worldpay
from FIS

CUSTOMER OPERATING INSTRUCTIONS

UK AND ROI

OCTOBER 2019

Contents

1 Your Customer Operating Instructions

Make the most of accepting payments through Worldpay with our Customer Operating Instructions.

This guide will help you:

- Accept card payments efficiently and smoothly
- Receive prompt payments to your bank account
- Protect your business by minimising the risk of fraudulent activity and threats. Understand your role in protecting your business from risk

The contents of the Customer Operating Instructions form part of your contract with Worldpay. It's also important that you make note of:

- Your current Worldpay Terms and Conditions
- Your Terminal User Guide
- Any prompts displayed on your payment terminal
- Any updates and specific instructions we send you from time to time

2 Important information

2.1 Your Customer Number

When you join Worldpay we will issue you with a unique Customer Number also known as the Merchant ID or MID. Your MID will be in your Welcome to Worldpay email / letter and on your monthly invoices. You will need to quote your MID whenever you write to us or call the Worldpay helpdesk or the Authorisation Centre.

2.2 Your contract with us

This document forms part of your contract with Worldpay. It covers the services we have agreed to provide to you and may include some others. Your application form (which also forms part of your Worldpay contract) shows which services you have requested.

You must ensure that you only accept payments for the goods and / or services that you told us your business provides, as detailed in your application form. Taking card payments for other goods and/or services without the knowledge and prior agreement of Worldpay may result in termination of your contract with us.

If you have any doubt about your contractual obligations after reading this document, we recommend you obtain legal advice.

2.3 Changes to your details

If your circumstances change or you change or update your details, you must notify us as soon as possible. All changes can be requested through Worldpay Dashboard or you can call us. You are required to notify us of any of the following:

- If you change the nature of your business – for example, if you start selling a different kind of goods or services, begin trading online or offer guarantees or warranties
- If you change your website address and / or intend to sell via a new website address.
- If you change the length of the guarantees or warranties offered on your products
- If you change the legal entity of your business – for example from sole trader to limited company
- Change to your bank account details
- Change of postal, trading address or registered address
- Change of trading name
- Change of email address
- Change of contact name
- Change of contact number
- If a partner / director / owner changes name
- If a partner / director leaves or a new partner/director joins
- If you open or close an outlet / site
- If you do not want to take all or any particular card product types issued in the EEA any more

Worldpay may suspend or withdraw some, or all of your card-processing facility if you do not let us know about any of the above changes.

2.4 Terminating your acquiring contract with us

If you have less than ten employees and an annual turnover and / or balance sheet under €2 million (or sterling equivalent) then you can give us one month's notice at any time to terminate your Worldpay contract for acquiring services. For customers who do not fit within these criteria, or where we have agreed to provide you with other products of services, different contracts lengths and termination rights may apply. Please review your contract(s) carefully.

If Worldpay terminates your contract, we will give you notice as set out in your applicable Worldpay contract. You are also legally required to return any equipment hired from us.

3 Payment security

3.1 General security information

- You must not store Sensitive Authentication Data (SAD) after authorisation, even if it is encrypted. This includes full magnetic stripe data, three or four digit security codes and PIN / PIN block information (this is the information relevant to the card and the cardholder contained within the chip). If you do not need the data (i.e. to meet specific industry regulations), do not store it
- You must not use card and verification details for any purpose other than completing the card transaction
- You must not pass this information to anyone else, except for the purpose of helping you to complete the card transaction
- You are only allowed to keep a separate record of the card number and expiry date, if both the following conditions apply:
  - You have the specific agreement of the cardholder, and
  - You are only going to use this information to help with future transactions, such as recurring payments or new orders believing further orders are likely
- You must give Worldpay current progress updates about your own PCI compliance when asked, so we can update the card schemes. Failure to supply this information could lead to receiving card scheme-imposed fines for non-compliance

3.2 Reducing fraud

This section will help you reduce your risk of losing money through fraud.

Card Present (CP) and Card Not Present (CNP) transactions have different risks associated with them and these need to be understood. CNP transactions carry a greater risk of fraud as you're unable to verify the purchaser. This can make your business susceptible to both credit card and chargeback fraud. If a CNP transaction is confirmed as fraud, the liability falls with you.

3.2.1 Important security tips

- Follow all the prompts on your terminal
- Be alert and aware – for card present transactions, if you are suspicious about a card or the person presenting it, contact the Authorisation Centre, select the option for a 'Code 10' call and follow the instructions provided by the Authorisation Centre
- Be discreet when you are suspicious – don't take risks with anyone's safety
- If your terminal has a supervisor card or code, keep it safe and secure and change the code regularly – anyone who has access to this could make fraudulent refunds to a card which may result in financial loss for your business
- Never allow a third-party to authorise or process card transactions using your facility – this would breach your contract with us and may result in withdrawal of your facility and/or card scheme fines. You will be liable for any fraud / chargebacks irrespective of the fact you have processed transactions on behalf of someone else

- Keep your terminal in sight during a transaction and take it back from your customer as soon as they have entered their PIN

Note: Authorisation does not guarantee payment. It simply means that at the time of the transaction the card has not been reported lost or stolen and that there are sufficient funds available. Find out more about Authorisations and referrals.

Card Present transactions	Card Not Present transactions: MOTO	Card Not Present transactions: eCommerce
These are face-to-face transactions, such as chip and PIN, where your customer and their card are present at the point of sale.	These are transactions where your customer and the card are not present at the time of the transaction.	These are sales over the Internet (including from retailer apps on mobile devices) where the customer and their card are not present at the point of sale.

3.2.2 Training your staff

Alert, well-trained staff members are your front line defence against card fraud and can significantly reduce the risk of financial loss to your business. Ensure that your front line staff are trained on properly handling terminals and that your on-site controls are strong. This includes ensuring that front line staff keep terminals on-site during a transaction. Please make sure your staff read this guide carefully, and any other fraud prevention publications we send you.

Transaction Monitoring

Our Transaction Monitoring Team will contact you with any concerns about transactions you have processed. As part of our merchant account risk review, we can request documentation in order to understand the basis on which funds will be paid to you and your business.

Withholding payments

We may withhold payments from your business while we complete our investigation into whether a genuine transaction has taken place that relates to goods and services provided by your business. We aim to complete investigations in a timely and efficient manner, but there is no set time for our investigation to be completed.

3.2.3 Card present transactions

These are face-to-face transactions where your customer and their card are present at the point of sale. Find out more in Using your terminal.

Look out for the warning signs

Be aware of how customers normally behave when they are shopping. If you notice anything out of the ordinary, or something that just doesn't feel right, it could be a sign of potential fraud. Act on your instincts and don't go ahead if you are suspicious. Look out for:

- Random, careless or bulk purchases – most customers ask questions and, for example, try on clothing, but a fraudster will just buy goods that can be easily re-sold
- Rapid repeat visits – a customer who returns to buy more in a short period of time may be making the most of the fact that the card has been accepted already
- Nervous or hurried customers – they may be worried about being caught
- Cards signed in felt-tip pen – this can be used to disguise the original signature – remember all cards should be signed in ballpoint pen
- Interruptions – a customer who tries to distract you during the transaction, and who seems familiar with how the authorisation process works, may be trying to prevent you from noticing something suspicious. Never turn your attention away from the terminal once you have started processing the transaction, as you may miss prompts on the screen, or miss a fraudster attempting to interfere with the terminal
- Fake authorisation calls - neither Worldpay nor the card issuing bank will EVER call you during the processing of a transaction to provide you with an authorisation code. If this happens it will be an attempt by fraudsters to force through a transaction, and will result in a loss to your business if the transaction is charged back. If you receive one of these calls please cancel the transaction (if safe to do so) and perform a 'Code 10' call
- Worldpay, Police or other 'official' impersonation – you will never receive a phone call from the Worldpay Authorisation Centre, the police, your terminal provider or any other official, requesting you to provide any card details over the phone. None of these organisations will ever ask for details over the phone, so these will be an attempt by fraudsters to gain card details from you. If you receive one of these calls, please report it immediately to the Worldpay helpdesk
- A shopper who repeatedly uses a contactless card or cards or makes multiple low value purchases where you would normally expect them to pay in one go

Take extra care when a signature is needed

Not all cards have chip and PIN, these need to be verified using a signature. Knowing when these cards can be used and their security features will help you to identify genuine transactions and spot potential fraud. You could be financially liable if a transaction is confirmed as invalid or fraudulent. In certain circumstances, you can accept:

- Chip and signature cards – you should only use a signature to verify a transaction in exceptional cases. The main ones are if the customer has a non-UK-issued card, or an impairment that means they need to sign. Follow the prompts on your terminal
- Magnetic stripe and signature cards – these will mostly be non-UK-issued cards from countries that have not yet upgraded to chip and PIN. Follow the prompts on your terminal

Fraud Checklist for Signature Verification

If you do carry out a transaction using a signature as verification, you should take extra security precautions:

- Check the security features of the card. Find out more in our Card recognition guide
- Check the cardholder's signature matches that on the back of the card
- If possible, check that the spelling on the card is the same as the signature – fraudsters sometimes don't spell the name correctly
- Check the title on the card matches the gender of the person presenting it
- Check the signature strip for tampering – has another strip been placed over the top of the original one? If the word "void" appears on the strip, this could be an indication that the genuine signature has been removed and a substitute used
- If you have an ultraviolet (UV) lamp, put the card under it and check the appropriate inbuilt security feature
- While the point-of-sale receipt is printing, check the last four digits of the card number on the receipt match those on the front of the card. If they don't, make a 'Code 10' call

Retaining a card

If the Authorisation Centre asks you to keep a card explain politely that the card issuer has asked you to do so. Your own company policy will decide whether you detain the cardholder or call the police. Never put yourself, your staff or the public at risk.

If the Authorisation Centre does not ask you to keep the card, you may decide that a card or a transaction is suspicious – for example, if you have identified it as counterfeit. Card thieves act fast, and will often try to use a card before the owner notices that it has gone.

There may be a reward for recovering a card that is being misused.

Preserving evidence

Treat a withheld card with care. The police will require it as evidence, and use it to catch and prosecute the thieves.

If staff come into contact with criminals, it is far better – and less stressful – if they are prepared for the possibility and have an agreed process to follow.

Staff should follow these instructions as well as those in your own policy.

Preserve the card:

- Don't cut the card in half
- Handle it by the edges so as to preserve fingerprints
- Cut off the bottom left-hand corner (as seen from the front) – don't cut it in half
- Don't damage any other part of the card
- Handle it as little as possible and place it in a plastic bag or envelope until you can give it to the police

Keep the voucher or receipt:

- Keep the best copy possible
- Don't pin or staple anything to it
- Put it in the same envelope / bag as the card to give to the police

Keep the video / CCTV:

- If you have a video surveillance system, keep the tape and give it to the police.
- Keep a copy if you can

Note down a description of the person who presented the card:

- Write down the details immediately while they are fresh in your memory
- Think about the person's unique features such as their accent, scars, tattoos and body language rather than the clothes they are wearing

Involving the police

If your company policy dictates, inform the police via Action Fraud.

If the police ask for the card you should:

- Allow the Police Officer to take it
- Take a note of the officer's name, number and station
- Obtain the Crime Reference Number
- Get a receipt and keep it safely as this may enable you to claim a reward

If someone leaves a card behind

- Keep it somewhere safe for at least 24 hours, in case the cardholder comes back for it
- If someone comes to claim the card, ask them for signed proof of identity, such as a driving licence or other cards, and compare the signatures
- Ask them to sign a blank receipt and compare the signatures. Then destroy the receipt. If you are then happy with the cardholder's identity, give them the card
- If you are suspicious, ask them to come back with additional proof of identity, such as passport or driving licence. If you are still not satisfied when they come back, call the Authorisation Centre and select the 'Code 10' option. Our operator will talk you through the process
- If the cardholder does not return to reclaim the card, please send it to us to be cancelled. Looking at it; from the front, cut off the bottom left-hand corner. Do not cut through the signature strip, magnetic stripe, hologram or chip. Then send the pieces with a short note giving your address and the date you found the card to:

Card Rewards Section
Gateshead Card Centre
5th Avenue
Gateshead
NE11 0EL
United Kingdom

Rewards

Depending on the circumstances, there may be a reward for cards you hold on to when asked by the Authorisation Centre.

Return these cards to:

Card Rewards Section
Gateshead Card Centre
5th Avenue
Gateshead
NE11 0EL
United Kingdom

When you send the card, please also provide the following information:

- The name and address of your business
- Your Customer Number and telephone contact details
- The date on which you kept the card. The name on the card
- The card number (the long number across the centre of the card). Details of the person who should get any reward

If the police take the card as evidence, include the Police Officer's details in the above list plus the date reported and the Crime Reference Number. Keep a copy of these details.

3.2.4 Card Not Present transactions (CNP)

If become suspicious at any time we recommend you do not continue with the transaction or send out the goods. If you have already processed the transaction, you will need to make a refund to the card. See Refunds.

For international cards there may be a currency difference between the sale and refund due to exchange rates, and you may be liable for this difference if a chargeback is raised. Contact our helpdesk for clarification before issuing a refund.

CNP transactions are considered high-risk because you have no opportunity to physically check the card or meet the cardholder. Although most CNP sales are genuine, this type of transaction is appealing to fraudsters. Take extra care with CNP payments because you will be financially liable if a transaction is confirmed as invalid or fraudulent.

Look out for the warning signs (Mail Order Telephone Order)

Here are some signs that a transaction is likely to be fraudulent. Get to know them and make sure that all members of your staff recognise them too. Sometimes the first sign of fraud can just be a general feeling that something isn't quite right. Act on your instincts and don't send out the goods until you've carried out further checks.

- Multiple or bulk orders – be vigilant for customers buying lots of the same item – either in the same transaction or separately
- First-time customers who place multiple orders – the risk of fraud is smaller when dealing with customers you know
- High-value orders – orders larger than normal may indicate fraud. High-value items such as jewellery or electrical goods are often targeted by fraudsters because they are easy to resell, so take extra care with this type of transaction. Ensure that you obtain ID from your customer, such as passport or driving licence
- Hesitant customers – customers who seem uncertain about personal information, such as their postcode or spelling of their street name, could well be using a false identity. Also look out for customers being prompted when giving the requested information
- Same name, different title – could your customer be using the card of a family member?
- Sales that are too easy – be suspicious if a customer is not interested in the price and / or detailed description of the goods, but is only interested in delivery times
- Suspicious card combinations such as:
  - Transactions on several cards where the billing address matches but there are different / various shipping addresses
  - Multiple transactions on a single card over a very short period of time
  - Multiple cards beginning with the same first six digits (card BIN) offered immediately after the previous cards are declined
  - Customer offering multiple different cards one after another without hesitation when previous cards are declined
  - Orders shipped to a single address but purchased with various cards
  - Requests for urgent delivery – this could be genuine, but rush orders are common in fraud scams that aim to obtain goods for quick resale before the card is reported stolen
  - Overseas shipping address – be careful when shipping overseas, especially if you are dealing with a new customer or a very large order
  - Different shipping address – orders where the shipping address is different from the billing address may be legitimate (for example, when sending flowers or a birthday present) but requests to send goods to hotels, guest houses or PO boxes are often associated with fraud
  - Duplicate shipping address – has the shipping address been used previously for similar orders? Be cautious if you identify the same delivery address being used
  - Requests to send funds abroad – this is typically a request for money transfer or other payment method to pay for couriers, interpreters or other similar services or requests. For example, a request to take a

payment greater than the value of the goods / services being purchased, where the customer requests the surplus funds to be sent overseas or to another bank

Note: Authorisation does not guarantee payment. It simply means that at the time of the transaction the card has not been reported lost or stolen and that there are sufficient funds available. Card thieves act fast and will often try to use a card before the owner notices it has gone. Find out more about Authorisations and referrals.

