we'd recommend that you always try to process Card Present transactions where possible and make sure the cardholder is verified by their PIN or signature.

Tips for phone reservations

As these are Card Not Present transactions, you should ask for as many details as possible to check that the cardholder's authentic. This won't prevent all types of fraud, but it will help to deter some fraudsters.

Ask for:

- the caller's name and the name of the person who needs the vehicle (if it's not the caller)
- their direct-dial phone number (not a mobile)
- the number of days they're going to rent the vehicle
- the card number and the cardholder's name
- the cardholder's billing address
- the card 'valid from' and 'expiry' dates
- the card security code (the last three digits on the back of the card)

If your vehicle registration system allows you to check the card security code, you should enter it at the time of the transaction. Just make sure you don't keep or store this.

You should also clearly explain and agree the hire rate and get the caller's permission to accept your cancellation and no show policy. Once you've confirmed that you've accepted their order, send the cardholder a copy of your Terms and Conditions and written confirmation of the reservation details, along with the cancellation and no show policy.

Tips for taking fax or mail reservations

Just like taking phone reservations, we recommend taking as many details as possible. Use the checklist on the left – except for taking the CSC.

When taking orders from company cardholders, check that the fax or letter looks genuine. You should also check if:

- the company logo looks real
- the corporate colours are correct
- the switchboard number is real by calling them
- it contains a registered address for Ltd and PLC companies
- it's signed by someone in authority

Ideally, you'd also reply in writing (can be by email) to confirm that you're accepting the reservation and send a copy of your Terms and Conditions, including your cancellation policy, reservation details and no show policy.

Note regarding terms and conditions

If a dispute is raised you may be asked to prove that the cardholder was aware of the terms and conditions at the time the reservation was made. If you are unable to provide proof we may not be able to defend on your behalf.

Tips for taking online reservations

These types of transactions are effectively classed as Card Not Present transactions and carry higher risk for chargebacks. That's why we'd recommend using internet authentication so you can check the cardholder's genuine (see page 27).

You should also use the same procedures and precautions as you do for phone reservations (see our checklist on the left). And make sure your customers confirm they accept your Terms and Conditions, e.g. by having a tick box.

Extra checks for all transactions

You can check that the billing and company address are correct by comparing it to the address listed by the Royal Mail at royalmail.com. Use your reservation system (or stand-alone computer) to do this. Or you can even invest in PC software to do this for you.

You can also check:

- **streetmap.co.uk**
- the Electoral Roll. Companies like Equifax do this and will charge for the service (**0845 600 1772** or **equifax.co.uk**). Or you can buy and install electoral-roll software

Guaranteed reservation

When a cardholder makes a reservation and gives you their card details, but no payment is taken. Cardholders have a 24-hour window to cancel their booking – from the time they receive your confirmation. Make sure your Terms and Conditions clearly spell this out, and we recommend you flag them to your customer when you send their booking confirmation.

If you can, do an account verification transaction/check to validate their card.

Not sure how to do it? Speak to your payment solution provider who will be able to help. Just so you know, you may be charged an authorisation fee.

Your cancellation policy

You can have a cancellation policy in your Terms and Conditions which you'll need to clearly explain to your customer.

You also can't ask for more than 72 hours' cancellation notice before the scheduled collection time and date of booking.

Your no-show policy

If the cardholder doesn't arrive or doesn't cancel their reservation, you can charge one day's hire to the card (at the end of hire period) given when the reservation was made. If this happens, send a copy of the transaction receipt with a copy of your Terms and Conditions to the billing address you've been given. 'No-show' must be clearly written in the space where the cardholder would usually sign the transaction receipt – this should also show the card number, expiry date and cardholder name. It's important your Terms and Conditions clearly show a 'no-show' charge will be made for one day's hire.

When you charge for a no-show, you must send the transaction receipt, along with a copy of the invoice, to the cardholder. If you don't send these to the customer, the cardholder may dispute the transaction with their card issuer, which could lead to a chargeback to you.

