**worldpay**

# Merchant Operating Instructions

UK and Republic of Ireland

January 5, 2026

# Contents

# 1    Your Merchant Operating Instructions

Make the most of accepting payments through Worldpay with our Merchant 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 Merchant Operating Instructions form part of your contract with Worldpay. It's also important to make note of:

- Your current Worldpay Terms and Conditions
- Any prompts displayed on your payment terminal
- Any updates and specific instructions we occasionally send you

worldpay

# 2 Important information ...........................................................................................5

# 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 noted in your 'Welcome to Worldpay' email/letter and you can find it 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 you. Your application form (which also forms part of your Worldpay contract) shows which services you have requested.

You must only accept payments for the goods and/or services that you told us your business provides 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/ update your details, you must notify us as soon as possible. All changes can be made on Worldpay Dashboard, an online platform where you can manage your Worldpay account. Alternatively, you can call us. You are required to notify us if you change any of the following:

- 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
- Your website address and/or intend to sell via a new website address
- The length of the guarantees or warranties offered on your products
- The legal entity of your business – for example from sole trader to limited company
- Your bank account details
- Postal, trading address or registered address
- Trading name
- Email address

- Contact name

- 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 card product types issued in the EEA anymore

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

## 2.3.1  Customer Due Diligence (CDD)

We may periodically ask you to update or re-verify your information to meet regulatory requirements. It's a regulatory obligation to gather and verify the information of your business controllers and that of any beneficial owners.

Merchants can use Worldpay Dashboard to upload information and documentation that we request to complete our periodic review of your account. This helps us to allow your business to continue to operate in a secure payment environment. Click here to learn more about Customer Due Diligence, why we do it and how to provide your information.

## 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 EUR (or GBP equivalent), then you can give one month's notice at any time to terminate your Worldpay contract for acquiring services. For merchants who do not fit within these criteria, or where we have agreed to provide you with other products or services and/or different contracts lengths, then 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 ....................................................................................7

# 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

- Only use card and verification details for completing a card transaction

- Not pass this information to anyone else

- Only 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

    – 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

- Give Worldpay 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

Card Present (CP) and Card Not Present (CNP) transactions have different risks associated with them. CNP transactions carry a greater risk of fraud as you are 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 terminal prompts

- If suspicious during card-present transactions, contact the Authorisation Centre and select 'Code 10' call and follow the instructions provided. Be discreet and prioritise people's safety

- Keep your supervisor card/code secure and change it regularly to prevent fraudulent refunds

- Do not allow third-parties to authorise/process transactions with your facility to avoid contract breaches and liability for fraud/chargebacks

- Keep the terminal on-site and in sight during transactions. Retrieve it immediately after PIN entry

**worldpay**

- Train staff to handle terminals and strengthen on-site controls to prevent card fraud

- Ensure staff read this guide and other fraud prevention materials thoroughly

> *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: Mail order/telephone order (MOTO) | Card Not Present transactions: eCommerce |
|---|---|---|
| Face-to-face  transactions, such as chip and PIN, where  your customer and their card are present at the point of sale. | Transactions where  your customer and the card are not present  at the time of the transaction. | Online sales (including retailer  apps on mobile devices)  where  the customer and their card(s) are not present at the point of sale. |

### 3.2.2   Transaction Monitoring

On occasion, our Transaction Monitoring team may contact you to discuss payments you have processed. As part of their review, they may request documentation from you to further understand your business and such payments. During this time there may be a short delay in settlement, however you would be kept informed throughout and can contact the team for updates via email or telephone.

**Withholding payments**

We may withhold payments from your business while we complete an investigation into whether a genuine transaction has taken place, which relates to goods and services provided by your business. We aim to complete investigations in a timely and efficient manner, however timescales may vary.

To protect your business from fraud, we strongly recommend undertaking the appropriate customer diligence and where possible, initiating transactions via a secure payment method. If you have a physical point of sale (POS) device, contactless and chip and PIN are the most secure. If you process via e-commerce, 3DS is recommended as it applies additional security onto the authorisation of the transaction.