Look out for fraud warning signs (eCommerce)

Here are some signs that an eCommerce transaction is likely to be fraudulent:

- A risk alert from the payment service provider or acquiring bank / issuer. This indicates that there is a cause for concern and that further checks are required before an order is fulfilled
- Multiple transaction attempts using the same or similar shopper details, such as name, email address or IP address across one payment
- Different shopper details with one element the same – such as ten transactions from the same IP address giving different shopper names and email addresses
- Multiple cards used by the same shopper, especially where the card numbers are similar
- Obvious 'card testing', where the last four or eight digits of cards in a series of attempted payments contain similar numbers, or the card numbers are cycled repeatedly in a rough pattern or sequence
- Nonsensical shopper details, such as 'dgsgsgdf@dsgsd.com' as a shopper email address or 'gdfgdfgfg' as a shopper name or billing address
- High-value transactions, especially where the amount is out of the ordinary for your usual daily processing amounts
- Mismatching Card Security Code (CSC) or mismatching Address Verification Check (AVS). Consider rejecting orders that carry mismatches or carry out further checks
- Mismatching combination of billing country, issuer country and IP country, especially, but not limited to, instances where the payment details are from any country or area which is associated with high risks of online fraud
- A delivery country that's out of the ordinary for your business and regarded as high-risk
- Use of 'freemail' email addresses, such as Yahoo!, Hotmail, MSN, Gmail, Live or YMail. Although these email services are completely legitimate, they are often associated with fraud attempts because they are easily available and relatively anonymous
- An email address that bears no relation to the shopper name
- A request to hurry the order shortly after it has been placed

- Multiple purchases of the same item which might otherwise be considered unusual e.g. 15 pairs of shoes. Typically a fraudster is looking to sell the items they obtain
- Indiscriminate buying or unusually large orders that seem out of the ordinary
- A request to change the delivery address, especially to a high-risk area / country (see above).
- Shoppers who give card numbers by email and seem reckless with sensitive information. Sending full card numbers by unencrypted email is not PCI DSS compliant
- Shoppers who give a high number of card details or lots of different billing information
- A request to conceal or alter payment details, or the way in which the payment is made, to make it look more legitimate
- General inconsistency between the shopper's name, email address, or the way they communicate and the kind of goods or services being purchased

How to combat eCommerce fraud

Here are some important ways to help reduce the exposure of your business to fraud:

- Make the most of up to date industry tools like cardholder authentication, 3D Secure (Mastercard Identity Check, Visa Secure and American Express Safekey), CSC and AVS checks. Ask the Worldpay helpdesk or your Payment Service Provider (PSP) for more information
- Screen transactions and consider applying risk scoring and alerts to flag suspect activity that merits further checks. You may be able to design your own in-house system – or ask your PSP
- Compare new shopper information to data you already hold. Keep records of previous fraud attempts and chargebacks and reject orders where there are matches
- Look for patterns such as similarities between transactions and repeat use of the same shopper name, email address or IP address – and investigate anything suspicious
- Verify the shopper's identity if you are suspicious. Test their contact details to see if they work – send an email and call the telephone number. You may also ask for copies of utility bills, card statements, passport or driving licence (with any sensitive details obscured)
- Establish a fraud policy setting out what should be done if fraud is suspected and ensure that all members of your staff are trained to act

What else to consider

- Establish authenticity of customer. It's advisable to establish the authenticity of a customer before delivery by obtaining residential address, telephone number, etc. – perhaps checking with data that is available publicly
- Search the Internet for imposters. We recommend that you regularly search the Internet for websites using similar names to your own. These may have been set up to impersonate your company illegally
- A number of companies, such as PSPs, provide services to help you to look out for potential fraudulent transactions. Fraud-screening measures include:
  - Parameter-based technology to filter card transactions
  - Third-party name-and address-checking techniques

  - Methods of validating cardholder data
- Consider the use of fraud prevention software / tools, the benefits often outweigh the cost involved

To find out more about how we can help and Worldpay's fraud prevention products, contact us, alternatively get in touch with your PSP.

Additional security

We recommend you use the Card Security Code (CSC) and Address Verification Service (AVS) available through your terminal.

If we have supplied your terminal, you will be prompted for the information needed to make the additional checks – if you have any other terminal, speak to your supplier to find out how to take advantage of these.

These additional checks cannot confirm cardholder names. Take additional steps if you are in any doubt about the transaction.

One option would be to request a landline number and check with a directory enquiries service.

Please be advised that although these measures may help in cutting back on fraud, if the cardholder raises a chargeback for fraud you may still be liable.

Delivery

There are also opportunities for fraud at the delivery stage. It is important you have policies to reduce this type of fraud. Here are a few recommendations that may help:

- Make sure that goods are always delivered to the billing address (preferably inside your customer's premises) and to the person set out in the order
- Obtain a signature from the cardholder as proof of delivery – this can be used as evidence in the event of a dispute
- Don't release goods to third parties such as friends or relatives of the cardholder, taxi drivers, couriers not arranged by your business, messengers, etc
- If using your own staff for delivery, consider using a mobile terminal (see our website for details of our mobile card machines) to enable you to take the transaction as card present when the goods are delivered
- If a cardholder changes their mind and wishes to collect the goods, they should attend your premises in person and produce their card. You must either cancel or refund any previously completed CNP transaction and process a new card present transaction

3.2.5 Refund fraud

Stolen terminals present a significant fraud risk. When a terminal is stolen, all of the payment data within it can be used to process refunds to any card.

Reduce your exposure to refund fraud by following these guidelines:

- Remove refund functionality on portable devices

- Allow only fixed terminals on-site to process refunds. Alternatively consider only allowing refunds to be processed by specific sites, locations or offices where it makes sense for your customers
- Check that all terminals are accounted for regularly. Fraudsters use distraction techniques to obtain portable devices and even replace them with duplicates to avoid immediate detection
- Ensure that your front line staff are trained on properly handling terminals and that your on-site controls are strong. This includes ensuring that front line staff keep terminals on-site during a transaction
- Power down the base stations for the affected device as soon as a theft is realised and inform the Worldpay helpdesk immediately

3.3 PCI DSS

Keeping cardholder data secure is crucial to reducing the risk of fraud and being a responsible customer.

The PCI Security Standards Council (PCI SSC)[1] sets out twelve mandatory information security requirements to help make sure that sensitive cardholder information remains safe at all times.

The requirements apply to any organisation or customer, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data, even if a 3rd party processes transactions on your behalf. You are required by your contract with Worldpay to comply with the PCI Data Security Standard requirements and to certify your compliance annually. You must update your compliance in line with any changes to your business as they happen.

As a card acquirer, Worldpay has a responsibility to report our customers' PCI DSS compliance status to the card schemes (including Visa and Mastercard) on a quarterly basis. Any customer who does not comply runs the risk of fines from the card schemes. A monthly non-compliance fee is charged by Worldpay if a customer is not compliant within 60 days of joining us.

In addition, customers who suffer a data breach may be subject to fines being levied by the card schemes for the loss of card data, associated fraud spend, loss of business and reputation. There are also fines for storing Sensitive Authentication Data (SAD) post-authorisation e.g. the 3 digit security code on the back of the card.

[1]The PCI SSC is formed by Visa, Mastercard, American Express, JCB and Diners/Discover

In addition to confirming your compliance annually, you must ensure that this degree of protection is maintained long term. PCI DSS is intended to protect your business and customers against real data security risks – it is not a box ticking exercise.

3.3.1 PCI DSS Levels

Customers are classified between PCI level 1 – 4 depending on the nature of their business and volume of transactions processed. See below for details of the levels and associated PCI accreditation requirements. You can find a step-by-step guide for Levels 1 - 3 below.

For Level 4, customers can use Worldpay's SaferPayments programme to confirm compliance with PCI DSS. SaferPayments has been designed to give businesses a helping hand through the Payment Card Industry Data Security Standard (PCI DSS) certification process.

Level 1 – Customers processing more than 6 million Visa or Mastercard transactions a year of which less than 20,000 are eCommerce:

- Annual on-site audit carried out by a Qualified Security Assessor (QSA), providing a Report on Compliance (ROC)
- Quarterly vulnerability scan by an Approved Scan Vendor (ASV)
- Attestation of Compliance Form

Level 2 – Customers processing between 1 and 6 million Visa or Mastercard transactions a year:

- Annual on-site audit carried out by a QSA providing a report on Compliance (ROC), or an Annual Self Assessment Questionnaire (SAQ) if carried out by an Internal Security Assessor (ISA)
- Quarterly vulnerability scan by an ASV
- Attestation of Compliance Form – part of the SAQ

Level 2 customers that choose to complete an annual SAQ must ensure that staff engaged in the Self Assessment attend PCI SSC Internal Security Assessor training. Staff must pass the associated accreditation programme annually in order to continue the option of Self-Assessment, for compliance validation. Alternatively, Level 2 customers may, at their own discretion, complete an annual on-site assessment conducted by a PCI SSC approved QSA rather than complete an annual SAQ.

Level 3 – Any customer processing 20,000 to one million Visa or Mastercard eCommerce transactions per year:

- Annual SAQ.
- Quarterly vulnerability scan by an ASV - if applicable
- Attestation of Compliance Form – part of the SAQ

Level 4 – Any customer processing up to one million Visa or Mastercard transactions per year of which less than 20,000 are eCommerce:

- Annual SAQ (recommended)
- Quarterly vulnerability scan by an ASV - if applicable

Level 4 customers have access to Worldpay SaferPayments to help them through the process of certifying compliance with PCI DSS. We also offer SaferPayments Plus - a managed service where Worldpay will proactively guide you through PCI DSS compliance. To find out more, visit our SaferPayments website.

SaferPayments are open weekdays from 8am to 8pm Monday to Friday and 9am to 5pm on Saturday.

UK 0330 808 0663

ROI 1890 989 575

3.3.2 About the annual on-site audit

The annual on-site audit is an independent risk assessment, usually carried out by a Qualified Security Assessor (QSA), who follows a standard testing procedure, built around the 12 PCI DSS requirements. If you have a security consultant to complete on-site reviews, they may be able to carry out the PCI DSS on-site audit. In some cases your own staff can complete the audit.

To find out more, visit our SaferPayments website.

3.3.3 About the quarterly vulnerability scan

A vulnerability scan checks that your IT systems are protected from external threats, such as hacking or malicious viruses. The scanning tools test your network equipment, hosts, and applications for known vulnerabilities. Scans are intended to be non-intrusive, and are conducted by an authorised network security scanning vendor.

Regular quarterly scans are necessary to check that your systems and applications continue to provide adequate levels of protection. Any vulnerabilities need to be addressed and a follow-up scan conducted to ensure that the remediation was successful.

For a current list of providers, go to the PCI SSC website.

3.3.4 Obligations of your service providers if you do not store card data on your own systems

Even if you do not store any cardholder account data in your own systems, you must still verify the PCI DSS status of any third parties who act on your behalf to store, process or transmit your customers' cardholder data. In accordance with the relevant PCI DSS requirements, you are responsible for monitoring the PCI DSS compliance of all third-party service providers you use who have access to cardholder data (including to possess, store, process or transmit it on your behalf), and / or who could impact the security of your cardholder data environment. Third-party service providers include:

- Resellers
- Software application providers
- Acquirers
- Payment Service Providers (PSPs)
- Card processing bureau

- Data storage entities
- Web hosting providers
- Shopping cart providers
- Miscellaneous third-party agents
- Software vendor

3.3.5 Level 1, 2 and 3 customers

A step-by-step guide

To implement PCI DSS you will need to:

- Find out more about the way your business handles card payments
- Determine whether your business handles cardholder data securely
- Put a remediation plan in place to address any associated data security risks

This step-by-step guide will help you to do this in a way that is manageable for your business. PCI DSS is intended to protect your business and customers against real data security risks – it is not a box ticking exercise.

Step 1: Get to know PCI DSS

Your first step should be to read and understand the full details of the Payment Card Industry Data Security Standard (PCI DSS) and its 12 mandatory requirements. To see the full and latest version, visit our SaferPayments website.

Step 2: Map all data flows in your business

Once you are familiar with PCI DSS, we recommend you put a project team in place within your business. This team's immediate priority should be to analyse the way that card payments are processed in your business and to map out all the related data flows.

This analysis must:

- Identify any systems which store cardholder data
- Identify which of these systems are under your direct control

Depending on the size and type of your business, at least some of these systems may be under the control of a third-party service provider or vendor – such as:

- Till vendor
- POS vendor
- Integrated solution provider
- Internet Payment Service Provider
- Payment gateway provider
- Web hosting company

Your business is responsible for the activity of these service providers. All third-parties who are involved in the handling of cardholder data must be compliant with the requirements of the Data Security Standards.

Once you have completed Step 2, you should be in a position to:

- Ensure all your service providers comply with PCI DSS:
  - To find out more, go to Step 3
  - If you do not work with any service providers, go straight to Step 4
- Implement PCI DSS compliance within your own business. To find out more, go to Step 4

Step 3: Check and monitor the status of your service providers

You are responsible for monitoring the PCI DSS compliance of all third party service providers who have access to your cardholder data (including to possess, store, process or transmit it on your behalf), and / or who could impact the security of your cardholder data environment.

If data becomes compromised by a service provider you work with, you can be held responsible for any associated costs.

Because cardholder data security is so important for the payment card industry, it is likely that your service providers will know about PCI DSS. Many service providers are already compliant; others have a formal programme in place to become compliant. Service providers should register to complete their PCI DSS compliance.

For a current list of service providers that are compliant or working towards compliance, see 'Procedures and Guidelines' on the PCI SSC website.

If your service providers are not on this list, you need to ensure that they take action toward becoming compliant.

Worldpay may seek your support and intervention during Step 3. For example, we may ask you to take certain steps to ensure that a particular service provider you work with is on track to becoming PCI compliant.

Step 4: Conduct a gap analysis and scope the project

Having mapped out the data flows in your business, you should have identified any of your systems that store, process or transmit cardholder data. With these systems as your primary focus, you should:

- Assess how much remediation work may be required to comply with PCI DSS
- Assess what resources are needed, and how long this work is likely to tak
- Consider putting a project team in place and discuss respective roles and responsibilities - including communicating with us and your service providers, specifying technical changes, establishing training needs, etc

At this stage you should consider whether to engage the services of a Qualified Security Assessor (QSA) a specialist auditor, certified by Visa and / or Mastercard to help you achieve PCI DSS compliance. Some customers appoint a QSA from the outset. Others prefer to carry out the initial scoping work internally and bring in a QSA later for a more thorough review.

Visit the PCI SSC website for a current list of QSAs.

Step 5: Select your validation option

There are different ways to test and validate your compliance with PCI DSS, depending on the size of your business and how your card acceptance systems are set up.

Visit the PCI SSC website for further details.

Step 6: Plan and implement remediation

Choose your validation option and determine your need to carry out a more thorough gap analysis. Then you can develop a full remediation plan to become PCI DSS compliant.

Your remediation plan can be developed by your own team, or you can appoint a Qualified Security Assessor (QSA) to provide an independent perspective.

It's important to remember that the underlying aim of PCI DSS is the security of your business and of customers' data, not the compliance process.

Give individual members of your project team specific remediation activities and agree acceptable timelines. Some activities may depend on a third party or vendor becoming compliant, whilst others can be undertaken internally.

We recommend that you begin any remediation work on your own systems as quickly as possible. By doing whatever you can as soon as you can, you take a vital step forward in protecting your business and customers against the risk of data compromise.

Step 7: Certification

In order to go through the final certification stage, your business will need to:

- Complete the remediation of all systems under your control
- Confirm that all your service providers are fully compliant – and that their compliant products and services have been implemented within your own card acceptance systems
- Complete an SAQ or appoint an independent QSA (depending on your business' PCI level)

Once certified, confirm to Worldpay that you have achieved compliance. We will, report your status to the card schemes where this is required.

As well as protecting yourself against many associated business risks, you will be able to confirm your compliance in your own messaging and marketing collaterals.

Staying compliant

PCI DSS compliance is about understanding your risks and meeting the requirements of the standard to ensure you are protected. If you make any changes or additions to your business' card payment methods, such as opening a new type of outlet, then you must update your PCI DSS certification accordingly.

You must remain compliant and complete an on-site audit every year, and a vulnerability scan every quarter. We recommend you put business processes in place to maintain compliance, including:

- Reviewing your access control policy regularly
- Integrating vulnerability scans into your regular business routine
- Ensuring that any new systems or applications are fully compliant
- Creating procedures to make sure your anti-virus systems are regularly updated

You should also ensure that your service providers continue to be PCI DSS compliant and incorporate relevant clauses into your contracts with them to require this.

4 Transactions

4.1 Using your terminal

4.1.1 Point of Sale requirements and display material

Before you begin to accept card payments you will need to take a few steps to ensure your customers are aware that they can use them at your shop or business.

You can now choose to accept only some of a card scheme's card product types such as personal prepaid, debit or credit cards or commercial cards (i.e. as used by businesses) which are issued in the European Economic Area (EEA). However you must accept all of the card product types that are issued by that card scheme outside of the EEA.

You are required by card scheme rules to clearly display at your shop entrance and point-of-sale counters the card product type(s) you have chosen to accept.

Within the EEA, you are not permitted, for most card transactions, to add a surcharge to the value of the goods or services sold[1].

Display materials are available for your business to show your customers which card product types you accept. Use the decals in your Welcome Pack if you accept all card product types for a particular card scheme.

You can order POS display material at Worldpay Accessories or call us:

UK customers: 0800 289 666 (Freephone)

ROI customers: 00800 9899 2000 (International Freephone)

If you only wish to accept some EEA issued card product types you can download your required point- of-sale display materials from the relevant card scheme directly. Use the links below:

Visa
Mastercard / Maestro

[1] EU regulations for merchants within the EEA mean they are no longer allowed to surcharge consumers on regular debit and credit cards, except if the card is an unregulated commercial card or a card issued outside the EEA, and only if local country law permits it.