Not got the cardholder's CSC code? The capture of CSC is mandatory for all Card Not Present transactions. However, Visa have made an exception to the rule for no show and delayed transactions. If your equipment doesn't let you bypass the CSC field for Customer Not Present transactions, we recommend you select customer present and write 'no-show' on the signature line.

Collecting the vehicle

When your customer comes to collect the vehicle you should:

- ask to see their card
- ask them to read your Terms and Conditions, and then sign the rental agreement
- carry out any visual check to make sure the card's genuine
- explain your cancellation or no show policy and ask the cardholder's permission to be charged extra or delayed charges
- get payment by processing a Card Present transaction if possible (see page 5 for more on how to accept these). If you already have payment you should get an imprint of the card on the card rental agreement as proof that they've agreed to pay by card

You can't ask them to sign a blank transaction receipt, just in case there are any other charges.

If you can't honour the reservation, you'll need to provide the agreed or comparable vehicle at no additional cost to the cardholder or transportation to another outlet.

Pre-authorisation

Pre-authorisations have to be processed within 30 days for Mastercard transactions and 31 days for Visa. For Visa, any Incremental Authorisation Requests do not extend the 31 day timefame. You should base your estimate on:

- how long the customer plans to rent the car
- the rental rate and tax
- and the mileage rates

You can't use this to cover possible damage or other insurance excess amounts. Pre-authorisations are valid for the length of the rental period. For extended hire, we'd recommend you close the customer's account after 14 days and bill them every two weeks.

You can update estimates as often as you need, up to and including the date the vehicle's returned to you. When you issue a new estimate, make sure it doesn't include amounts that have already been authorised.

How to make pre-authorisations

The cardholder will need to verify that they're the genuine cardholder by using their PIN. We've explained how to do this on page 8.

Useful tips for pre-authorisations

- Make sure your transaction receipt always includes the details of the authorisation code, the dates and the amounts
- Always tell the customer how much you've estimated, as it will reduce the funds available on their card. Explain that they've not been charged yet, and their final bill might be different to the estimate
- If your customer decides to reduce the hire period, you can refund them. Just make sure refunds go onto the card they used for the original payment

The end of the hire period

If you've pre-authorised an amount, you might not need to get another authorisation code when the hire period's over. This all depends on the final amount to be paid and the card scheme you're using.

For Visa transactions:

- You can use the code provided during the pre-authorisation if the final bill is within 15% of that amount

You'll need a final authorisation code if:

- there's a 15% difference between the estimated transaction and the final amount
- you haven't got a previous authorisation
- the customer is paying by Visa Electron and the final bill is more than the sum of all the estimated authorisations you've already received for the hire period

For Mastercard transactions:

- if the final bill is more than the estimated amount, you'll need another authorisation code for the difference

Accidents or damage to the vehicle

If the hire vehicle's involved in an accident, you can charge cardholders for the damage. You'll need to get an estimate of the cost from an organisation that can legally provide these services and then send this estimate to the customer.

If you'd like to do this for Visa cardholders, you'll need to meet the following conditions.

- The customer must have agreed in writing to pay the charges by a Visa card (the permission should be part of your rental agreement). It's essential that your car rental agreement clearly states that any extra or collision charges will be charged to the card they originally paid with
- They'll need to sign to agree that they accept these Terms and Conditions and their signature must be on the same page of the car rental agreement as the Terms and Conditions that state that you can charge them. If this doesn't happen, we might not be able to defend any chargeback claims
- The charge must be made within 90 days of the rental return date
- There's a bigger risk of chargeback if you don't let the customer know about the charge – so you should tell them this is happening

For Mastercard cardholders, you'll need to meet the below condition.

- You should get a separate cardholder signed authority by processing a Card Present transaction. If the card is disputed later, you can use this as proof that the cardholder authorised the extra charge

How to deal with delayed charges

To process a delayed charged (e.g. damage, fuel, insurance, parking tickets etc), the customer must have agreed to them, by signing the rental agreement and agreeing to the Terms and Conditions. You'll also have to meet the below conditions.