### 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](#).

## Warning signs of potential fraud

- Random, careless or bulk purchases – fraudsters often buy easily to sell goods
- Frequent visits – customers making repeat purchases may be exploiting card acceptance
- Nervous or hurried customers may indicate fraudulent activity
- Cards signed in felt-tip pen may conceal the original signature. All cards should be signed in ballpoint pen
- Distractions – customers causing interruptions during transactions might be attempting fraud; always keep the terminal in sight to avoid interference from the fraudster
- Fake calls – be alert for fraudulent authorisation calls. Neither Worldpay nor banks will provide authorisation codes over the phone. Cancel such transactions and perform a 'Code 10' call
- Impersonation scams – report any calls requesting card details from supposed officials to the [Worldpay helpdesk](#)
- Contactless abuse – Monitor shoppers making multiple low-value contactless purchases instead of a single transaction

### *Take extra care when a signature is needed*

Cards that do not have chip and PIN need to be verified with 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. Usually 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 and check the following:

- Security features of the card. Find out more in our [Card recognition guide](#)
- The cardholder's signature matches that on the back of the card
- The spelling on the card is the same as the signature – fraudsters may spell the name incorrectly

- The signature strip for tampering e.g. another strip placed over the top of the original one. If "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 to the cardholder 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.

You should have an agreed process to follow in the event your staff encounter criminals. Staff should follow these instructions, as well as those in your own policy.

Preserve the card:
- Cut off the bottom left-hand corner (as seen from the front), don't cut the card in half

- Handle it by the edges to preserve fingerprints

- 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

**Voucher or receipts**
- Keep any vouchers/receipts

- Don't pin or staple anything to it

- Give to the police

**Video/CCTV**

- If you have a video surveillance system, keep the recording and give a copy to the police

- Note down a description of the person who presented the card as soon as possible, noting unique features (e.g. their

accent), 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 safe as this may enable you to claim a reward

## If someone leaves a card behind

- Store it safely 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 happy with the cardholder's identity, give them the card
- If you are suspicious, ask them to provide additional proof of identity, such as a passport or driving licence. If you are still not satisfied, 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. Cut off the bottom left-hand corner (front-facing). Do not cut through the signature strip, magnetic stripe, hologram or chip. Send the pieces and provide 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 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 you are ever suspicious, 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 appeals to fraudsters. Take extra care with CNP payments because you will be financially liable if a transaction is confirmed as invalid or fraudulent.

**Warning signs of fraud in Mail Order Telephone Order transactions**

- Bulk orders: Be cautious of customers purchasing large quantities of the same item
- First-time shoppers: Exercise extra vigilance with new customers placing multiple orders
- High-value purchases: High-value orders, especially for easy to sell items like jewelry or electronics, may indicate fraud. Verify customer identity with ID e.g. passport or driving licence

- Hesitant information: Customers unsure about personal details may be using false identities
- Name discrepancies: Same name but different title can suggest misuse of a family member's card
- Easy sales: Be wary if customers are uninterested in product details and focus solely on delivery

- Suspicious card use:
    - Multiple cards with matching billing but varying shipping addresses
    - Numerous transactions on one card in a short time
    - Cards with similar BIN numbers used after declines
    - Multiple cards offered without hesitation after declines
    - Orders to a single address using various cards
    - Urgent delivery requests, often linked to quick resale scams
    - Overseas shipping, especially for new customers or large orders
    - Different shipping from billing addresses, often linked to fraud
    - Repeated use of the same delivery address for similar orders
    - Requests to send funds abroad, often for services like couriers

*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](#).*

## Warning signs for eCommerce transactions

- Risk alerts: Pay attention to alerts from payment service providers or banks indicating potential fraud
- Repeated attempts: Multiple transactions using similar shopper details such as name, email, or IP address
- Inconsistent shopper information: Different shopper details with one common element, such as the same IP address
- Multiple cards: Same shopper using several cards, especially with similar numbers
- Card testing: Sequential card numbers or similar digits in attempted payments
- Nonsensical details: Unusual shopper information, like nonsensical email addresses
- High-value transactions: Transactions exceeding your normal daily processing amounts may indicate fraud
- Mismatched security checks: CSC or AVS mismatches should prompt rejecting the transaction or further investigation
- Country mismatches: Billing, issuer, and IP country mismatches, especially from high-risk areas of online fraud
- Unusual delivery locations: Delivery to unfamiliar or high-risk countries
- Freemail addresses: Use of free email services are often linked to fraud as they are relatively anonymous
- Unrelated email names: Email addresses not matching shopper names
- Urgent orders: Requests to expedite orders shortly after it was placed