JCB
Diners / Discover
Amex

The card scheme names – Mastercard, Visa, Visa Electron, JCB, Diners / Discover and Maestro – and their associated decals, signage, symbols and logos are registered trademarks. As one of our customers, you are allowed to use them in your advertising, as long as you follow their guidelines. If you want to use American Express trademarks you must ask them directly for permission.

4.1.2 Using your terminal

If your terminal is supplied by Worldpay you'll need to make sure that it is connected and powered on at all times. This is critical for your terminal to receive software updates. These are needed to ensure your terminal is updated with the latest software including compliance updates in line with payment regulations.

Terminals supplied by Worldpay automatically connect to our Terminal Management System (TMS) using 0800 telephone numbers with the exception of IP broadband or mobile terminals. These terminals connect directly over the internet similar to a computer. This happens every 28 days and the calls usually last between 2 – 5 minutes. You will also get additional software updates, normally two per year, which can take between 30 minutes and 2 hours to complete depending on the size of the update and the strength and speed of your connection.

Terminal Management System (TMS) update costs

The type of connection your terminal uses to connect to the TMS will affect the costs associated with software updates. When using an IP broadband or mobile connection your call costs are free, as you will not be charged any additional fees by Worldpay over and above any monthly IP connection fee. The table below details charges which will be based on connection type and the duration of the call for the software update.

You will only be charged one payment, billed by your telecoms company, which is made up of two charges.

Terminal type	Call costs	
	Service charge	Call charge
Standard dial-up phone line (PSTN)	Maximum of 7p per minute	Standard connection cost for 0800 numbers[1]

[1] Current as at 15 November 2016

Terminal type	Call costs	
	Service charge	Call charge
IP broadband connection	No charge	No charge
Mobile terminal	No charge	No charge

If you use one of our Worldpay terminals, we recommend that you use an IP broadband or mobile connection. To find out more about how to convert your existing terminal to one with a IP broadband connection, contact us on 0345 761 6263 (UK) or 1 800 24 26 36 (ROI).

Please refer to Ofcom call costs guide for the latest minimum and maximum charges.

4.1.3 Card present (CP) transactions

CP transactions are also known as face-to-face transactions, as your customer pays with their card at the point of sale (POS).

Step-by-step guide (chip and PIN)

1. Follow the terminal prompts and key in the full amount of the transaction.
2. Ask the cardholder to either insert their card into the chip reader slot on your terminal or separate PIN entry device.
3. If you offer a Purchase with cashback transaction service you can find more about the process here.
4. Your terminal will now usually ask the cardholder to enter their PIN. If it doesn't, this could be because the cardholder has a card that does not support chip and PIN technology (such as a chip- and-signature or magnetic-stripe-and-signature card). Your terminal will advise which method is required – always follow the prompts on the terminal.
5. Ask the cardholder to check that the transaction amount is correct and to enter their PIN.
6. Most terminals will then authorise the transaction automatically. If the terminal prompts you, call our Authorisation Centre immediately and follow the instructions. Find out more about Authorisations and referrals.
7. Wait for the terminal to print out a terminal receipt.
8. Only give the cardholder the goods they are buying when you have received authorisation and completed the transaction. If authorisation is not given, do not go ahead with the transaction. Ask your customer for an alternative payment method.
9. Ask the cardholder to take their card from the terminal and give them their copy of the terminal receipt.

Things to remember:

- Keep your copy of all terminal receipts in a secure fireproof place for at least 13 months in case there is a query later or these details are required to help defend a chargeback. Do not alter them in any way. If there is a dispute, the cardholder's copy will normally be taken as correct
- Remember that even where authorisation is given, this is no guarantee of payment and the transaction is still open to being charged back
- Customers are not permitted to use any terminal outside of the country in which they received it

Accepting contactless transactions

Contactless is a standard method of payment. Contactless cards enable purchases to be completed by tapping the card over a contactless reader on an enabled terminal.

The benefits of using contactless are:

- Improved customer payment experience
- Faster transactions
- Helps retailers to remove cash from their business

There are also other consumer contactless devices such as mobile phones, wristbands and key fobs. These work in the same way as a card. The contactless payment is made by waving the contactless consumer device over a contactless enabled terminal.

If a card has the following symbol it can be used for contactless payments:

To provide additional security and protect both consumers and retailers, the contactless transaction will occasionally be disabled. A prompt for a chip and PIN transaction will appear on the terminal. This is a normal action which has been; built into the system.

Note: The contactless option is only available where the terminal has been activated for contactless. If your terminal has not been activated, please contact Worldpay and we will be happy to advise how you can offer contactless payments to your customers. Please note that all terminals must be able to accept contactless payments by 1st January 2020 in line with card scheme rules.

Step-by-step guide:

1. Key the full amount of the transaction into the terminal.
2. The terminal will prompt for either a card to be presented, inserted, or swiped against the contactless reader[1].
3. Ask the cardholder to check the amount. If cardholder has a contactless card (check for contactless symbol – see above), the cardholder will be able to tap the card against the contactless reader. A PIN is not required to be entered when a contactless transaction is made.
4. All contactless payments will need to be authorised. Most terminals will process the authorisation request automatically. Do not be confused by the 'beep' from your terminal as this simply indicates that the card or mobile payment device has been 'read' by your terminal and is unrelated to authorisation. Your terminal will display a message showing whether the transaction has been authorised or declined. If declined, you will need to ask your customer for a different payment method.
5. Wait for the terminal to print out a receipt, if requested by the cardholder.
6. Only provide the cardholder with the goods, or services they are purchasing when you have received authorisation and completed the transaction.

When a signature is needed

You should only use a signature to verify a transaction when prompted by your terminal. Extra security checks

Where using a signature as verification, you should take the following extra security precautions:

- Make sure the card is not damaged, cut or defaced in any way
- Check the signature strip for signs of damage or tampering
- Check any specific security features for that card. Find out more in the Card recognition guide
- If you are unsure make a 'Code 10' call. Find out more about Reducing fraud

Step-by-step guide (when a signature is needed)

1. Following the terminal prompt, key in the full amount of the transaction.
2. Insert the card and follow the terminal prompts which will tell you when a signature is required.

---

[1] Whilst the no-verification contactless limit is set at £30/€30, High Value Contactless for transactions above this value has launched. This allows consumers to tap and pay with their smartphones for any value just by using on-device verification (e.g. security code/PIN, fingerprint recognition, etc.) on their mobile phone. For High Value Contactless transactions follow the prompt on your terminal and ask the cardholder to follow the prompts on their smartphone.

3. Most terminals will then authorise the transaction automatically. If the terminal prompts you to, call the Authorisation Centre immediately and follow the instructions. To find out more read Authorisations and referrals.
4. Wait for the terminal to print out a terminal receipt.
5. Check that the card number, expiry date and card type on the terminal receipt are the same as on the card. If any details are different, hold on to the card and cancel the transaction immediately. Then call the Authorisation Centre and select the 'Code 10' option.
6. If all the details match, check the transaction and amount, then ask the customer to sign the terminal receipt.
7. Check that the signature matches that on the card. If you are not sure, we recommend asking for additional identification such as a driving licence or a passport. If you are still in doubt call the Authorisation Centre.
8. If you are happy with the signature, confirm the transaction on the terminal and give your customer their card and receipt.
9. Only give the cardholder the goods they are buying when you have received authorisation and completed the card transaction. If authorisation is not given do not go ahead with the transaction. Ask your customer for an alternative payment method. Find out more about Reducing fraud.

See Keeping records for details of how receipts, paper vouchers and other high security items must be securely stored. Remember that even where authorisation is given, this is no guarantee of payment and the transaction is still open to being charged back.

Troubleshooting

You must always follow the prompts on your terminal. Never magnetic-swipe the card or manually PAN-key the card number into your terminal to avoid using the higher-level security features (such as chip and PIN) unless prompted to do so by your terminal.

- If the cardholder enters their PIN incorrectly- the cardholder will usually have three chances to enter their PIN. If all these fail, follow the prompts on the terminal. They will show whether the transaction can be completed on the card using another verification method or if the cardholder will need to provide another means of payment
- If the cardholder has forgotten their PIN- if your terminal allows PIN bypass follow the terminal instructions. If your terminal does not allow PIN by-pass ask the cardholder for another means of payment
- If you receive a message that the PIN is locked - please advise the cardholder to get in touch with their card issuer and ask for a new PIN, so that they can start using the card again in the future
- If the chip reader does not work - if the card offered contains a chip, the card must be entered into the chip card reader. If a terminal message says the card cannot be read:
  - Insert the card again (or try again with the card the other way round)
  - If this doesn't work the card may be damaged and you may be prompted to swipe the card instead.
  - If the card is still cannot be read ask the cardholder for an alternative payment method

  Please note: if you swipe or key enter a chip card and the transaction is later found to be fraudulent, the transaction may be charged back to you.
- Failed magnetic stripe transactions – key entry (excluding Maestro and Visa Electron cards)

Some customers may have magnetic stripe only cards. If the terminal says the magnetic stripe cannot be read:

- Try swiping the card again
- If it still cannot be read, you may be able to key in the card details using the number keys on the terminal
- Follow the prompts on your terminal for the information needed including the Primary Account Number (PAN).
- After you have entered the PAN and are waiting for authorisation, it is best practice to use a manual imprinter to obtain an imprint of the card on a paper voucher and complete all details on the voucher. The imprint of the card on the paper voucher proves that the card was present when the transaction took place. In the event of a chargeback dispute this may be used to attempt a defence. However, if found to be fraudulent, the transaction may still be charged back to you
- Clearly write "no value, swipe failure" on the paper voucher
- The cardholder must sign both the paper voucher and the cardholder receipt printed by the terminal
- Check the cardholder's signature matches the one on the reverse of the card
- Do not send this voucher to us for processing as the transaction is being completed through the terminal. In the event of a customer query or dispute we will contact you to request a copy of the paper voucher and the electronic receipt
- Explain to the cardholder why this process is taking place and reassure them that the paper voucher will not be processed but will be held as a record which will be sent to Worldpay if the transaction is disputed
- If your terminal breaks down completely. If your terminal has stopped working and you have purchased a backup pack, you can still accept card payments using your paper vouchers and imprinter. Find out more in the Terminal failure

Note: If you swipe or key enter a chip card and the transaction is later found to be fraudulent, the transaction may be charged back to you.

American Express

Please use the separate instructions provided by this company.

4.1.4 Purchase with cashback

Purchase with cashback (PWCB) may be good for your business and the people who shop with you. For your customers, being able to get cash when they spend at a local outlet is a convenient way to save time. This could encourage them to visit more regularly – potentially boosting your takings. From a security perspective, PWCB also reduces the amount of cash held on the premises, making your business less vulnerable to crime.

Offering Purchase with cashback

- You will need Worldpay's agreement to offer Purchase with cashback

- You must process the transaction through your terminal. If your terminal is not working, you cannot offer cashback (i.e. you cannot use paper vouchers for this)
- Cashback can only be offered if you're in the UK and a UK issued card is presented. And similarly if you're based in the ROI and a ROI issued card is presented
- Your customer must be making a purchase at the same time as requesting cashback
- Your customer must be present to enter their PIN (or sign the terminal receipt if the card does not support chip and PIN)
- The amount of cashback must not be more than £100 for UK customers and €100 for those in ROI.
- Your customer must use one of these cards:
  - Maestro
  - Visa Debit[1]
  - Visa Electron[2]
  - European-issued Debit Mastercard

Note: No new Visa Electron cards are being issued and the brand will be completely removed in 2022.

Before you start

- Be sure that the card belongs to the person presenting it. If you are suspicious you could ask the cardholder for other identification such as a driving licence or a passport. Find out more in Reducing fraud
- The PWCB process is not the same for all terminals. As well as following the basic step-by-step guide below, read your Terminal User Guide for specific instructions
- If suspicious about the card or the cardholder, call the Authorisation Centre and select the 'Code 10' option". Our operator will talk you through the process

[1] If the card is issued in the same country as the merchant's place of business.
[2] Your terminal should be configured to recognise where the card was issued.

Step-by-step guide

1. Ask the cardholder to insert their card into the chip reader slot on your terminal or separate PIN entry device.
2. Following the terminal prompts, key in the full amount of the transaction, then enter the PWCB amount separately.
3. Your terminal will now usually ask the cardholder for a PIN. If it doesn't, this may be because the cardholder has a non-UK-issued card, or an impairment that means they need to sign. For non- chip and PIN transactions, you should check that the card is not damaged and shows no sign of having been cut or written over. You should also check the specific security features for the card you are accepting. Ask the cardholder to check that the transaction amount is correct and enter their PIN.
4. Most terminals will then authorise the transaction automatically. If the terminal prompts you to call the Authorisation Centre, you must do so immediately and follow the instructions.
5. Only give the cardholder the goods they are buying and the cash amount when you have received authorisation and completed the card transaction. If authorisation is not given, do not go ahead with the transaction. Ask your customer for an alternative payment method.
6. Wait for the terminal to print out a terminal receipt.
7. Confirm the transaction on the terminal and give your customer the goods they have purchased, the cash amount, their card (they should remove it from the PIN pad if a chip and PIN transaction) and their copy of the terminal receipt.

See Keeping records for details of how receipts, paper vouchers and other high security items must be securely stored.

4.1.5 Refunds

When you process a refund on a card transaction, the amount of the refund is returned to the customer's card account and a corresponding debit will be made to your nominated bank account. If the refund facility is used where there is no corresponding originating transaction, this is not classed as a refund and does not fall within the terms of your contract. This is a breach of your contract for which you will be responsible.

Before making a refund

You must only process a refund if there was an original purchase. If there was no corresponding original purchase and you make a refund you will be in breach of your contract and we may withdraw your card processing facility. We may also suspend or withhold some or all funds for the transactions processed through the facility.

- Check that your customer has given you the card used for the original transaction - we recommend that the refund is made back to the card used for the original purchase where it is still available. If such card is not available at the time of refund then you may use another card
- You must not give a cash or cheque refund for a card transaction – fraudsters often try to obtain cash this way
- Never refund more than the original transaction amount
- If the customer has received a replacement card, the card number may have changed. In this case, take reasonable steps to make sure you refund to the original account. For example, check that the start date of the new card is after the purchase date, and ask them for proof of identity

- If the card has expired, you should still process the refund back to it, letting your customer know that they need to contact their card issuer to arrange for the funds to be received

Making a refund using your terminal

The way you do this depends on which terminal you have – please refer to your Terminal User Guide. If you need to use a supervisor card, please make sure that this is kept in a controlled environment and stored securely at close of business each day. If your terminal uses a supervisor code you should ensure it is changed regularly (including from any default setting) to prevent fraudsters from guessing the code, and only known by those people you have authorised to make refunds. It is your responsibility to ensure that you keep your supervisor code or supervisor card safe and secure. You will be responsible and liable for any improper use of the refund facility by your employees or others.

Making a refund using paper vouchers and the manual imprinter

1. Use a red Worldpay refund voucher, marked REFUND.
2. Put the customer's card in the imprinter, with the refund voucher on top, and print as usual. Give the card back.
3. Write on the voucher what the refund was for.
4. Sign the voucher yourself.
5. For the refund to reach the customer's account, you will need to post the refund voucher to us within three working days. The address to post these to is:

   VPU Worldpay
   Victory House
   5th Avenue
   Gateshead
   NE11 0EL
   United Kingdom

Please see Using paper vouchers for further details

See Keeping records for details of how receipts, paper vouchers and other high security items must be securely stored.

American Express refunds

Please use the separate instructions provided by this company.

4.1.6 Terminal failure

You should always use your electronic terminal to process card transactions. If your terminal stops working temporarily because of a fault, or if your power supply or telephone connection is interrupted, you can use our 'back-up' service (card imprinter and paper vouchers) but should only use these until the terminal is working again.

Using paper vouchers

You must only use paper vouchers as a 'back-up' when your terminal is not working or if your terminal instructs you to do so. You should advise Worldpay or your terminal supplier as soon as possible if your terminal is not working.

While you are using paper vouchers, you can only take Debit Mastercard, Mastercard Credit, Visa Credit, Visa Debit, JCB or Diners / Discover payments. You will not be able to accept certain cards that don't have raised numbers. Please check your contract for more information on accepted card types.

Remember you can only accept card types listed in your contract. If you take any others, the transaction may be returned unpaid.

You need to call for authorisation for every transaction using paper vouchers. Find out more in Authorisations and referrals.

Never split a transaction into two or more separate amounts on the same card, or split a transaction between two or more different cards or vouchers as a way of avoiding authorisation or referral of the full amount on one card. You however can split transactions between a card payment and cash. For the card element you will need to telephone for authorisation.

For American Express cards please use the separate instructions provided by this card company.