- Your Terms and Conditions will need to clearly explain that the cardholder is legally responsible for the charges and that they'll be taken from the card they originally paid with
- Their signature must be on the same page of the car rental agreement as the Terms and Conditions that states this. If not, we might not be able to defend any chargeback claims
- Any charges must be processed within 90 days of the rental return date, check out date or disembarkation date – and you must get further authorisation
- The charge must be made using a separate transaction, with the words 'Signature on file' clearly visible
- You'll also need to write to the cardholder about any damage charges within 10 working days of the vehicle's return date – sending it to the address on their rental agreement. This needs to include details of the damage, the cost and the currency in which the damage will be charged to them and an estimate of the cost of repairs from an organisation who can legally provide these services.
- You'll need to send a copy of the transaction receipt to the cardholder
- You'll also need to provide written documentation that:
  - explains the charge and links it to the cardholder's use of the good or services during the rental period
  - includes any accident, police or insurance reports (if applicable)
  - for rental cars and trucks give at least two quotes from companies that are legally permitted to perform repairs
  - shows the amount of damage or loss that will be paid by insurance, and the reasons why the cardholder is liable for the amount claimed
  - tells the cardholder that payment for loss or damage with their card is optional and not an obligation or default option

Once they receive this from you, the customer can reply with another estimate for the cost of repairs. They'll need to do this within 10 working days of receiving your letter. It's then up to you to agree on the estimated cost before you process the delayed or amended transaction. If you do this without agreeing the cost with the customer, you'll be liable for chargeback claims.

If a dispute is raised you will need to forward copies of this documentation to us. An English translation of the documentation will be required.

You need to wait 20 working days from the date you receive the confirmation receipt before you process the charges.

To help us defend a dispute relating to a traffic offence you will need to send us:

- a copy of the signed rental agreement
- documents from the appropriate civil authority
- the licence number which should match the number on the rental agreement
- notice of the amount charged
- English translation of any documentation

Accepting split sales

You can accept split sales – that's where a customer asks to split payments between cards, cash or cheques, or to share costs with other customers. Just bear in mind that these can result in a high number of chargebacks.

That's why you must always get authorisation no matter what your floor limit is. You also need to tell the authorisation operator that the transaction's part of a split sale at the beginning of the call. And you can only process one transaction for each card.

Your refund policy

If you operate a no-refund policy, you must make this clear to your customers when they make a reservation.

And if you do agree to refunds, be aware of opportunities for fraudsters. To avoid these you should:

- always credit refunds to the card that made the booking
- never refund by cash, cheque or other payment types

If you make a charge to a card by a mistake, you need to refund it to them within 30 days. If you're using Barclaycard processing equipment that's contactless-enabled, you can make contactless refunds up to the value of the current limit. These won't need cardholder verification.

Extended hire

We'd strongly recommend that you don't allow your customer to hire the vehicle for more than two weeks without settling their bill. You can ask customers who want to extend the lease for more than two weeks to pay the current total due – ideally by doing this in person.

Failing that, they can use the card details provided at the original booking (although there's a risk that this amount could be disputed at a later date if you don't have a signature or PIN).

Disputed transactions

If a transaction is disputed, it's essential for you to show that the card was present and authorised (if needed). Unless it's a contactless transaction, we won't be able to defend you from chargebacks if a PIN, signature or authorisation wasn't given.

The most common reasons why disputed transactions are charged back for vehicle rentals are:

- for delayed or amended charges
- when a fraudster makes a reservation with a card but never arrives. Usually that's because the fraudster is making the reservation to check that the card is valid and funds are available. The genuine cardholder will only find out when you charge them a 'no show' fee later on

But sometimes they might need a full breakdown of the charge. We'll always let you know what's needed when we get in touch.

Head to **barclaycard.co.uk/business** to learn more about chargebacks and how to avoid them. Or give our dedicated Chargeback team a call on **0844 755 0094** and we'll be happy to help.