- Bulk purchases: Large quantities of the same item, such as multiple pairs of shoes
- Indiscriminate buying: Unusually large or varied orders
- Address changes: Requests to alter delivery addresses, especially to high-risk areas
- Reckless card sharing: Shoppers providing card numbers via unencrypted emails are not PCI DSS compliant
- Excessive card details: Shoppers providing a high volume of card or billing information
- Payment alterations: Requests to modify payment details for legitimacy
- Inconsistent communication: Discrepancies between shopper's name, email, and purchased goods/services

## How to combat eCommerce fraud

To help reduce the exposure of your business to eCommerce fraud, consider the following:

- Industry tools: Use cardholder authentication and security measures like 3D Secure, CSC, and AVS checks. Contact Worldpay or your Payment Service Provider (PSP) for more details

- Transaction screening: Implement risk scoring and alerts to flag suspicious activities. You can develop an in-house system or seek assistance from your PSP

- Data comparison: Compare new shopper data with existing records. Keep track of past fraud attempts and chargebacks, and reject orders with matching details

- Pattern recognition: Monitor for patterns, such as repeated use of the same name, email, or IP address, and investigate any suspicious activity

- Identity verification: If suspicious, verify the shopper's identity by testing their contact details. Consider requesting copies of utility bills, card statements, or identification documents, ensuring sensitive details are obscured

- Fraud policy: Develop a clear fraud policy and train staff to respond appropriately when fraud is suspected

## What else to consider

- Verify customer authenticity: Confirm customer details like residential address and phone number, possibly using publicly available data
- Monitor for imposters: Regularly search online for websites using similar names to yours, which might be set up to impersonate your company
- Utilise fraud screening services: Engage with companies like PSPs that offer:
  - Parameter-based technology to filter card transactions
  - Third-party name and address verification
  - Cardholder data validation
- Invest in fraud prevention tools: Consider using fraud prevention software, as the benefits often outweigh the costs

For more information on Worldpay's fraud prevention products, please contact us or 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 further action if you are in any doubt about the transaction, e.g. request a landline number and check with a directory enquiries service.

Although these measures may help in reducing 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:

- Ensure 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 frontline 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 Payment Card Industry Data Security Standard (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 always remain safe.

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 third-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 merchants' PCI DSS compliance status to the card schemes (including Visa and Mastercard) on a quarterly basis. Any merchant who does not comply runs the risk of fines from the card schemes. A monthly non-compliance fee is charged by Worldpay if a merchant is not compliant within 60 days of joining us.

In addition, merchants 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.

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.

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

### 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 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 1 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 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.

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

If you do not store any cardholder account data in your own systems, you must still verify the PCI DSS status of any third-party who acts 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
- 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 able 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
- What resources are needed, and how long this work is likely to take

Consider putting a project team in place and discussing 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.

The aim of PCI DSS is to protect the security of your business and customers' data, not the compliance process.

Delegate specific remediation activities within your project team 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 to protect your business and customers against the risk of data compromise.

*Step 7: Certification*

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 with your own messaging and marketing collaterals.

## 3.3.6    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' 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 annual on-site audit and a quarterly vulnerability scan. 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 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, credit or commercial cards (i.e. as used by businesses), which are issued in the European Economic Area (EEA). However, you must accept all 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 by calling us on:

UK merchants: 0800 289 666 (Freephone)
ROI merchants: 0 0800 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
JCB
Diners/Discover
American Express

The card scheme names – Mastercard, Visa, Visa Electron, JCB, Diners/Discover, Maestro, and American Express – and their associated decals, signage, symbols and logos are registered trademarks. As our merchant, you are

25

allowed to use them in your advertising, providing you follow their guidelines. You must not mischaracterise any card, account access device, or payment device bearing any of the card schemes' (or their affiliates') trademarks.