Step-by-step guide to using paper vouchers

1. Place the imprinter on a firm surface, with its sliding bar all the way over to the left.
2. Put the card into the imprinter with the raised numbers facing upwards. Make sure the card is securely slotted into the right place or you might damage it.
3. Place the Worldpay voucher on top of the card and tuck it in.
4. Slide the bar from left to right and then back again. You don't need to press down or force it.
5. Take the voucher out and check the numbers have printed through clearly on each sheet. If they haven't, destroy the voucher and try again with a new one.
6. If you cannot get a good imprint do not write the card details on over the top. If you keep having problems with the imprinter, contact the Worldpay helpdesk immediately to order a replacement and ask how to proceed.
7. When you have a good imprint, complete the voucher by writing the full details of the transaction clearly in the appropriate sections of the voucher with a ballpoint pen. Complete the amount in both pounds and pence or Euros and cents.
8. Ask your customer to check and sign the voucher, while you hold the card and watch them sign.
9. Check that the signature on the voucher matches the one on the card. You should always call for authorisation when using paper vouchers. If you are suspicious, when you call the Authorisation Centre and select the 'Code 10' option.
10. Only give the cardholder the goods they are buying when you have received authorisation and have completed the transaction.
11. If you are given an authorisation code, write it clearly on the voucher in the space provided using a ball point pen.

12. If authorisation is not given do not go ahead with the transaction. Destroy the partially completed voucher immediately. Ask your customer if they can pay with another card or cash. If you are offered another card for payment you must contact the Authorisation Centre again to obtain authorisation on the new card before starting a new transaction.
13. When the transaction is complete, give the card back to the cardholder together with the top copy of the voucher and the goods they have purchased.
14. Keep the rest of the voucher copies for processing and for your records.

See Keeping records for details of how receipts, paper vouchers and other high security items must be securely stored.

Processing paper vouchers

For the money from paper voucher transactions to reach your bank account, you need to complete and send us a Banking Summary Voucher.

If you have made any refunds using paper vouchers, you will also need to send to us the processing copies of the refund vouchers.

The address to send these to is:

VPU Worldpay
Gateshead Card Centre
5th Avenue
Gateshead
NE11 0EL
United Kingdom

Using Banking Summary Vouchers

The Banking Summary Voucher has three parts:

- White – processing copy
- Blue – this copy is for your records
- Yellow – this copy is also for your records

How to prepare Banking Summary Vouchers

1. Place your Banking Summary Card in the imprinter together with the Banking Summary Voucher and take an imprint of your retailer card.
2. Turn the voucher over and complete the back of the white copy:
   - List the individual amounts of the sales vouchers.
   - Calculate and complete the total of all sales vouchers.
3. Turn the voucher back over so that the blue copy appears and write in:
   - The number of sales vouchers and their total value.

- The number of refund vouchers and their total value
- The total amount by deducting the refunds from the sales. If the value of the refund vouchers is higher than sales, then put a minus sign in front of the total to show it is a negative value

4. Sign and detach the white copy and put it with the sales vouchers, in the same order they are listed, plus any adding-machine listing(s) if you have used these. Please do not use staples, pins or clips to hold the vouchers together.
5. Keep the blue and yellow copies for your records and to help you when you reconcile your bank statement.
6. Please send the white copies of the Banking Summary Voucher and paper voucher(s) within three working days to the Voucher Processing Unit at:

VPU Worldpay
Victory House
5th Avenue
Gateshead
NE11 0EL
United Kingdom

The maximum number of vouchers you can submit with a Banking Summary Voucher is 200, but you can submit more than one Banking Summary Voucher at a time. If your list of transactions won't fit on the back of the Banking Summary Voucher, please include a separate list of the amounts making up the total. This could be an adding-machine listing.

Adjustments

- If there are any errors on the Banking Summary Voucher, we will write to you with full details. Any adjustments are normally made to your account within five working days of the date of the letter
- Any adjustment will be made to the account from which we normally debit your service charge, unless you have made different arrangements with us

4.2 Online payments

We provide a range of services to enable you to trade online. Our payment gateway solutions are designed to connect simply to your eCommerce store.

4.2.1 Important information

Before you can make eCommerce sales, you need an agreement with Worldpay that allows you to accept eCommerce transactions. Without this you will be in breach of your contract.

- When this arrangement is in place we can give you guidance about setting up and integrating your website with our gateway
- You will be issued with a new customer account just for your eCommerce sales. You must never use an existing non-eCommerce account for your online sales
- Your floor limit for eCommerce sales must be zero to ensure all transactions are authorised

- You must always advise and obtain Worldpay's approval in advance should you intend to take transactions from a new website that we had no prior knowledge of

4.2.2 Payment types you can accept

Our gateway solutions allow you to accept the full range of card product types (such as consumer prepaid, debit, credit or commercial i.e. business cards) on our hosted payment pages, including:

- Visa Debit and Credit
- Mastercard Debit and Credit
- Maestro
- Visa Electron
- American Express
- JCB
- Diners / Discover

Note: No new Visa Electron cards are being issued and the brand will be removed completely in 2022.

Note: If you do not wish to accept certain EEA Issued card products (i.e. consumer pre-paid, debit, credit or commercial cards), then information on what other cards and payments you do accept must be provided to the customer before they enter into a purchase agreement.

4.2.3 Reducing fraud and chargebacks

Most eCommerce sales are genuine. However, because the Internet is relatively anonymous – you don't see the card or the shopper – some people see it as a less risky way to attempt fraud. Fraudsters want to obtain goods they can sell on for cash; others 'card test', placing an order to check if the card details they have will be authorised. See How to combat eCommerce fraud.

If an eCommerce transaction is disputed, it's very difficult to prove that the real cardholder ordered the goods. In this case you will be responsible for any challenge raised. To reduce the risk of fraud and chargebacks, it's extremely important to follow the correct procedures.

When making an eCommerce sale, you must do all you can to check your customer's identity and make sure that they are entitled to use the card being offered. If you employ a third party Payment Service Provider (PSP) to

capture and process your eCommerce transactions, they should deal with the below process for you. Note that you should only use a PSP that is compliant with the PCI DSS requirements – see Payment security.

Details to collect:

- Card number
- Card expiry date
- Cardholder's name and initials as they appear on the card. Cardholder's full postal address / billing address
- Delivery address, if different
- Card Security Code (if your PSP software is enabled to capture these details) – the last three numbers on the signature strip (please note: this information must only be used for one transaction and must not be stored for future use). Example Cards has details of card features including the location of the CSC code, see section 17.3.

Authorisation

- All eCommerce transactions must be authorised

Note: Authorisation of a transaction does not guarantee payment. An authorisation only checks that at the time of the transaction the card has not been reported lost or stolen and the availability of funds. An authorisation cannot always validate the address you have been given. You should consider undertaking additional checks as appropriate.

Find out more about Authorisations and referrals.

4.2.4 Cancellations after an eCommerce order is taken

- If an eCommerce transaction is cancelled for any reason and the original transaction was authorised, you must cancel the authorisation code. If you need Worldpay to cancel the code on your behalf contact the Authorisation Centre
- If you employ a third party Payment Service Provider to capture and process your eCommerce transactions, you must also let them know that the transaction is cancelled
- If the transaction has already been processed, you will need to make a refund

4.2.5 Keeping customer data secure

- Card details must be captured and stored securely, either on your own secure server or by a PSP able to connect to Worldpay
- Card details must always be encrypted and the host server must be protected by a firewall

- Email is not a secure way to transfer card transaction data. You must ensure that the card number is omitted from the order confirmation message sent to your customer
- To find out more about payment and information security visit our SaferPayments website

4.2.6 Cardholder authentication

Cardholder authentication is a security tool designed to help you authenticate cardholder details in an online eCommerce environment. It brings together the 3D Secure cardholder authentication schemes that verify a cardholder's identity when they make an online purchase - Mastercard Identity Check, Visa Secure and American Express SafeKey.

The card schemes use systems that enable an online shopper to prove they are the genuine cardholder, by requesting they enter a unique password at the shopping-cart stage.

This is an additional check; a security "box" may appear on screen allowing the shopper to enter elements of their unique password or answer a series of questions if required. This feature is provided by the shopper's card issuer and will usually appear within your payment page. The process only takes a few seconds and the customer is unlikely to notice any interruption to the sale process.

Most chargebacks happen when a cardholder denies that they have made a purchase. This security tool goes a long way towards proving that a sale is genuine. If you have cardholder authentication and offer it to your customers, you will be protected from most chargebacks with a fraudulent reason code. Please note that the use of Mastercard Identity Check is compulsory for eCommerce Maestro transactions.

4.2.7 If you change your Payment Service Provider (PSP) or website

If you decide to change your PSP, please contact the eCommerce helpdesk with your new details. They may be able to update your existing account. If not they will arrange for a new Customer Number to be set up for you so that you can begin trading with your new PSP as soon as possible.

You must also tell us if you decide to change your website or the goods which you sell through it. If you don't make us aware of this it may result in termination of your contract with Worldpay and / or in fines from the card schemes for which you will be responsible.

4.2.8 Website guidance

Before you carry out any eCommerce sales, your legal advisers should review your website to check that all contractual and legal issues are covered adequately and the website contains appropriate disclaimers and restrictions.

As a minimum, your website must clearly display:

Information about your business

- Who you are – you must clearly disclose your business name so that cardholders can easily determine who they are dealing with (and distinguish you from other parties such as your suppliers). Your website domain name must be recognisable by the cardholder based on their online shopping experience. If you are a company, you should include your full company name and incorporation / registered number, together with

your physical and online addresses. Your identity should be consistently conveyed on all communications with the cardholder

- A customer service phone number (including both country and area codes) that cardholders can use to resolve disputes. The number quoted must not be that of a mobile phone. If you deliver goods or services internationally, both domestic and internationally accessible numbers must be listed. Your email address should allow you to be contacted 'directly and rapidly'. This should be the email address of your customer service desk if you have one
- Your VAT registration number
- Details of any Trade Association membership, including registration number, details of the code of conduct to which you subscribe and details of how to contact them
- Details of any professional body you are registered with, your professional title, the member state which granted it and a reference to the applicable professional rules in that member state and information as to how these rules can be consulted electronically
- Accurate disclosure of merchant outlet location before the cardholder completes the purchase is important for eCommerce transactions as such information may affect fees, taxes and shipping times
- Display the country of the merchant outlet either:
  - On the same screen view as the checkout screen that displays the final amount
  - Within the sequence of the webpages the cardholder accesses during the checkout process

Information to be given before an order is placed

- A description of the products and services (including any guarantees) you are offering, clearly explaining your shipping practices together with any export restrictions. The cardholder must be able to clearly determine when they can expect to receive their merchandise
- Total costs for products or services, including all appropriate shipping, handling and tax charges. You must quote all prices in a currency agreed with us and the currency offering must be clear to the cardholder. Where applicable, you should indicate details on currency conversion (exchange rate)
- Clear, easy-to-find terms and conditions and procedures, which state the exact commitment that the cardholder is being asked to make, must be made available in a format that the cardholder can store and reproduce
- Your returns policy must be made clear to the cardholder before payment is requested. Your refund policy should provide a full refund including the cost of the shipping, handling and applicable tax charges
- Your cancellation policy must be made clear to the cardholder before payment is requested. If you are offering a free trial period, you must:
  - Ensure at the time of enrolment that the cardholder has given explicit consent to enter into an ongoing subscription service
  - Ensure that you provide confirmation of the agreement, start date of subscription, details of services, ongoing transaction amount and billing frequency / date and a link to a simple mechanism to enable the cardholder to easily cancel any transactions online. You must ensure that this is also disclosed in the transaction receipts

- A clear statement that the cardholder is committing to a payment - where they are prompted to enter their account number, giving an option to cancel at that point. You may only request a card account number as payment for goods or services and must not request or use the account number for age verification or any other purposes other than payment. If possible it is advisable to get proof that the cardholder is aware of and agrees to this policy, in order to try and defend any disputes raised by the cardholder regarding the cancellation / return of goods / services
- Clear instructions on how to complete the order together with instructions for correcting input errors before the order is placed, irrespective of the way the order is taken or may be accessible thereafter
- Details of languages offered for conclusion of the order
- Seek formal agreement from the cardholder before storing card details for use in any future purchase

Information to be given after the order is placed

- An effective, accessible way to correct any input errors which took place at the point of confirmation
- An email acknowledging receipt of the order, which must be sent the customer 'without undue delay'
- Confirmation in 'durable form' – such as email – of:
  - The name and geographical address of your business
  - A description of the main characteristics of the goods
  - The price, including all taxes and delivery costs where appropriate.
  - Arrangements for payment and delivery
  - The geographical address to which any customer complaint should be addressed
  - Information about after-sales service and guarantees

Commercial communications

You must ensure that any unsolicited commercial communication sent by email is clearly and unambiguously identifiable as soon as it is received. You must clearly identify in all communications, any promotional offer (including any discount, premium, gift or competition) and ensure that any conditions which must be met to qualify for it are easily accessible, and presented clearly. You must also comply with the following basic standards:

- Data Protection Legislation within the applicable law must be adhered to in order that the collection of personal information is not processed, traded or disclosed illegally
- You must ensure you have appropriate operational and technological processes and procedures in place to safeguard against the unauthorised access or unlawful processing, or disclosure, of personal information
- The security measures you must take include the use of the most up to date technologies to protect the personal information collected or stored on your web site and / or systems. Especially sensitive or valuable information, such as financial data, should be protected by reliable encryption technologies

- Distance-selling requirements must be complied with as laid down in the applicable law[1]. Complying with other applicable trading standards and laws and regulations as the same are created from time to time

4.2.9 Card Not Present transactions

Card Not Present (CNP) transactions are those where the card and cardholder are not with you at the point of sale. Offering your customers this option gives you and them extra flexibility, but it's important to understand that you will need Worldpay's agreement to accept these transactions:

- Mail Order Telephone Order transactions
- eCommerce transactions

Before deciding to accept CNP transactions you should consider all risks to your business. This is because they carry a higher risk of fraud and you will be financially liable if a transaction is confirmed as invalid or fraudulent. Please carefully read the Reducing fraud section covering CNP transactions.

Can I accept CNP transactions?

You can only accept CNP transactions if the CNP section of your application form (which forms part of your contract with us) has been completed and accepted by us. If it has not, and you would like to make CNP sales, please contact the Worldpay helpdesk. Having Worldpay's agreement to accept CNP transactions does not automatically allow you to accept card payments over the Internet. To do this, you will need to have an agreement with Worldpay that allows you to accept eCommerce payments and an Internet payment facility. To find out more, please read the eCommerce transactions section of this document.

Authorisation

All CNP transactions must be authorised. Find out more about Authorisations and referrals.

Note: Authorisation is not a guarantee of payment. An authorisation simply means that at the time the transaction was taken and you obtained authorisation the card has not been reported lost or stolen and there are sufficient funds available. An authorisation cannot always validate the address

[1] A Guide for e-Business to the EC Directive regulations 2002 and related material can be found on the HMSO website

you have been given and therefore you should consider undertaking additional checks as appropriate.

4.3 Mail Order and Telephone Order payments

This section covers only Mail Order and Telephone Order (MOTO) sales. Find out more about taking card payments over the Internet in the eCommerce transactions section.

4.3.1 Which cards can I accept?

You can accept:

- Mastercard
- Debit Mastercard
- Visa
- Visa Debit.
- Visa Electron
- Domestically issued Maestro
- JCB
- Diners / Discover

Note: No new Visa Electron cards are being issued and the brand will be removed completely in 2022.

Note: If you do not wish to accept certain EEA Issued card products (i.e. consumer pre-paid, debit, credit or commercial cards) you must provide information to customers on what other cards and payments you do accept, before they enter into a purchase agreement.

4.3.2 Reduce the risk of fraud

Most MOTO sales are genuine. However, because they are relatively anonymous – you don't see the card or the shopper – some people see it as a less risky way to attempt fraud. Many want to obtain goods they can sell on for cash; others 'card test', placing an order to check if the card details they have will be authorised.

If a MOTO transaction is disputed, it is very difficult to prove that the real cardholder ordered the goods. To reduce the risk of fraud and financial loss to your business, it's extremely important to follow the correct procedures.

Find out more about Reducing fraud and Additional security checks for MOTO transactions in Card Not Present transactions.

4.3.3 What details do I need from the cardholder?

To process a MOTO transaction, you will need to take the cardholder's:

- Card number – the long number across the centre of the card
- Name as it appears on the card – including any initials
- Card expiry date
- Full postal / billing address, including postcode, as it appears on the cardholder's statement
- Chosen delivery address – if different from above
- Card Security Code (CSC) - three-digit code at the end of the signature strip (NOTE – CSC needed for telephone order transactions only, NOT required for Mail Order transactions)

If you have a limited returns policy, such as no refunds, you must make this clear to customers before asking for payment. To avoid disputes, we recommend you ask them to agree to your terms, in writing if possible, before completing the transaction.

Note: Never ask for a customer's PIN.

4.3.4 The Data Protection Act 2018

Please remember that if you are collecting personal data like the above, you need to comply with your obligations under data protection legislation. This includes any requirement to resister as a data controller. Worldpay will not take responsibility if you fail to do this and action is taken against you.