Sector-specific trading – Lodging and accommodation

Best practice guide for reducing chargebacks

There are certain types of chargebacks that happen most often to hotel, lodging and accommodation businesses. To help you avoid chargebacks, we've created this best-practice guide. It takes you through the right chargeback procedures step-by-step and also gives you handy hints on how to cut back on potential chargeback costs.

Authorise every transaction

It's important to do this, just remember that authorisation doesn't guarantee payment. It only confirms that the card hasn't been reported as lost or stolen and that there are enough funds available to make the transaction.

You'll still be legally responsible if the cardholder later states they didn't make a Card Not Present transaction (except for contactless payments). And we might not be able to defend you if there isn't a signature on the final bill. There's also a risk if a guest checks out using a priority check-out service.

Advance booking tips

When you can, ask guests to make their own reservations, rather than through a third party. It goes without saying this might not always be possible and you might have to take bookings from secretaries, for example.

Tips for phone bookings

As telephone reservations are Card Not Present transactions, ask for as many details as possible to check if the cardholder is genuine. You should ask for:

- the caller's name
- their direct-dial number – rather than a mobile number
- the name of the guest the accommodation is for (if it's not the caller)
- their arrival date and time
- the number of nights they're staying
- the card number they'll be using to pay
- the card expiry date
- the cardholder's name and their billing address – this might not match the company address
- the card security code (CSC) – this is the last three digits of the signature strip, or in the box next to it, on the back of the card

If it's a corporate booking, you should also ask for:

- the caller's name and job title
- the name of the company or organisation
- the company or organisation switchboard number

If you can, do an account verification transaction/check to validate their card.

Not sure how to verify an account or card? Speak to your payment solution provider, who'll be able to help. (Just so you know, you may be charged an authorisation fee for this.)

You should also discuss and agree the room rate and your cancellation policy and ask the caller to accept these terms. Once the caller's agreed, you can give them their reservation code.

If the booking is made by a third party, for example a travel agent, make sure they tell their customer about your Terms and Conditions. Then ask the caller to confirm the reservation in writing by fax or email.

Tips for fax or mail bookings

Double check the fax or letter looks genuine.

Some obvious things to look out for are:

- is there a company logo in the correct corporate colours? You can check on the internet

- is there a switchboard telephone number? If so, call – it should be answered with the company name
- is there a registered address for Ltd and PLC companies?
- has it been signed by someone in authority?

Bookings by fax or post should include the same details as telephone reservations – except for the CSC. The customer also needs to confirm they've accepted your cancellation policy. Our advice is to call the sender to confirm their booking, card details and the CSC. It's also a good idea to confirm their reservation in writing, by fax or post, and include a copy of your Terms and Conditions along with your cancellation policy.

Note regarding terms and conditions

If a dispute is raised you may be asked to prove that the cardholder was aware of the terms and conditions at the time the reservation was made. If you are unable to provide proof we may not be able to defend on your behalf.

Tips for taking online bookings

Internet transactions are, in a nutshell, Card Not Present transactions and more likely to end up as a chargeback. That's why we'd recommend using internet authentication so you can confirm the bookings are being made by genuine cardholders (see page 27 for more on this).

You should also use the same procedures and precautions as you do for phone reservations (see our checklist above). And make sure your customers confirm they accept your Terms and Conditions, e.g. by having a tick box.

Extra checks for all transactions

You can check that the billing and company address are correct by comparing it to the address listed by the Royal Mail at royalmail.com. Use your reservation system (or stand-alone computer) to do this. Or you can even invest in PC software to do this for you.

You can also check:

- **streetmap.co.uk**
- the Electoral Roll. Companies like Equifax do this and will charge for the service (**0845 600 1772** or **equifax.co.uk**). Or you can buy and install electoral-roll software
- the Yellow Pages or BT Telephone Directory for the customer's listing. You can then call and ask for the person who sent the fax

Mastercard guaranteed reservation

When a cardholder makes a reservation and gives you their card details, but no payment is taken. Cardholders have 72 hours before they're due to arrive to cancel their booking. Make sure your Terms and Conditions clearly spell this out, and we recommend you flag them to your customer when you send their booking confirmation.

Visa guaranteed reservation

Cardholders have at least a 24-hour window to cancel their booking from the time they receive your confirmation. You need to make sure your Terms and Conditions clearly spell this out. We also recommend you flag this to your customer when your send their booking confirmation.

If you can, carry out an account transaction check (account verification) to validate their card.

If a guest cancels their reservation within your policy timeframe, give them a cancellation code for their records, and yours.

Your cancellation policy

If your cancellation policy is any different from the above, you risk getting chargebacks.

The cancellation policy only applies when your customer pays by Visa, Mastercard or JCB cards.

Taking advanced booking desposits

If you take advanced deposits under the Mastercard rules, this is the only amount you're allowed to take from the customer's card. You'll also give up your right to charge a one night's no show payment.

Operate a no-refund policy? You have to make the cardholder aware of this when they book.

Any customer refunds need to be credited to the card used for the booking – never give cash or cheques. Don't forget Maestro cards can only be used when the cardholder is present, as it has to be processed electronically using the magnetic stripe or embedded chip.

Guest arrival and check-in

When it comes to check-in, ask to see the card your guest made their booking with and ask them to fill in a registration form. Your registration form should point out any paid extras like newspapers, room service, and so on.

Pre-authorisation

After you've accurately estimated the value of the goods or services being provided, a pre-authorisation lets you estimate the final bill and reserve the funds on the card account while the guest is staying with you. It's sometimes called an 'estimated authorisation' and is something the cardholder needs to agree to beforehand.

Pre-authorisations have to be processed within 30 days for Mastercard transactions and 31 days for Visa. For Visa, any Incremental Authorisation Requests do not extend the 31-day timefame. To do this:

- estimate the final amount and get pre-authorisation
- tell your guest how much you've pre-authorised as this will reduce the funds they have available, explain that they've not been charged yet, and their final bill might be different to the estimate
- check the registration form and card signatures match up. Give the card's hologram and signature strip the once over, too – have they been tampered with?

Guest checking out early? Simply give them a refund. You'll find instructions in the operating guide for your processing equipment – everything from how to do a pre-authorisation using a Chip and PIN card, to processing refunds.

Pre-authorisation departures and check out

If you've pre-authorised an amount, you might not need to get another authorisation code when your guest checks out. This all depends on the final amount to be paid and the card scheme you're using.

For Visa transactions:

- you can use the code given at pre-authorisation if the final bill is within 15% of that amount
- but if the final bill is 15% above the pre-authorised amount you'll need to get another authorisation code for the difference

For Mastercard transactions:

- if the final bill is less than the estimated amount, you can go ahead and use the pre-authorisation code
- if the final bill is more than the estimated amount, you'll need another authorisation code for the difference

Express and priority check out

We're sorry, but if you have an express or priority check out service, we may not be able to defend you from a chargeback if a cardholder denies any transactions.

Extended stays

We'd recommend that you ask guests staying longer than two weeks to settle their bill. And if they need to stay longer, they can pay the current total due. Or you can use the card details they gave you at check in – although there's a risk the amount could be disputed at a later date without getting their signature or PIN. If their bill is more than 15% over their pre-authorised check in amount, get another code for the rest of their stay.

If your guest used a Maestro card or Mastercard and there are extra charges, get a separate signed and swiped voucher or printed document to prove the cardholder agreed to the charges.

Processing delayed or amended charges

Additional charges can be given to the cardholder after checkout for things like room charges, mini bar charges and breakfast on the last day. However, the cardholder must give their consent to receive them.

Delayed or amended charges must be processed to the cardholder's account within 90 days of the check-out date. We recommend these details are included in your Terms and Conditions to reduce the possibility of chargebacks.

You'll need to send a copy of the transaction receipt with 'signature on file' written in the cardholder signature box. You'll also need to send a copy of the Hotel Registration Form clearly showing the cardholder's signature and their acceptance of any additional charges being charged to their credit card account.

We recommend that you process additional charges separate with the cardholder's authority. This helps safeguard you from the total bill (including accommodation) being charged back.