4.3.5 How to complete a MOTO transaction

Follow the prompts on your terminal and enter the information asked for, including the additional security checks of the Card Security Code and Address Verification Service if your terminal is set up for these services. The exact process depends on the terminal you have. Please read your Terminal User Guide to find out more.

4.3.6 Additional security checks for MOTO transactions

To help make MOTO transactions as secure as possible, you will need to key in details on your terminal for both of the following. You will then get a response on your terminal to help you decide whether to go ahead with the sale.

Card Security Code (CSC)

This is a three-digit code at the end of the signature strip or in a separate white box next to the signature strip. American Express cards have a four-digit CSC on the front of the card. (NOTE – CSC needed for telephone order transactions only, NOT required for Mail Order transactions). Never record the CSC – it must only be used for one transaction.

Address Verification Service (AVS)

The 24 / 7 Worldpay helpdesk can carry out a name and address check over the telephone. This service verifies that the name and address details provided match the details registered to the card issuer. A fee applies to this service. Contact the Worldpay helpdesk for details.

AVS is also available through Worldpay terminals and can be used to check the numerical part of the cardholder's registered billing address with the card issuer. Care should be taken when obtaining details from the cardholder to ensure the address detail provided are exactly those they have registered with their card Issuer (i.e. as it will appear on their statement) to avoid a possible address mismatch.

Due to the nature of overseas addresses and the way in which they are stored by card issuers, we may not, in all cases, be able to provide a full address match.

Examples of CSC and Address Numbers:

- Card number - 5123 4567 8901 2345
- Three-digit CSC – 696

Mr AN Other **22 High Street** **Anytown** **AB21 2BB**	**Mr A N Other** **Flat 4** **22 High Street** **Anytown** **AB21 2BB**
You should key CSC: 696 Postcode numbers: 12 Address number: 22	You should key CSC: 696 Postcode numbers: 12 Address numbers: 422

Mr AN Other **Level 10** **Tower Building** **200 High Road** **Anytown** **AB21 2BB**	**12345 Corporal A N Other** **BFPO 7899** **22 Sun Avenue** **Cyprus** **CYP 12**
You should key CSC: 696 Postcode numbers: 12 Address numbers: 10200	You should key CSC: 696 Postcode numbers: For BFPO addresses no data is to be entered in this field Address number: 78992212[1] (the first eight numeric starting with the BFPO number

Mr AN Other **Home Farm Cottage** **Lane End** **High Village** **Anytown** **LU3 1NH**	**Mr AN Other** **22 Wall Street** **New York** **1234567[2]**
You should key CSC: 696 Postcode numbers 31 Address number: If no numbers just press Enter	You should key CSC: 696 Postcode numbers: 1234567 (first eight numerics of ZIP Code) Address number: 22

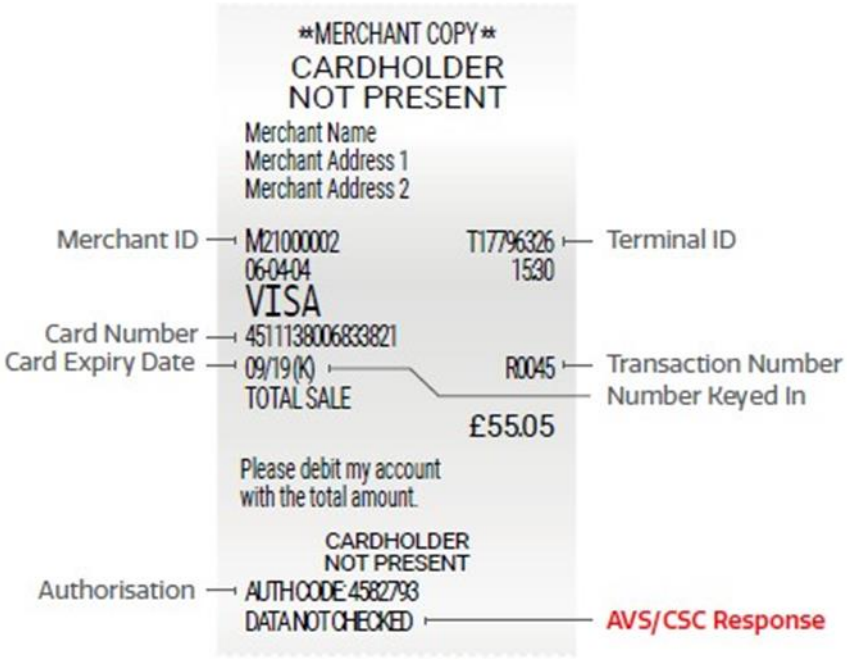
What do the CSC / AVS responses mean?

After you have keyed in the CSC and AVS data, as long as the transaction has been authorised, one of the responses shown below will appear on your terminal. It can also be found at the bottom of your copy of the till receipt. Please read the response carefully, as in some cases it may identify a higher risk. For example, if data

[1] Some terminals may limit the number of digits which can be entered in these fields. Where this is the case enter as many digits as your terminal will allow

[2] Some terminals may limit the number of digits which can be entered in these fields. Where this is the case enter as many digits as your terminal will allow

cannot be matched and where you should consider additional checks to reduce the risk of fraud. Please refer to Reducing fraud.



It's important to understand that these checks are an additional security measure. They can help you make an informed decision, but they are not a guarantee of payment.

The below tables shows CSC / AVS responses. However it's important to note that the exact wording of the response may vary depending on the terminal or service provider you use. Please refer to your terminal or service provider if a different response is received. Having carried out these checks, it is your responsibility to understand what the response means and to decide whether you want to proceed with the transaction.

Response	What this means	What we suggest you do
Data Matched	Both the CSC and AVS match the card issuer's records	If you have been given an authorisation code and there are no other suspicious circumstances, in most cases you will want to go ahead with the sale, as long as you are confident you can securely deliver goods / services to the address that has been verified. Delivering to a different address increases the risk associated with any CNP sale. Find out more in Reducing fraud.

Response	What this means	What we suggest you do
Card Security Code Matched	The CSC matches. Address postcode and house number details cannot be fully matched	There is a possibility that the transaction is fraudulent, but it could also mean that the cardholder has moved recently and not updated their details with their card issuer. Another possibility is that the details have been taken down incorrectly or that the cardholder address is abroad and we have been unable to verify with the card issuer. Before going ahead, you should check the address details with your customer and satisfy yourself that they are the rightful cardholder before progressing with the sale.
Address Match Only	Only CSC cannot be matched. Address postcode and house number details match	There is a possibility that the transaction is fraudulent, but it could also mean that the cardholder has given you the wrong CSC. Before going ahead, check the CSC with the customer and satisfy yourself that they are the rightful cardholder. Beware of repeated attempts by the cardholder to get the CSC right. This could indicate fraud. Please read the Reducing fraud guidance.
Data not Matched	The CSC and one or both of the address number details do not match	There is a possibility that the transaction is fraudulent. We recommend you do not go ahead without further checks to satisfy yourself that the person offering the card is the rightful cardholder. For example, you should ask for additional ID, such as a copy of the passport or driver's licence, or ask for copies of utility bills.
Data not Checked	The card issuer has not been able to check the data	This could be because the card issuer doesn't support either of these security checks or their system is down. If this happens you need to make a decision based on the information you have, to satisfy yourself that the person offering the card is the rightful cardholder, before processing the transaction.

4.3.7 Making an informed decision

Even when the AVS and CSC do not match, the transaction may still be authorised for the value of the transaction. If this happens, it is your decision whether to accept or decline the transaction based on the results of the CSC / AVS checks. Please remember that these checks are not a guarantee of payment.

These additional checks through your terminal also cannot confirm cardholder names. Therefore you should take additional steps to do so if you are in any way unsure about the transaction.

It's up to you to decide whether to proceed or not. When you make your decision, bear in mind that you will be financially liable if the transaction is confirmed as invalid or fraudulent/returned unpaid by the card issuer, even if the CSC / AVS data matches and an authorisation code has been given.

4.3.8 Protect your business

Most MOTO sales are genuine but the risk of fraud is higher because the cardholder and card are not present. Follow all the processes outlined in this section and refer to Reducing fraud.

4.3.9 Delivery, documents and record-keeping

Goods ordered by mail or telephone order must be delivered to the person who ordered them and not released to third parties, including relatives, couriers not arranged by your business and taxi drivers.

A signature should be obtained from the cardholder as proof of delivery – this can be used as evidence in the event that a dispute subsequently arises.

For all MOTO transactions you must send the following documents to the cardholder with the delivery:

- Sales invoice, to support the transaction
- Cardholder's copy of the receipt from the terminal

See Keeping records for details of how receipts, paper vouchers and other high security items must be securely stored

If a cardholder wishes to collect the goods they must come to your premises in person and produce their card. In this case, you must either cancel or refund any previously-completed MOTO transaction and process a new card present transaction, following the instructions in your terminal guide and the prompts on your terminal.

4.4 General payments information

4.4.1 Card recognition guide

The majority of cards you are processed as chip and PIN or contactless and do not need you to see the card. But be careful if the transaction is not completed by entering PIN or the card is a signature-only card. In this case you must verify that the signature on the receipt matches that on the card. As more and more cards are available, you see cards of various shapes, sizes and colours. Provided you ensure that all the security features are present, including those specific to the individual card schemes, you can accept the card for payment.

We recommend that all your staff know the process for accepting card payment. Make sure they are familiar with these security features and always follow the prompts on your terminal.

Not a chip and PIN card or contactless card?

Most cards are now chip and PIN and / or contactless enabled, but you may sometimes see chip and signature or magnetic swipe and signature cards. You must accept these cards as long as you verify the card. You must

ensure that the card has all the security features explained in this section, including those specific to the individual card schemes.

Key security features

As cards are normally placed in or tapped against card readers by the cardholder, you may not have the opportunity to check all of these security features. But if you are suspicious for any reason, here are key details to check.

Note: Note that not all cards are embossed or have a full account number or cardholder name.

Genuine cards will always have a:

- Card logo – see examples
- Hologram – see examples
- Ultraviolet image
- Card Security Code (CSC) - A three-digit code at the end of the signature strip or in a separate white box next to it. American Express cards have a four-digit CSC on the front

Example cards

To see images and details of example cards please connect directly to the applicable card scheme websites or view the sample Visa card below:

Mastercard
Diners / Discover
JCB
American Express

4.4.2 Keeping records

Terminal receipts, paper vouchers and other transaction records are high-security items, so restrict access to them. Keep your copies of all transaction details in a secure fireproof place for at least 13 months. This is in case there is a query later or you need the details to help defend a chargeback.

Note: For any Visa transactions where a cardholder signature was required, keep it for 120 days. If you work in the travel or entertainment sector then you must keep receipt documentation for 6 months.

Do not alter transaction records in any way. If there is a dispute, the cardholder's copy will normally be taken as correct. After 13 months, make sure that you dispose of all transaction records securely. You can reduce this disposal time to 120 days where a signature is required or 6 months for the travel or entertainment sector.

See Payment security for more details of data security requirements.

What to look out for?

Chip

If there is a chip; check if there is any visible damage.

Card number

The card number – the long number on the front – should be clear, even and in line.

The first four digits of the card number will be laser-imprinted on the front of the card beside the embossed details and should be identical to the embossed details (smaller type, above or below the beginning of the long embossed number).

Cardholder title and name

Should be clear, even and in-line. Embossed cards must have either a cardholder name or description such as 'club member' or 'gift card', etc. For flat-printed cards the cardholder name or description is optional.

Check that the title and name on the card match the gender of the person presenting it.

Expiry date / valid from date

All cards have an expiry date, but only some have a valid from date. Check that the card isn't being presented before its 'valid from' date or after its expiry date.

Contactless indicator

This 'wave' symbol indicates that the card can be used to make payments without swiping it or inserting it into a terminal. This symbol usually appears on the front of the card.

Card scheme logo

To download card scheme logos, please visit our Adding card logos website.

Hologram

These may be on the front or back of the card. The 3D image should move when the card is tilted. If the Visa logo has been placed on the back of the card it will usually be a miniature version.

These are the most common holograms currently in use:

- Mastercard – the world(/globe)
- Visa – a dove, which appears to fly
- Maestro (UK-issued) – William Shakespeare's head
- Visa Electron – not all these cards have a hologram. If there is one, it will be a flying dove

Signature strip

The signature strip should not stand higher than the surface of the card. Check that either the full card number or the last four digits of the card number are printed in reverse italic text on the signature strip. However, if the transaction is not completed by entering the PIN or the card is a signature-only card, you will need to verify that the signature on the receipt matches that on the card.

Card Security Code (CSC)

Usually on the reverse of the card, either on the signature strip or in a white box to the side of the signature strip.

Combination cards

These cards allow cardholders to choose how they pay – for example, by debit or credit account. When the customer offers the card, they choose which function they want to use. Combination cards look very much like regular cards but have:

- Two card numbers, one of which is printed on the back of the card
- Two three-digit security codes
- A description of the different functions on some cards, near the card scheme logo

The processes to follow when accepting a combination card are the same as for all other cards. The difference is the terminal will prompt you for a decision about the function to use for the transaction.

Examples of card UV images

If an ultraviolet lamp is available place the card under and check for the appropriate mark.

Note: Some Visa Electron cards do not carry UV features.

4.5 Reconciling your invoice

If you have a Worldpay terminal, you must complete an end of day "reconciliation" report at the end of each day's trading. You must do this within your allocated banking window.

Completing an "end of day" report checks that the transactions have been processed correctly and are not stored in the terminal. If funds are stored in the terminal it can delay the funds being credited to your account. You will also find the report very useful to help reconcile your accounts.

If you're unsure of how to do this, see the instructions in our Terminal User Guide.

4.5.1 Accessing your invoice

We can provide your invoice by post or electronically depending on your preference. Customers registered with Worldpay Dashboard from Worldpay have online access to their invoice. The invoice can be downloaded in PDF format and you can print it. In addition, Worldpay Dashboard offers access to transaction and settlement data including card sale trends and analytics. All other customers get a physical paper copy. For more information and to determine eligibility, you can speak to the Worldpay helpdesk team.

If you are already registered on Worldpay Dashboard, you can use the Manage Account pages to turn off paper invoicing.

How to receive by post

If you're currently receiving invoices online and would like to switch to paper invoicing, use the Manage Account pages on Worldpay Dashboard to turn on this feature.

4.5.2 Settling your invoice

Your Worldpay invoice details all of the transactions processed that month, plus any associated charges. Your invoice for the period is available in the first week of each month. You must pay as described in our invoice and terms and conditions.

Failure to pay the amount due is a breach of the terms of your contract/s which we will require you to remedy. If you do not pay or agree satisfactory arrangements to pay any outstanding sums we may close your account. We also reserve all our rights under our contract with you. These include the right to defer settlements and set-off any amounts owed by you, and / or to suspend your payment facilities.

Where you take UnionPay transactions, we deduct any merchant service charge from the transaction amount before remitting the balance to you. We will send you a statement the month after you have taken any transactions which shows those transactions and the amount deducted.

4.5.3 Electronic Management Information (MI)

In addition to your monthly invoice, you can sign up to receive detailed Monthly Electronic Management Information (MI). If you sign up, you will receive this information by email during the first week of each month.

To receive MI you must have:

- Registered your email address with us
- Access to the internet
- Microsoft Excel 97 (or later version)

To register, write to the following address and ask that your account is set up with access to Electronic Management information. You must quote your Customer Number and provide the email address we can use to send the monthly MI email.

Amendments
Worldpay
Victory House
Fifth Avenue
Gateshead
NE11 0EL
United Kingdom

Opening MI files

To open the MI files you must download a formatter to convert the file to a user friendly version. To download and install the File Formatter:

1. Download the file formatter or paste www.worldpay.com/sites/default/files/reconciling-your- invoice.xls into your web browser.
2. If a message about macros appears, select "Yes – enable macros". Be patient – this may take a minute to load.
3. Save the spreadsheet to your PC / file server.
4. Click the "Add IMIX toolbar" button on screen.

You'll only need to do this once – File Formatter remains on your computer.

When you get your monthly MI:

1. Open the file in Excel.
2. Click on the IMIX CVS File Formatter toolbar.
3. The file will then be converted to a user-friendly format.

4.5.4 Premium Transaction Charges

When applicable your monthly invoice will summarise the premium charges that are payable. If required the MI will provide more detail.

4.5.5 More information

Further information, Frequently Asked Questions and a video overview are also available on our web site.

4.6 Other transaction types

Recurring transactions are an easy way for you to collect regular payments from customers, such as membership subscriptions and monthly insurance premiums. To avoid any disputes, it's very important that you follow your

4.6.1 Recurring transactions

The basics

To set up a recurring transaction, you must:

- Have an agreement with Worldpay that allows you to take recurring transactions
- Use the Customer Number provided by us under this agreement to process recurring transactions, not your normal Customer Number
- Before you store the card number, you must have the cardholder's written authority to do so. You must also have an approval response from the card issuer to the first transaction under the agreement
- Check the card is one of these: Mastercard, Visa Credit, Visa Debit, Visa Electron, JCB, Debit Mastercard, Diners / Discover

- Obtain authorisation for the first payment in the sequence of recurring transaction. This authorisation must be by a secure method:
  - Chip and PIN for card present transactions, or
  - Card Security Code (CSC) for Mail Order Telephone Order (MOTO) transactions, or
  - Visa Secure / Mastercard Identity Check for eCommerce transactions
- Never process a transaction that is declined

In addition, you must provide valid contact details (telephone number, email or web site) that will appear on the cardholder's statement. Contact us if these details change.