To apply any additional charges to a Mastercard, a separate cardholder-signed authority must be given by processing a Card Present transaction. If the charge is disputed later, this will be used as proof that the cardholder knowingly authorised the charge.

Disputed transactions

If a transaction is disputed, it's essential for you to show that the card was present and authorised (if needed). Unless it's a contactless transaction, we won't be able to defend you from chargebacks if a PIN, signature or authorisation wasn't given.

The most common reasons disputed transactions are charged back for lodging or accommodation businesses are when:

- **the booking was made fraudulently with a card, so the guest doesn't show up**. This is usually because the fraudster's using your booking system to check the card is valid and funds are available. The genuine cardholder won't be aware it's been used until you charge them a no show fee
- **you don't reply to requests for information within 14 days**. In most cases, the card scheme just needs a copy of the final transaction receipt to show that the card was present and (except for contactless) the transaction was authenticated by the cardholder

But sometimes they might need a full breakdown of the charge. We'll always let you know what's needed when we get in touch.

Information and chargeback requests

If we let you know a cardholder is disputing a charge, make sure you always give us the right information to help us defend the challenge.

No shows

If the cardholder doesn't arrive or doesn't cancel their reservation, you can charge one night's stay to the card (at check out time) given when the reservation was made.

If this happens, send a copy of the transaction receipt with a copy of your Terms and Conditions to the billing address you've been given. 'No-show' must be clearly written in the space where the cardholder would usually sign the transaction receipt – this should also show the card number, expiry date and cardholder name. It's important your Terms and Conditions clearly show a 'no show' charge will be made for the first night of their booking.

When you charge for a no-show, you must send the transaction receipt, along with a copy of the invoice, to the cardholder. If you don't send these to the customer, the cardholder may dispute the transaction with their card issuer, which could lead to a chargeback to you.

Not got the cardholder's CSC code? The capture of CSC is mandatory for all Card Not Present transactions. However, Visa have made an exception to the rule for no show and delayed transactions. If your equipment doesn't let you bypass the CSC field for customer not present transactions, we recommend you select customer present and write 'no-show' on the signature line.

Express and priority check out charges

Got a dispute about an express or priority check out and you didn't get a signature? Please send us:

- a copy of the check-in receipt proving the card was present and you carried out a pre-authorisation
- a copy of their registration form with their signature and proof they agreed to the charge for their stay, plus any other relevant details

Other charges

If the cardholder disputes charges made after they've checked out – for minibars, breakfast and so on – please send us a copy of the receipt with 'Signature on file' written in the cardholder signature box. Include a copy of their registration form with their signature and proof they agreed to pay any extra charges and we will also need a breakdown of what the charges relate to.

For other handy hints on preventing chargebacks, check out **barclaycard.co.uk/business/chargebacks**. Or give our dedicated Chargeback team a call on **0844 755 0094** and we'll be happy to help.

Contact numbers

Customer services

0844 811 6666*

Monday to Sunday: 8am to midnight
Bank Holidays: 9am to 6pm (closed Christmas day)

We can answer questions about:

- extra processing equipment
- statement queries
- literature and point of sale materials
- information on products and services
- changing your details
- any other questions you have

PDQ Helpdesk

0844 811 6666*

Monday to Sunday: 8am to midnight
Bank Holidays: 9am to 6pm (closed Christmas day)

We can answer questions about:

- processing equipment faults
- PDQ transactions
- other queries about PDQ

Authorisation

0844 822 2000*

We can answer questions about:

- transaction authorisations over your floor limit
- suspicious card activity
- any concerns you have about card validity

Multiple mail and phone transactions

0844 811 4470*

Open 24 hours a day, seven days a week
(including Christmas day)

We can help:

- to authorise more than one mail or phone order at a time

Sales centre

0800 616 161*

Monday to Friday: 8.30am to 6pm
(closed weekends and Bank Holidays)

We can answer questions about:

- extending your existing or a new business

Chargeback department

0844 755 0094*

Monday to Friday 9am-5pm

We can answer questions about:

- chargebacks or retrievals

eCommerce Team

0844 822 2099*

Monday to Sunday: 8am to midnight
(closed Bank Holidays)

We can answer questions about:

- trading on the internet

Complaints handling

0844 811 6666*

Monday to Friday 9am-5pm

We can answer questions about:

- any problems with our service
- you can also visit **barclaycard.co.uk/paymentacceptance**

*Call charges may apply

Glossary and jargon buster

3D Secure

3Domain secure – the technology behind the internet authentication process. This covers the many domains involved during internet authentication, between us, you and the cardholder's issuer.

AAV

Account-holder authentication value – a unique reference generated by Mastercard and Maestro card issuers during the internet authentication process to prove authentication took place.

ACS

Access control server – the server used by the card issuer to manage the 3D Secure process.

APACs

Association for Payment Clearing Services – now known as UK Finance. This sets UK industry standards for payments.

BIN (Bank Identification Number) cache

A record of issuer BIN ranges stored on your authentication system. Update it regularly to make sure the local information on cardholders taking part in the scheme, and card issuers is correct.

Card acquirer

A financial institution – us for example – that is a member of a card scheme like Visa and Mastercard. Acquirers enter into agreements with merchants to process card transactions on their behalf and arrange to pay authorised funds.

Card issuer

A bank, building society or financial institution that issues credit or debit cards.

Card Not Present

Card transactions carried out when the cardholder isn't present, e.g. ones over the phone, online or by mail order.

Card schemes

A payment card organisation like Visa or Mastercard.

Card security code and address verification service

A service that confirms the cardholder's address, postcode and card security as part of the authorisation process.

CAVV

Cardholder authentication verification value – a unique reference generated during the 3D Secure process by Visa card issuers to prove authentication took place or was attempted.

Chargebacks

This is when a cardholder disputes a transaction on their statement. If it's a valid complaint, the transaction may be charged to us and passed on to you.

Chip and PIN

This is where a cardholder enters their unique 4-digit personal identification number (PIN) instead of signing a receipt. It's now standard technology in the UK and aims to reduce fraudulent transactions.

Chip cards

Payment cards with a built-in computer microchip that securely stores cardholder's information.

Code-10 calls

This is another name for a suspicious transaction.

If you're suspicious about a card or the person trying to use it, call our Authorisation Department straight away on **0844 822 200**. If the customer is with you and you can't talk freely, tell the operator you're making a Code-10 call – you'll then be asked questions and advised how to proceed.

Compromised card numbers (card number mismatch)

These are illegally copied numbers from genuine cards. Fraudsters encode the numbers onto the black magnetic stripe on the back of stolen cards, which look like the genuine article. The embossed number is usually different from the magnetic stripe details and shows up on processing equipment receipts, so make sure you cross check them.

Contactless transaction

A way for customers to pay (up to a certain amount) using near-field communications (NFC) technology – without entering a PIN or inserting their card into the device. Instructions are securely exchanged between a chip card (or other contactless device) and specially adapted point-of-sale processing equipment.

CRReq

Card Range Request – a type of 3D Secure procedure message used to find the BIN cache.

CRRes

Card Range Response – a type of 3D Secure procedure message containing the list of BIN ranges, which are part of the 3D Secure process.

Directory server (DS)

The servers hosted by the card schemes, Visa and Mastercard, containing details on the cardholders and card issuers signed up to 3D Secure.

ECI

eCommerce Indicator – confirms how protected you are during the internet authentication process for an online transaction.

Embossed cards

Cards with raised letters and cards, which can be felt and imprinted on paper if needed.

Encryption

The process of converting a message so it can't be read.

Firewall

Computer hardware, software and physical measures that prevent unauthorised access to and from a private network or server.

Floor limit

The card schemes set floor limits. If a transaction is over this, you'll need to get authorisation.

HPP

Hosted Payment Page – the web page used to collect the cardholder's credit or debit card details, hosted securely by another organisation.