Note: Never ask for a customer's PIN and never store your cardholder's Card Security Code (CSC). The CSC may be used for the first transaction but is not required for subsequent transactions.

Entering into a recurring transaction agreement

You must get the cardholder's consent to a recurring transaction agreement. Before you get the cardholder's consent, you must explicitly state:

- The amount of the recurring transaction and whether this amount is fixed or variable
- The date(s) on which the recurring transaction will be charged to the card and whether the date is fixed or variable
- The method of communication for all cardholder correspondence
- That the recurring transaction agreement may be cancelled by the cardholder at any time

You must also obtain the following information from the cardholder allowing you to take payments from their account:

- Cardholder name
- Full address
- Postcode
- Telephone number
- Card account number
- Card expiry date
- Agreed payment pattern
- Authority and understanding the authority will remain in force until such time as it is cancelled in writing

The Data Protection Act 2018: Please remember that if you are collecting personal data such as the above, you must comply with your obligations under data protection legislation. This includes any requirement to register as a

data controller. Your failure to do this and any subsequent action that may be taken against you will not be the responsibility of Worldpay.

See Keeping records, for details of how you must store receipts, paper vouchers and other high security items.

Confirmation of a Recurring Transaction Agreement

You must send confirmation to the cardholder, using an agreed method of communication, that a recurring transaction agreement has been established. You must send this confirmation no later than two business days after the agreement was put in place.

Notification of a Recurring Transaction Agreement

You must notify the cardholder at least seven working days before the recurring transaction payment is taken and using an agreed method of communication, if any of the following situations occur:

- The payment amount and / or payment date has changed
- More than 6 months have elapsed since the last payment
- A trial period, introductory offer or promotional activity has expired

Cancellation

It's important to understand that a cardholder may cancel their authority to debit their card account at any time.

You must act on the cardholder's instruction, send confirmation of the cancellation using an agreed method of communication and collect no further payments.

If any payment is returned unpaid – for example, if the account has been closed – you must contact the cardholder and ask them to pay in another way. Never re-debit the card as this may lead to chargebacks and ultimately suspension or termination of your Worldpay facility.

If you offer recurring transactions for eCommerce sales, you must offer an online cancellation facility.

4.6.2 Our other services

In addition to sales transactions, Worldpay also allows you to accept card payments for the following services:

- Hotel Services
- Vehicle Rental Services
- Bureau de Change
- Dynamic Currency Conversion
- Tax free shopping

Hotel Services

We offer two card payment services that can help you to run your hotel business more efficiently. These are enabling your guests to make guaranteed reservations over the phone or online and providing express checkouts.

Guaranteed reservation

With our guaranteed reservation service, hotel guests who give their card number when they make a booking are guaranteed a room. It also entitles you to charge the card for one night's stay (plus any applicable taxes) if the guest does not arrive. You can also charge the card if the guest cancels their booking after an agreed deadline or with insufficient notice. To use this service, you need agreement(s) with us to process MOTO transactions and eCommerce (if you accept bookings over the Internet).

Which cards can I accept for guaranteed reservations?

You can accept:

- Mastercard
- Debit Mastercard
- Visa
- Visa Debit
- JCB
- Diners / Discover

You cannot accept:

- Maestro
- Visa Electron

What details do I need from the cardholder?

When a guest calls to make a guaranteed reservation, you will need to take their:

- Card type
- Card number – the long number across the centre of the card
- Name as it appears on the card – including any initials
- Card expiry date
- Full postal / billing address, including postcode, as it appears on their statement
- Contact address – if different from above
- Contact telephone number
- Planned date of arrival and length of stay
- Number and type of room(s) wanted

Note: Never ask for a customer's PIN.

The Data Protection Act 2018

Please remember that, if you are collecting personal data like the above, you must comply with your obligations under data protection legalisation. This includes any requirement to register as a data controller. Your failure to do this and any subsequent action that may be taken against you will not be the responsibility of Worldpay.

What information must I give the cardholder / guest?

When the booking is made, you must provide the cardholder with the following information in writing:

- Rates for the room(s) they have booked
- Booking conditions
- Hotel address
- Your internal reservation code for their guaranteed reservation. Your cancellation policy
- You must also explain the following conditions:
  - The guest is able to cancel the reservation without penalty provided it is cancelled within 24 hours of the reservation being confirmed
  - The deadline for cancellation is 6pm local time on the booked date of arrival
  - If the guest cancels later than this, they will be charged for the night

You can set your own deadline earlier than this, up to a maximum of 72 hours before 6pm on the arrival date. If this is your policy, you must explain this at the time of booking and confirm it in writing at least three days before the arrival date. To help defend any cancellation disputes raised by a cardholder, it is best to have proof that the cardholder has read and accepted the policy at the time of booking.

If the guest fails to arrive at the agreed time, the reserved room is held until noon on the day following the reservation date.

If they do not arrive during this time, they are charged for one night's stay, and the rest of the booking is cancelled with no charge. This is called a 'no-show'.

For eCommerce transactions you must also provide copies of the relevant web pages detailing the terms and conditions of the booking, plus the actual website address.

What if a guaranteed reservation is cancelled?

If a guest cancels their booking within the deadline or with sufficient notice, you must not process a card payment. You should also provide them with this information in writing:

- A cancellation reference number, which you should also keep on file
- If the cardholder asks you to, you must include the cardholder's name, the last four digits of the card number, the card expiry date and your own cancellation code in this written confirmation

'No-shows' and late cancellations

If a guest fails to appear before noon on the day following their reservation, or calls to cancel the booking after the deadline, you can charge their card for one night's stay (plus any applicable taxes) in the room that they have reserved as set by your cancellation policy. To do this:

- Follow the instructions in Card Not Present transactions, using the information the cardholder gave when accepting the booking
- On the transaction receipt, write "NO SHOW"
- Under 'total' enter the room rate for the room(s) that they booked
- Send a copy of the bill for the 'no-show' booking to the billing address the cardholder gave when booking

What if the accommodation has been overbooked?

If a guest has made a guaranteed reservation but the room is not available when they arrive, you must provide them with:

- Comparable alternative accommodation
- Transport to the alternative accommodation and between establishments, if requested
- Forwarding of all messages and calls to alternative accommodation
- Two three-minute telephone calls, free of charge

If you do not provide these services, you may be excluded from taking Mastercard, Visa or JCB payments for guaranteed reservations in the future.

Keeping records

You must file copies of the following and keep them securely for a minimum of 13 months (for Visa transactions copies can be retained for 6 months) in case there is a query later or the details are required to help to defend a chargeback.

- Cardholder's name, address and card number
- The terms and conditions for the reservation, as provided to the cardholder at the time of the booking
- The confirmation code
- Transaction receipt, if a night's stay is charged
- Hotel bill
- Any correspondence relating to confirmations received from the cardholder acknowledging the terms and conditions of the booking

Express checkout

This convenient service means that when guests are ready to leave, they can return their keys and go without waiting for their bill to be made up. It is very important to follow the correct procedure carefully to reduce the risk of chargebacks.

Which cards can I accept for express checkout? You can accept:

- Mastercard
- Debit Mastercard
- Visa
- Visa Debit
- JCB
- Diners / Discover

You cannot accept:

- Maestro
- Visa Electron cards

How do I use express checkout?

When the guest arrives:

- Ask them whether they would like to use the service – not all guests will and some prefer to check their bill before paying it
- If they agree, ask for the card with which they intend to settle their bill
- Ask your guest to write down the billing address for the card. This is normally their home address, but some company cards are billed to the company address

Processing the transaction

When you have verified the card and the cardholder, follow the instructions in Card present transactions – Chip and PIN.

- The expected amount of the bill (the room rate, multiplied by the number of days accommodation) needs to be pre-authorised. Find out how to process pre-authorised transactions in your Terminal User Guide
- Explain to your guest that the bill is debited to their card account after they have left and that there is no need to pay on checking out
- If the transaction is not authorised, you will need to ask your guest for another method of payment. If they give you another card, you will need to verify this again before starting a new transaction

After your guest has left

Work out the final bill.

- Follow the instructions to complete the transaction using your terminal
- Send the bill and a copy of the terminal receipt to your guest at the billing address supplied. You must do this within three working days of the transaction
- If the final bill is higher than the pre-authorised amount, you will need to complete a top-up authorisation. Find out more in Authorisations and referrals or in your Terminal User Guide

- If the top-up authorisation is declined, you will need to contact your customer and ask them for another method of payment

Delayed or amended charges

There may be times when you need to process extra charges or change the amount agreed because of other costs incurred during the stay. These extra costs are called delayed or amended charges.

For hotel stays the following services may be the subject of a delayed or amended charge transaction:

- Room charges
- Food or beverage charges

A delayed or amended charge transaction must be completed within 90 calendar days of the transaction date of the previous transaction to which the delayed or amended charge transaction relates.

Please be advised that the card schemes do not allow merchants to process a delayed / amended charge for any damages incurred during a cardholder's stay.

Processing the transaction

When carrying out a delayed or amended charge transaction, you must:

- Include the words "Signature on File" on the Transaction Receipt
- Send a copy of the transaction receipt to the cardholder at the cardholder's address

Disputes (including chargebacks)

If we receive a disputed card transaction, we will write to you asking for documentation to help defend the dispute. You must supply us with the documentation within the timescale indicated in the letter. If you don't or are too late, a chargeback debit to your bank account will occur.

You must provide evidence that the charges billed were incurred by the cardholder during their stay. If you do not have any documentation to do this, we will not be able to defend a dispute on your behalf. If we cannot defend the dispute, and a chargeback debit will be processed to your bank account.

Please note that any transaction processed in a Card Not Present environment is taken at your own risk. The transaction can be subject to a chargeback dispute for which you may be liable and results in a debit to your bank account.

Vehicle Rental Services

Being able to accept card payments for vehicle rentals gives you and your customers' flexibility. It also offers you the added security of pre-authorising payments before the customer takes the vehicle away.

Before you start

You must let us know if you intend to accept card payments for vehicle rentals, because there are special requirements for these transactions. To minimise disputes and chargebacks, read this section thoroughly and ensure that you understand the specific requirements and risks of these transactions.

What information must I give the cardholder?

When a customer rents a vehicle from you, you must provide them with a rental agreement that includes all applicable terms and conditions for the rental, including:

- Cancellation policy and procedures
- Reserved vehicle rental rate
- Currency of the transaction
- Name and location of where the vehicle is to be collected from
- No-show' policy and procedures
- Any extra charges that they may be liable for, such as damages, parking tickets, no show policy and procedures and any limited refund policies

Make sure that the cardholder signs the rental agreement to confirm that they have read and understood the terms and conditions before you process any transactions. When a customer comes to collect the rental vehicle, you need to do two main things before they take the vehicle away with them – get their agreement to the rental agreement and pre-authorise the transaction.

- Get their agreement to the rental agreement
  - Ask your customer to read the terms and conditions and sign the rental agreement
  - Make sure that their signature is on the same page as the terms and conditions and details the card number to be used for payment for the rental and to be used in the event of any delayed and amended charges
  - You will need the cardholder's separate agreement to process any additional charges
- Pre-authorise the transaction
- Before the rental period begins you need to make an estimated authorisation request. This is called pre-authorising the transaction and should be based on the:
  - Vehicle rental period
  - Vehicle rental rate and associated taxes
  - Anticipated mileage

Note: Card schemes do not allow the pre-authorisation amount to cover any estimated cost of damages incurred during the rental period.

- Process the transaction
  - If the pre-authorisation request is approved, you get an authorisation code. You can use this authorisation code when you process the payment at the end of the rental period. Find out how to process pre-authorised transactions in your Terminal User Guide
  - If the pre-authorisation request is declined, ask your customer for another method of payment
- To reduce the likelihood of disputes you should let your customer know:
  - The pre-authorisation amount
  - That the available funds on their card will be reduced by this amount
  - That the final bill may be different to the pre-authorisation amount

If the rental period is extended during the rental, additional amounts must be authorised via top-up authorisations. This will ensure that funds are held available when you come to charge the card. You will also need additional authorisation to process the payment. Find out about top-up authorisations in your Terminal User Guide.

Maestro cards do not support pre-authorisation requests.

Note: Authorisation does not guarantee payment. It simply means that at the time of the transaction the card has not been reported lost or stolen and that there are sufficient funds available. Find out more about Authorisations and Referrals.

How to process payments

- You should process the payment after the customer has returned the vehicle
- The exception is for rentals of longer than 14 days. To minimise risk and ensure that payments are processed successfully, we recommend that after a 14-day rental period you close the account and process the required payment up to that date
- If the final bill is higher than the pre-authorised amount, you will need to complete a top-up authorisation. Find out more in Authorisations and referrals or in your Terminal User Guide
- Do not include charges for damages or insurance deductibles in the payment. These charges need to be processed separately as delayed or amended charges

What if the customer cancels or doesn't show up?

- If a customer cancels their reservation
  - You must not process a charge to the card for the booking. If you do, there is likely to be a dispute that may result in a chargeback. If your rental agreement says that a cancellation charge will apply, you will need to contact the customer to arrange for payment by another method
- If they do not cancel, but fail to collect a booked vehicle

- If your customer fails to collect their vehicle within 24 hours of the collection time and did not properly cancel the reservation in accordance with the agreed cancellation policy, you are entitled to charge their card up to the value of one day's rental:
  - Follow the instructions in Card Not Present transactions, using the information the cardholder gave when making the booking
  - On the transaction receipt, write "NO SHOW"
  - Under 'total' enter the rental rate for the vehicle(s) that the customer booked
  - Send a copy of the bill for the no show booking to the billing address the cardholder gave when booking

Delayed or amended charges

There may be times when you need to process extra charges or change the amount agreed because of damages or other costs incurred during the rental period. These extra costs are called delayed or amended charges. It is very important to follow the correct procedure as detailed below.

A vehicle rental company may process delayed or amended charges for fuel, rental damage, theft, 'no- shows', parking tickets and other traffic violations. The cardholder can only be charged for transactions incurred during their rental period that they agreed to in the pre-rental agreement. You should process these as soon as possible following the original transaction, and in any event no later than 90 days from then for Visa transactions. Before you can process these charges you must first provide evidence to your customer to support any claim. Supply documentation from the relevant civil authority including:

- The licence number of the rental vehicle
- Time / date of the violation
- Amount of the charge, in the local currency of that civil authority
- The statute that was violated
- Evidence to prove the cardholder had read the terms and conditions and accepted responsibility to pay for any delayed or amended charges incurred during their rental
- Evidence to prove the cost of any charges, as well as supplying proof that the vehicle was returned damaged or short of fuel
- Copies of any parking tickets or traffic violations incurred during the period of the hire
- Evidence to prove that the cardholder had agreed to the no-show amount and terms and conditions, such as a Click to 'accept' website' box

Special requirements when debiting for vehicle rental damage

In the event you experience a financial loss as a direct result of damages occurring during the cardholder's rental, you must provide the cardholder with written documentation containing the following information within 10 business days of the rental return / check-out date:

- An explanation of the charge, connected to the cardholder's use of goods or services during the rental period
- Any accident, police or insurance report(s)

- For damage to a rental vehicle, at least two quotes from entities that are legally permitted to perform repairs
- A specification of the portion of the damage or loss that will be paid by insurance and the reason why the cardholder is liable for the amount claimed as set by your policy
- Where a Visa card is used by the cardholder, a statement to the cardholder that payment for loss or damage using their Visa card is optional and not an obligation or default (i.e. they can use a different payment method if they wish)

You must wait 20 business days after providing the above documentation before processing a transaction to cover the cost of damage. You should note:

- The cardholder may provide an alternative written estimate for the cost of repairs within 10 business days of receiving documentation, at no cost to you
- If agreement is not reached with the cardholder for the cost of repairing the damage, the cardholder has the right to dispute any transaction to cover damage costs

Disputes (including chargebacks)

Visa cards transactions

In the event that we receive a disputed Visa card transaction, we will write to you requesting documentation to help us in defending the dispute. Should the documentation not be supplied to us within the timescale indicated in the letter this will result in a chargeback debit to your bank account.