HVP

High-value payments – if contactless limits go over the current transaction limit, they'll be classed as a high-value payment.

IAV

Issuer Authentication Value – this is a general term that corresponds to either the Visa CAVV or the Mastercard AAV. Both are unique references that are generated during the internet authentication process.

Internet, online or e-commerce transaction

Any transaction that's made by the cardholder over an electronic network, where the merchant isn't present.

Mastercard directory

This is a directory to show if a cardholder is taking part in an authentication scheme. If they are, the system will return the URL of the access control server to your 3D Secure service, you can then direct your cardholder to the right card issuer so they can authenticate their transaction or enrol in the scheme.

Merchant voucher summary (MVS)

This is the summary voucher that needs to be enclosed with the sales or refund voucher when they're paid into a Barclays branch or posted to the Financial Exceptions Department.

NFC

Near-field communication – a set of standards for two devices (e.g. point-of-sale processing equipment and a contactless card/device) to establish radio communication with each other by touching or bringing them close together.

PAReq

Payer authentication request – a type of 3D Secure procedure message. This is the message you send to the ACS containing relevant transaction details when the cardholder is redirected to the card-issuing bank for authentication or to enrol in a scheme.

PARes

Payer authentication response – a type of 3D Secure procedure message. This is the message returned to you by the ACS or card-issuing bank to confirm the outcome of the internet authentication process.

Payment service providers (PSPs)

Companies that offer facilities for processing online transactions, so businesses can trade over the internet.

PIN

Personal Identification Number – this is a unique 4-digit number that a cardholder uses to confirm they're the genuine cardholder.

Pop-up window

This is an internet browser pop-up window that's displayed in the main browser page.

Pre-authorisation

This lets you estimate the final bill (e.g. for hotel bookings or car hire) and reserve those funds on the card, so you can collect them at a later date.

Processing equipment

This is any item of payment-processing equipment, including PEDs (PIN entry device) you use to process face-to-face transactions.

Recurring transactions

This is when a customer gives you permission to take regular payments from them for goods or services that you'll supply over time (e.g. magazine subscriptions, insurance premiums). These can't be made with Maestro cards.

Retrieval requests or requests for information (RFI)

This is a request from a card issuer for more information or a copy of a transaction. If the transaction was over the phone or by post, you'll need to send them details of the cardholder's authority to take money from their account, along with a copy of the sales voucher or processing equipment receipt.

SecureCode

This is Mastercard's term for the 3D Secure internet authentication service they use to authenticate Mastercard-branded and Maestro-branded cards.

Server

A central computer that makes services and data available.

Split sale

When a transaction is split between more than one card, or a combination of card, cash and cheque.

Supervisor control

A plastic card or PIN code that lets you carry out supervisor actions on the device (e.g. to carry out the end-of-day banking procedure or to process a refund). This is supplied with your point-of-sale processing equipment.

Transaction laundering

This is – the not allowed – practice of processing someone else's card transactions using your merchant number. Doing this would break your agreement with us.

UCAF

Universal cardholder authentication field – that's the data field used by Mastercard and Maestro issuers to send the AAV.

VbV

Verified by Visa – that's Visa's term for their 3D Secure internet authentication service they use to authenticate Visa-branded cards.

VEReq

Verify enrolment request – a type of 3D Secure procedure message. That's the message sent to Visa or Mastercard's directory server to confirm if a cardholder's enrolled with the scheme.

We, us, our

Whenever we talk about 'we, us, or our', we mean Barclays Bank PLC and Barclaycard.

XID

This is a transaction identifier and is the reference used in the 3D Secure process to link the 3D Secure protocol messages together.

You, your

When we talk about 'you or your', we mean your business and the people in it (otherwise known as the merchant). Or it could be any agent or sub-contractor we've approved. If two people are classed as the merchant, you're both responsible to us individually and jointly.

This information is available in large print, Braille and audio, by calling 0800 161 5350

International calls will be charged at a higher rate. Please check with your service provider. Calls may be monitored or recorded in order to maintain high levels of security and quality of service.

BCD112079BROB1