When you reply you must supply:

- A dated copy of the original notification letter sent to the cardholder informing them of the delayed or amended charge that they incurred
- A copy of the original rental agreement
- An estimate of the cost of repairs from an organisation that can legally provide repairs in the local currency
- Documentation to support the billing amount of any parking or driving fines. The cardholder cannot be held responsible for any processing charges, or excessive charges where fines have gone unpaid and have therefore escalated
- Relevant civil authority accident report (if applicable)
- Documentation signed by the cardholder, showing that they agree to be liable for any charge incurred during the rental period on the relevant credit card number. The cardholder signature must appear on the same page as the terms and conditions. If the terms and conditions appear on a different page of the contract, then they must be initialled by the cardholder
- All relevant documentation must relate to the correct vehicle registration number
- A copy of the insurance policy of the rental company, if that rental company requires that the cardholder pay an insurance deductible for damages together with a copy of the vehicle rental agreement showing that the cardholder consents to be responsible for the insurance deductible
- Any other documentation demonstrating cardholder liability for the damage

If you do not have this documentation, we will not be able to defend a dispute on your behalf and a chargeback debit will be processed to your bank account.

Please note that any transaction processed in a Card Not Present environment is taken at your own risk and can be subject to a chargeback dispute resulting in a debit from your bank account.

Mastercard transactions

A charge for loss, theft or damage must be processed as a separate transaction from the underlying rental transaction. You must contact the cardholder and advise them of the loss, theft or damage and obtain authorisation from them for any additional charge you process. You should also provide the cardholder with documentation to support the charges as indicated in the Visa section above. If separate authorisation is not obtained from the cardholder it is likely that the transaction will be disputed as a chargeback resulting in a debit to your bank account.

Disputes (including chargebacks) on Mastercard

In the event that we receive a disputed Mastercard transaction, we will write to you asking for documentation to help us in defending the dispute. Should the documentation not be supplied to us within the timescale indicated in the letter this will result in a chargeback debit to your bank account.

Within your reply you must supply:

- Original signed / swiped transaction receipt processed after the original rental charge
- Chip and PIN transaction receipt processed after the original rental charge
- Signed and imprinted receipt form processed after the original rental charge

If you do not have this documentation then we will not be able to defend a dispute on your behalf and a chargeback debit will be processed to your bank account

Note: Please note that any transaction processed in a Card Not Present environment is taken at your own risk and can be subject to a chargeback dispute resulting in a debit to your bank account.

4.6.3 Bureau de Change

If you operate as a bureau de change, you can offer your customers the flexibility to exchange currency and pay by card for a range of different currencies, including Sterling. If you offer both travel agency and bureau de change facilities, you must have separate Customer Numbers and terminals for each facility.

Important extra instructions

To process bureau de change transactions, you must follow the instructions for Card present transactions, as well as those listed below.

The basics

- Your floor limit is zero so you will always need to obtain authorisation
- You cannot accept Maestro cards
- Always advise the cardholder that their card issuer may charge a cash-handling fee
- You must ensure that the additional identity checks are fully completed

Additional identity checks

- Before starting the transaction, ask the cardholder for a second form of identification (ID) – even if the payment card has their photograph on it
- This secondary ID must be a current official government document, such as a passport or a full (not provisional) driving licence, showing the cardholder's signature. Do not accept any other ID. The document must be current and not out of date
- If your customer does not have acceptable secondary ID, you must not go ahead with the transaction. Failure to undertake a secondary ID check may lead to chargebacks if cardholders dispute the transaction
- Examine the secondary ID carefully for any changes to the photograph (if shown) and signature
- Write details of the secondary ID on the front of the point-of-sale (POS) receipt – detailing the type of ID presented and serial number

Additional payment card checks

- The four-digit code, printed above or below the embossed account number on the face of the card, must match the first four digits of the account number
- Write this four-digit code on the front of the point-of-sale (POS) receipt with the words "card prefix" before it
- If you have a UV lamp, put the card under it and check the appropriate in-built security feature. Examples can be found in our Card recognition guide
- You can also use a UV lamp to view the in-built security features of any UK driving licence used as secondary ID

American Express and JCB

Please use the separate instructions provided by these card companies.

4.6.5 Tax free shopping

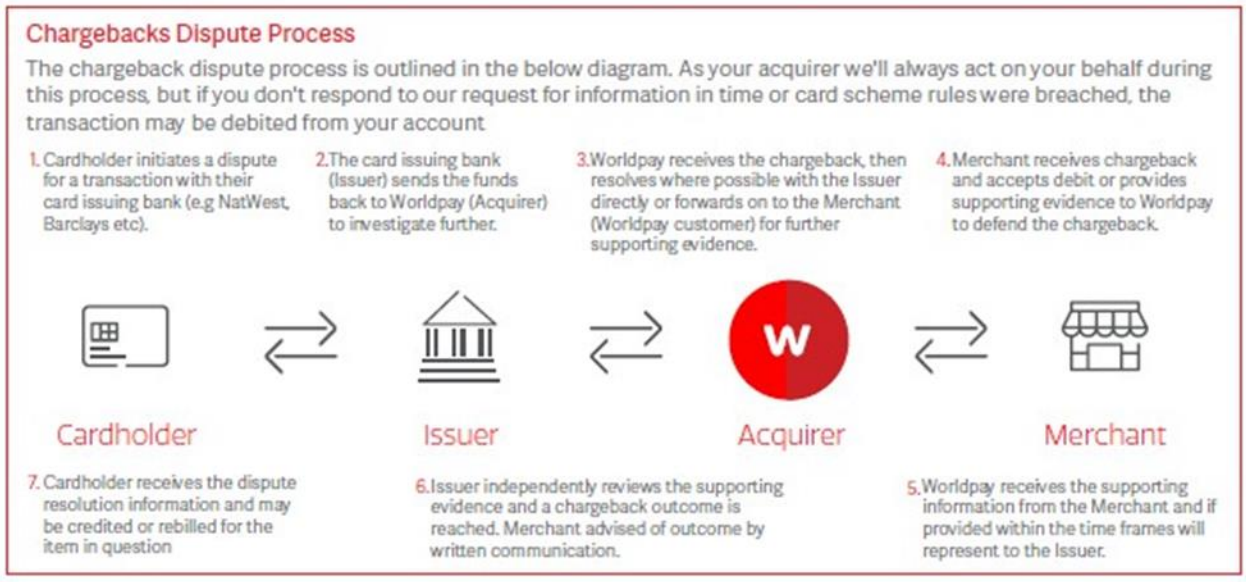
Tax free shopping enables travellers outside of Europe to receive a VAT refund on goods over £30 which they buy in the UK and take home. International shoppers are increasing familiar with the Tax refund proposition and expect retailers to offer this on high value items purchased. Worldpay have partnered with Fintrax and Global Blue, leading providers of Tax free shopping to help with merchant and customer's needs.

If you would like further information or to request a Tax free solution please contact - 0330 134 0187

4.7 Chargebacks

Card transactions are sometimes disputed by the cardholder or the card issuing bank, for example goods not received, transaction not recognised or authorised. When this happens we may contact you requesting further information by sending a Request for Information (RFI) letter. Try to supply the information requested by us in the timescales we specify. If you do not, then it is likely that an RFI may turn into a chargeback which you may be held liable for, even if you have proof that the transaction was genuine. Depending on the nature of a dispute you may sometimes get a chargeback letter without an RFI.

This can happen when it's clear that the right process has not been followed, for example, if you have taken a payment above your floor limit without obtaining a valid authorisation. Another example is when you take an eCommerce transaction without cardholder authentication (e.g. Visa Secure or Mastercard Identity Check), and in this case, the cardholder has declared they did not authorise or participate in the transaction. Where there is a valid chargeback we will write to you to let you know and Worldpay will debit your nominated bank account with the value of the disputed transaction. We will quote the same unique reference number as in the chargeback letter. You are responsible for making sure sufficient funds are in your nominated bank account to meet the chargeback. Failure to do so could result in your card processing facility being withdrawn.



4.7.1 Why chargebacks happen

Here are some of the most common reasons for chargebacks, but this is not a full list. If you are not sure about the reason for a chargeback, please contact the Worldpay helpdesk and select the chargebacks option.

Disputed payments

Some common reasons for disputes include:

- The cardholder claims someone was using the card without his or her knowledge or states that he / she does not recognise the transaction. It could have been stolen and used fraudulently – particularly for MOTO and eCommerce transactions

- There is a processing error, such as the wrong card number or wrong amount was keyed in
- The cardholder disputes some other aspect of the transaction, for example non-delivery, late delivery, unsatisfactory goods or services, or the wrong size / colour / price. For further information about Goods and services disputes

Wrong or suspect card details

There is also a high risk of a chargeback if there was a mistake when the transaction took place. Other common problems are:

- The card is not valid – for example it is out of date. No signature when one was required
- Details on the terminal receipt or voucher don't match the card – i.e. the embossed details on the card do not match the details on the electronic receipt or the details have been manually entered incorrectly - Primary Account Number (PAN) key entry
- Wrong process:
  - Your customer has been billed twice for the same sale
  - The transaction was by PAN key entry, but a separate imprint and signature was not taken on a back-up paper voucher. See Using paper vouchers
  - The sale required authorisation but it was not obtained
  - An authorisation call was made, but the sale was not authorised
  - You have submitted another authorisation request for the same transaction that had already been declined by the Issuer
  - Two or more transactions have been made on one card, for one sale in order to avoid authorisation or referral of the whole as one transaction - known as a 'split sale'
  - You have made a sale not covered by your contract with us – remember you will need an agreement with us which allows you to offer MOTO or eCommerce sales, Recurring transactions and Purchase with cashback
  - An electronic transaction has been stored on your terminal but not sent through to Worldpay within three working days (unless this has been agreed in advance)
  - You have keyed card numbers manually or used paper vouchers when your terminal was working
  - You have processed a card that is not covered by your contract with us
  - You have taken a non-UK-issued Maestro card and keyed in the number by hand
  - You have taken an Electron or non-UK-issued Maestro card and used a paper voucher
- A problem with your response to an RFI:
  - You have not replied to an RFI letter within the given timescales
  - You have replied to an RFI letter with illegible or incomplete documentation
- A problem with a paper voucher:
  - The signature on the voucher is missing, card details not imprinted, impossible to read, or doesn't match the card

  - The voucher supplied doesn't match the customer's voucher
  - The voucher is missing details, such as the date, amount or signature
- A problem with mail order:
  - You have not kept any paperwork signed by your customer that proves the goods were delivered correctly
- A problem with service or changes to specification:
  - You have not obtained confirmation from the cardholder that a service has been completed to their satisfaction
  - There have been changes in the price or specification and you have not obtained the cardholder's signature in agreement
- Other problems:
  - In some other way, you have gone outside your contract with us

Goods and services disputes

These types of chargeback disputes can be difficult to defend and therefore if a customer contacts you with a dispute you should keep accurate records of what is discussed or agreed. Where possible, ask the customer to put the complaint or query in writing / email and have the customer agree in writing to any resolution agreed. Proving the content of a telephone conversation at a later date is virtually impossible and the card schemes do not accept recordings of telephone conversations as evidence.

It is important to be aware that the cardholder does not always have to physically return the goods to you for a chargeback to be correctly raised.

Please also be aware that the use of 3D Secure protects you from fraud-related chargebacks, but chargebacks can still occur from goods and service disputes.

4.7.2 What if cardholders get in touch with you directly?

You and your customer may come to an agreement to issue a refund but this will usually be before to a chargeback is raised. If you want to make a refund after receiving a chargeback or an RFI letter, contact the Worldpay helpdesk to discuss it. This is because a response to the card issuer is still required.

- If the customer just wants their money back under your returns policy, find out more in Refunds
- Never give a refund for any other reason to the cardholder without checking with the Worldpay helpdesk
- If you have received an RFI or chargeback letter, you must never make a refund to the cardholder without consulting with the Worldpay helpdesk first
- If a refund is given then this should be processed to the card used to make the original payment

What is a Request for Information (RFI)?

It's when a card issuer or cardholder instructs us to ask you for details about a specific transaction. If this happens, we will send you an RFI letter asking you for the relevant transaction records.

A card issuer does not need a specific reason to ask for information about a transaction.

We will give you as much information as possible to help you trace the payment. This will include the transaction date, card number and transaction reference. The cardholder's name and address will not be given, in line with the UK Data Protection Act.

What to do if you receive an RFI letter

If you receive an RFI letter, you must send us the information we ask for as soon as possible. You will have a set time to reply – it is very important to respond by the date given or timescales specified.

- Response times are set by us to ensure there is sufficient time to provide a response to the card issuer within the timescales set by the card schemes. As a result, we cannot give you extra time to respond
- If you don't respond or are late with your reply, a chargeback debit may be applied to your account
- If you have Worldpay Online, you will receive an email before you receive an RFI letter

Information to supply if you receive an RFI letter

The more detailed information you give us in response to an RFI letter, the more likely it is that we will be able to answer the card issuer's query or defend your position. However, producing all the documentation you are asked for does not always prevent the card issuer making a chargeback.

You should supply:

- A copy of the invoice for the goods or services provided
- Any documents signed by the cardholder
- Any terms and conditions agreed at the time of the sale. The cardholder's agreement should appear on the same page(s) as the terms and conditions and can be in the form of a signature or "tick box", ideally with the cardholder's name alongside the tick box
- The terms and conditions should not appear on a separate page or hyperlink, they should be stated in full as part of the order and payment process
- If the goods were delivered – evidence of delivery. This should be signed by the cardholder and preferably include the delivery address on the same page as the signature
- For a rental – the rental agreement
- For a refund – the refund voucher
- For MOTO sales – a copy of the sales receipt or Mail Order Telephone Order schedule
- For eCommerce sales – a copy of the source documentation showing all the data captured at the point of sale, including the card number. You may need to print screen images. If necessary, ask your Payment Service Provider (PSP) to help
- For delayed and amended charges (i.e. minibar charges at hotels, parking tickets / damages for vehicle rentals) – a copy of the cardholder agreement to be billed for the additional charge
- Any additional comments relevant to the transaction or dispute – particularly where the cardholder may have approached you directly. You should include details of the outcome of this approach

The transaction documentation should include:

- Truncated card number (first 6 and last 4 digits of the customer's card number)
- Unless it is a PIN verified transaction, the cardholder's signature (in both face-to-face transactions and transactions by post or fax)
- Transaction amount
- Transaction date
- Your trading name and location
- Card expiry date
- Cardholder name and address (generally for Mail Order Telephone Order and eCommerce transactions)
- Description of goods / services provided

4.7.3 Secure record keeping

See Keeping records, for details of how receipts, paper vouchers and other high security items must be securely stored.

4.7.4 If the post is disrupted

If there is a problem with the post, your letters may be delayed, but will send them to you as soon as possible. Even if this written explanation is late reaching you, the chargebacks are debited from your account as usual.

4.7.5 Disputing a chargeback

You can dispute a chargeback that has been applied to your bank account. You will need to provide information relevant to the nature of the dispute. See Information to supply if you receive an RFI letter for details of the type of information you should supply.

Worldpay review any information you can provide in order to defend a chargeback on your behalf however, this must be provided within the required airframes. Your account will only be credited if the evidence provided meets the rules set by the card schemes.

Even if all procedures have been correctly followed and documented, this does not guarantee that you will succeed in disputing a chargeback. The technology we use is designed to ensure that chargeback enquires are resolved efficiently with minimum disruption to your business.

4.8 Merchant location

A Worldpay customer must have a valid business premises at the address given to Worldpay, which forms part of the contract. This is especially relevant for Card Not Present transactions:

- The merchant has permanent premises at which employees or agents conduct business activities and operations required to provide the cardholder with the goods or services purchased for the transaction. This location must be:

- Where the merchant conducts business activities and not from a post office; mail- forwarding address; the address of the merchant's law firm, agent or vendor; or an email address
- The country where those who are employed and accountable for the development, manufacturing, management and sale / distribution of the goods or services purchased in the specific transaction
- Where the merchant assesses sales taxes or value-added taxes related on the transaction activity (in places where taxes apply)
- The jurisdiction whose laws govern the contractual relationship between the merchant and the cardholder

The merchant country location must be the same for any subsequent transactions linked to the purchase, including adjustments, credits (including refunds), chargebacks and reversals.

5 Authorisations and referrals

5.1 Making a referral call

If you have an electronic terminal, the authorisation check is automatic in most cases. Sometimes your terminal will prompt you to make a manual authorisation call, known as a referral.

If you have a mobile or portable terminal, this will have been handed to the customer to input their PIN.

Note: You must always take back the terminal from your customer as soon as the PIN is entered. That way, you will know whether the transaction has been authorised or whether a referral call needs to be made.

You must make this call at the time of transaction, while the cardholder is present. If you are holding the card do not hand the card back to the customer until you have received authorisation and the code has been accurately keyed by you into your terminal.

See Worldpay contact details

5.1.1 Security questions

During some calls, the cardholder may need to answer one or more personal security questions. Explain that this is part of the card issuer's standard security procedure. The Authorisation Centre will usually ask to speak to the cardholder directly. Once your customer has answered the questions, they should pass the phone back to you. You should not use any information which is given to you by the cardholder. Only the Authorisation Centre can give you an authorisation code. You must not accept an authorisation code from anyone else (especially your customer).

5.1.2 If the transaction is authorised

You will be given an authorisation code, which should be keyed into your terminal by yourself when prompted. There's more information in your Terminal User Guide about keying the code.

5.1.3 If you are processing on paper

Write the authorisation code clearly on the voucher in the space provided.

5.1.4 If the transaction is declined

- Explain that the transaction has not been authorised and give the card back to the customer, unless the Authorisation Centre asks you to keep it and it is safe to do so
- If your customer asks why, advise them to contact their card issuer – there is normally a helpline number on the back of the card
- Remember, transactions are declined for many reasons – it may not be your customer's fault

- Make sure you destroy any partially completed sales vouchers in front of your customer
- If your customer still wants to go ahead with the purchase, ask them for an alternative payment method. Remember to check any new card carefully. Find out about Reducing fraud

5.1.5 Suspicious transactions

If you are suspicious about a transaction, follow the procedures to make a Code 10 call detailed in Reducing fraud.

5.1.6 Transaction changes after authorisation and before processing

Sometimes you need to make changes to a transaction after you have obtained authorisation. For example, if your customer decides to buy something different, or not to go ahead at all.

If you process payments electronically, you can cancel the sale on your terminal and it will make the adjustments automatically. This may take a few days to appear on the cardholder's statement.

If you have used a paper voucher for the transaction, cancel it by writing "CANCELLED" across all copies. Then print new vouchers and call the Authorisation Centre again with the following information:

- Card number – 12 to 19 digits across the centre of the card
- Card expiry date
- Your Customer Number
- The Authorisation number you obtained for the original transaction
- The original transaction amount – including any amount of cashback
- The new transaction amount – if it is completely cancelled, just say that it is cancelled

A refund would only need to be processed in the event that the transaction has actually been processed. Find out more in Refunds.

5.1.7 Split transactions

You must not split the sale into two (or more) separate amounts on one card in order to avoid obtaining authorisation for the full amount. If a sale is split in this way, you may be at increased risk of receiving a chargeback for which you will be liable.

5.1.8 Approval response validity

Pre-authorisations (ring fencing an amount from a payment card) can be conducted in certain merchant sectors only and are valid only for prescribed amounts of time.

Mastercard allow pre-authorisations for all transactions. Pre-authorisations expire 31 days following the date they were submitted.

For Visa cards, authorisations differ per sector:

- For Cruise Lines, Hotel / Lodging and Car / Vehicle Rental merchants, an approval response to an estimated authorisation and any subsequent incremental authorisations will expire 31 days after the initial estimated authorisation
- For other rental merchants, trailer parks and campgrounds, an approval response to an estimated or initial authorisation and any subsequent incremental authorisations will expire seven days after the initial estimated authorisation

For Card Not Present otherwise not specified the approval response will be valid for seven days from day of approval. For all other card present retail, prepayments, instalment / recurring, restaurant / bars, amusement parks, delayed charges, in-transit an approval response will only be valid for the day of the authorisation.

6 All the jargon explained alphabetically

A B C D E F G M N P Q R S T V W 3

A

Acquirer – a financial institution that is a member of the card schemes and provides facilities for businesses to accept card payments and receive these funds. Also known as a 'card acquirer'.

Address Verification Service (AVS) – fraud-prevention service that verifies the numerical elements of a customer address against a card.

Approved Scan Vendor (ASV) – a provider approved by the PCI Security Standard Council to carry out a vulnerability scan of your systems. Should be contacted as part of the PCI DSS compliance process if external vulnerability scans are required. A list is available from the PCI SSC website. Find out more in Payment security.

Authorisation – the process whereby a transaction for a specified amount is approved or declined by a card issuer or an acquirer on behalf of a card issuer. This approval confirms that the card number is valid, that as at the time of the transaction the card has not been reported lost or stolen and that funds were available. It does not confirm the authenticity of the card presenter or the card, or guarantee settlement of the transaction. The authorisation request may be generated by a customer terminal and processed electronically or may include voice contact between the customer and the acquirer. Find out more about Authorisations and referrals.

Authorisation call – a telephone call made to obtain authorisation for a transaction.

Authorisation code – a code (which must not be all zeros) generated by a card issuer or by an acquirer on behalf of a card issuer when an authorisation request is approved. Find out more about Authorisations and referrals.

B

Banking Summary Vouchers – only needed if you are using paper vouchers. Find out more in Terminal failure.

Batch – a collection of transactions held at a single terminal or outlet. A batch may contain any number of shifts or days data.

Batch totals – find out about these in Reconciling your invoice.

C

Card acquirer – see Acquirer.

Card issuer – the organisation that issues a payment card to the cardholder.

Card Not Present transactions – card payments processed when the card and cardholder are not present during a transaction. e.g. eCommerce, Mail Order Telephone Order.

Card number – the long number across the front of a card, also known as the PAN (Primary Account Number). Card present transactions – Card payments processed where both the card and cardholder are present during a transaction.

Card processing facility – the agreed products and services provided by Worldpay which allow you to accept and process card payments.

Card schemes – Visa, Mastercard, American Express, Diners / Discover, JCB (Japan Credit Bureau), China Union Pay and others. These independent organisations have set up systems for issuing and accepting card payments worldwide, some using local financial institutions as agents.

Card Security Code (CSC) – this is a three-digit code at the end of the signature strip or in a separate white box next to the signature strip on a card. American Express cards have a four-digit CSC on the front of the card. Never record the CSC – it must only be used for one transaction. The Card Security Code (CSC) is sometimes also called the Card Verification Value (CVV or CVV2) or Card Verification Code (CVC or CVC2).

Card testing – when a fraudster places an order over the phone or online to check if the card details they have will be authorised. Find out more in Reducing fraud.

Card Verification Code (CVC or CVC2) – refer to Card Security Code.

Card Verification Value (CVV or CVV2) – refer to Card Security Code.

Cardholder – the person to whom a card is issued, or an individual authorised to use the card.

Cardholder authentication – Worldpay cardholder authentication is a security tool designed to help you authenticate cardholder details in the online eCommerce environment. It brings together Mastercard Identity Check and Visa Secure and is also referred to as '3D Secure'.

Cardholder data – the data obtained as part of a transaction, including:

- PAN / card number
- Cardholder's name
- Expiry date
- Service code
- Sensitive Authentication Data

Chargeback – the term used for the process whereby a card issuer can dispute part or all of the value of a transaction on behalf of the cardholder via your acquirer. Examples can include a cardholder stating the transaction is fraudulent, or a cardholder states the goods have not been received. If a chargeback is deemed to be valid then this will result in your account being debited. Find out more in Chargebacks.

Chip and PIN – Chip and PIN is a programme aimed at Reducing fraud for those transactions where the cardholder and card are present at the time of the transaction. The chip (silver or gold coloured square on the front left side of the card) is embedded into a card to provide highly secure memory and processing capabilities.

In addition to holding the same personal data as the magnetic stripe, the chip provides additional security features to safeguard against counterfeiting.

The PIN is a four-digit number (or longer) that the cardholder enters into the PIN pad instead of signing a card receipt. Liability for counterfeit card transactions and lost and stolen card fraud now stands with the party in any transaction who is not chip and PIN compliant. Where all parties are compliant, counterfeit transactions are reduced significantly and there will be no recourse by the cardholder saying they did not authorise the transaction.

'Code 10' call – a call made to the Authorisation Centre if you are suspicious about a transaction. Find out more in Authorisations and referrals.

Compromise – intrusion into computer systems where unauthorised disclosure, modification or destruction of cardholder data is suspected.

Contract – your formal agreement with Worldpay.

Credit card – a payment card linked to an account which may be settled in full by a set date or repaid over a period of time, subject to minimum monthly repayments being made. Interest will normally be charged to the cardholder on any outstanding balance. Examples of credit cards include Mastercard and Visa.

Customer Number – the unique number you are given when you sign a contract with us which identifies your business on our systems. This is also known as the Merchant ID (MID).

D

Data controller – The Information Commissioner's Office website defines this role as:

"...a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed."

Debit card – a card that enables a customer to transfer money from a current account or other similar account to make a payment. Examples of debit cards include Maestro, Debit Mastercard and Visa Debit.

E

eCommerce transaction – a sale made over the Internet. You need a special agreement with us to handle these transactions.

Encryption – a way of converting information into an unintelligible format that allows storage or transmission of data without compromise.

Express checkout – a service available to hotel businesses. Find out more in Hotel Services.

F

Firewall – hardware, software, or both that protects data on a network or computer from intruders from other networks. Typically, an enterprise with an intranet that permits workers access to the wider Internet must have a firewall to prevent outsiders from accessing internal private data resources.

Floor limit – an amount agreed between Worldpay and our customer for a single transaction over which authorisation and approval must be obtained. Any transactions over the agreed floor limit will require authorisation to be obtained.

- In most instances floor limits will be set at zero. However, depending on the nature of your business, you may have different floor limits for transactions on your terminal, transactions using paper vouchers and for any Card Not Present transactions. Details of your floor limits can be found in your Worldpay contract
- Make sure all your employees know the right floor limit for each type of sale, but do not write floor limits down where customers can see them, or tell customers what they are
- Your electronic terminal has pre-programmed floor limits and will automatically telephone for authorisation when necessary
- The floor limit applies even if the cardholder asks to pay part in cash and part by card. If the total amount of the transaction is over your floor limit, telephone for authorisation – even if the card payment amount is below the limit. Tell the Authorisation Centre that it is a 'split sale'

G

Guaranteed reservation – a service available to hotel businesses. Find out more in Hotel Services.

M

Magnetic Stripe Data ('Track Data') – data encoded in the magnetic stripe on the back of cards which is used for authorisation during transactions when the card is presented. For chip and PIN transactions, the terminal uses equivalent data contained on the chip – this data should not be retained.

Mail Order Telephone Order (MOTO) – transaction where the order and card details are taken over the telephone or by post. Find out more in Mail Order / Telephone Order transactions.

Management Information (MI) – reports and analysis for monitoring your transaction processing and charges. Find out more in Reconciling your invoice.

Mastercard Identity Check – a method introduced by Mastercard to provide an additional, secure cardholder verification process before an eCommerce transaction proceeding over the Internet. Formerly known as Mastercard SecureCode.

Merchant ID (MID) – see Customer Number.

Merchant Operating Instructions – the original name for this guide which we are now referring to as our Customer Operating Instructions.

N

Network – a network exists if two or more computers are connected.

P

Paper vouchers – used for manual payment processing. Only to be used in emergencies - see Terminal failure.

Password – a mixture of characters that can be used to authenticate an individual, allowing them access to a system, computer or network.

Payment card – a generic term for any plastic card – credit, debit, charge and so on – which may be used on its own to pay for goods and services, or to withdraw cash.

Payment Card Industry Data Security Standard (PCI DSS) – a compliance requirement that aims to ensure that cardholder information is always stored, processed and transmitted securely.

Payment Card Industry Security Standards Council (PCI SSC) - an organisation founded by five global payment brands -American Express, Diners / Discover, JCB International, Mastercard Worldwide and Visa Inc.

Payment Gateway – this is your 'virtual cash till' for eCommerce transactions.

Payment Service Provider (PSP) – PSP's offer retailers online services for accepting eCommerce (internet) payments by a variety of payment methods including Payment Cards.

PCI SSC ISA - Payment Card Industry Security Standards Council Internal Security Assessor.

Personal Identification Number (PIN) – A set of digits (usually four) entered by the cardholder to authenticate a chip and PIN transaction.

Primary Account Number (PAN) – the cardholder number of up to 19 digits which is usually, although not always, embossed on the front of the card.

Purchase with cashback (PWCB) – an optional transaction type where a customer may, with the approval of Worldpay, allow a cardholder to draw cash up to an agreed limit as part of a standard sale transaction. This is also known as 'cashback'. Find out more about Purchase with cashback.

Q

Qualified Security Assessor (QSA) – these organisations are trained on PCI DSS by the PCI Security Standards Council and can confirm a customer's compliance status or simply offer support in reaching compliance.

QSA – Qualified Security Assessor – the PCI Security Standards Council maintains a list of all persons qualified to assess your systems and processes. For a list, see the PCI SSC website.

R

Reconciliation – The method by which a customer compares the business undertaken at their terminal with that recorded by the acquirer and credited to their bank account.

Recurring transactions – transactions that are authorised by a cardholder to be submitted at regular intervals (i.e., weekly, monthly, quarterly, etc.) and on a predetermined basis.

Referral – when your terminal prompts you to make a manual authorisation call. See Authorisation call.

Request for Information (RFI) – a request by either the card issuer or the cardholder for further information about a transaction.

S

Secondary Identification (ID) – additional identification that the cardholder may need to produce to prove their identity. This is usually a current government document with a photograph and address. Find out more in Reducing fraud.

Self Assessment Questionnaire (SAQ) – part of the Payment Card Industry Data Security Standard (PCI DSS) compliance process. Validation tool intended to help customers and service providers in self- evaluating their compliance with the PCI DSS. You can download the appropriate version from the PCI SSC website.

Sensitive Authentication Data (SAD) – this is defined as full magnetic stripe data, CAV2 / CVC2 / CVV2 / and PINs / PIN blocks – this data should not be retained by the customer.

Service code – messages contained within a card's magnetic stripe or chip that tells a terminal which process to follow for a transaction.

Service provider – business entity that is not a payment card brand member or a retailer directly involved in the processing, storage, transmission and switching of transaction data, cardholder data or both.

Split sale / Transaction – where a sale is split into two (or more) separate amounts on one (or more) card/s in order to avoid obtaining authorisation for the full amount on one card

Supervisor code – code set by terminal manufacturer which should be personalised and changed regularly to prevent compromise.

T

Terminal Receipt – the paper receipt that is printed when a transaction is completed.

Terminal User Guide – the instructions that came with your terminal. It is important to read these carefully together with these Customer Operating Instructions.

Top-up Authorisation – you will need top-up authorisation on pre-authorised transactions where the amount of the final transaction exceeds the original pre-authorised amount by more than the tolerance allowed by the card scheme.

'Track Data' – information about the card and cardholder that is kept in the card's magnetic stripe or chip. (See also 'Magnetic Stripe Data').

Transaction – a card payment in exchange for goods or services that you are provide which fall within the nature of business you described to us in your application form or which you subsequently notified us of in writing.

Transaction amount – the full amount the customer pays for the goods or services, including any VAT.

Transaction data – information that identifies the purchases a cardholder makes with their card.

V

Visa Secure – a method introduced by Visa to provide a secure cardholder verification process for eCommerce transactions. Formerly known as Verified by Visa.

Vulnerability scan – externally-facing scans of your Internet-facing IP addresses that check for unknown vulnerabilities in your network.

W

Written authority form – the form your customer needs to complete to authorise you to take recurring transactions from their card. Find out more in Recurring transactions.

3

3D Secure – see Cardholder authentication.

If you can't find the answer to your question in this guide then please get in touch. We are open 24 hours a day, every day of the year.

7 All the contact details you need

Our UK based Support team are on hand to help 24/7, 365 days a year so we're there whenever you need us.

Authorisation Centre

Authorisations – Card present transactions

UK customers: 0345 7 600 500*

ROI customers: 1 800 700 100

International customers: +44 1285 600500

Authorisations – Card Not Present transactions

UK customers: 0345 760 0530*

ROI customers: 1 800 700 300

International customers: +44 1285 600530

Name and Address checks

UK customers: 0845 300 7929

ROI customers: 1800 700 300

Worldpay helpdesk

You'll need your Customer Number when calling our Helpdesk. You can find this on your Welcome to Worldpay email / letter or one of your monthly invoices.

UK customers: 0345 7 61 62 63* (Text phone users may call 18001 0845 3003889*)

ROI customers: 1 800 24 26 36 (or National 01 702 5845)

International customers: +44 1720 616263

*Note: Calls to 03 numbers cost no more than calls to geographic numbers (01 or 02) and may be included in any free call packages.

Please refer to Ofcom Call costs guide or check with your telephone provider for the latest rates. Paper tally rolls for card payment terminals

Terminal tally rolls

If you need more terminal tally rolls for your terminal, you do not need to contact the Worldpay helpdesk. Instead you should contact the Worldpay approved supplier below or log on to the Worldpay Accessories and stationery website - Worldpay Accessories.

UK customers: 0800 289 666 (Freephone)

ROI customers: 00800 9899 2000

eCommerce helpdesk - Existing eCommerce customers

UK customers: 0330 333 1233

ROI customers: +44 870 366 1233

New sales

UK customers: 0808 253 0519 (Freephone) or 02890-099201 from Northern Ireland

ROI customers: 04890 099 201

Other ways to contact us

Our contact details are available on the website www.worldpay.com

To contact Worldpay in writing, please write to:

Worldpay
Gateshead Card Centre
Victory House
5th Avenue
Gateshead
NE11 0EL
United Kingdom

8 About this guide

8.1 Changes

Version	Change description	Date
1.0	First version	October 2019

8.2 Legal