[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.

## 4.1.2   Using your terminal

Terminals supplied by Worldpay must always be connected and powered on. 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 except for IP broadband or mobile terminals. These terminals connect directly to the internet. 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.

| Terminal type | Call costs |
|---|---|
| Standard dial-up phone line (PSTN) | **Free** - Standard connection cost for 0800 numbers[1] |

[1] Current as of 4 June 2024

| Terminal type | Call costs |
|---|---|
| IP broadband connection | No charge |
| Mobile terminal | 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 an IP broadband connection, contact us on 0345 761 6263 (UK) or 1 800 242 636 (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 note:

- 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
- 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 receive 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
- Help 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.

*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. All terminals must now be able to accept contactless payments 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. 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.

## 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.

These steps help ensure secure and efficient handling of card transactions while minimizing the risk of fraud and chargebacks:

- Cardholder PIN issues:
    - Incorrect PIN: Cardholders typically have three attempts to enter their PIN. Follow terminal prompts to determine if another verification method is possible or if an alternative payment is needed
    - Forgotten PIN: If your terminal allows PIN bypass, follow the instructions. Otherwise, request another payment method
    - Locked PIN: Advise the cardholder to contact their issuer for a new PIN
- Chip reader problems:
    - Card cannot be read: Try reinserting the card. If unsuccessful, the card may be damaged, prompting a magnetic swipe. If still unreadable, request another payment method
    - Fraud risk: Swiping or manually entering a chip card could result in chargebacks if fraudulent
- Magnetic stripe transaction failures:
    - Stripe unreadable: Attempt another swipe. If unsuccessful, key in card details using the terminal's number keys. Follow prompts for necessary information, including the Primary Account Number (PAN)
    - Manual imprinter: Use a manual imprinter to create a paper voucher, marking it "no value, swipe failure." Ensure the cardholder signs both the voucher and receipt, and verify the signature matches the

card's reverse
- – Paper voucher: Retain the voucher for potential disputes, but do not send it for processing. Explain the process to the cardholder and reassure them the voucher is for record-keeping only
- Terminal failure:
  - – Backup pack: If the terminal fails completely and you have a backup pack, you can continue accepting card payments using paper vouchers and an imprinter. Find out more in [Terminal failure](#)

Please use the separate instructions provided by American Express for American Express transactions.

## 4.1.4 Purchase with cashback

Purchase with cashback (PWCB) may be good for your business and your customers. Being able to get cash when spending at a local outlet is a convenient way to save time. This could encourage customers to visit more regularly – potentially increasing sales. From a security perspective, PWCB also reduces the amount of cash held on the premises, making your business less vulnerable to crime.

**Offering PWCB**

- You will need Worldpay's agreement
- 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 (or 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 (€100 for ROI)
- Your customer must use one of these cards:
  - – Maestro
  - – Visa Debit[1]
  - – Visa Electron[2]
  - – European issued Debit Mastercard

*No new Visa Electron cards are being issued, and the brand was 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, you can refer to the Product Help Centre 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 or PIN device
2. Follow terminal prompts to enter the full transaction amount and the PWCB amount separately
3. The terminal will usually request a PIN. If not, this may be a non-UK-issued card. You should check the card's security features and ensure it's undamaged. Confirm the transaction amount with the cardholder
4. Most terminals will auto-authorize. If prompted, call the Authorisation Centre immediately
5. Only provide goods and cash after receiving authorisation and completing the transaction
6. Wait for the terminal to print a receipt
7. Confirm the transaction, then give the customer their purchases, cash, card, and 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 would 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 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 the Product Help Centre. 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). You 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.

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 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 the sliding bar to the left
2.  Carefully slot the card into the imprinter with raised numbers facing up
3.  Place the Worldpay voucher on top of the card and tuck it in
4.  Move the bar left to right and back without applying force
5.  Ensure numbers have printed clear. If not, destroy the voucher and retry
6.  Contact Worldpay helpdesk if imprinter issues persist. Do not handwrite card details
7.  Fill out transaction details clearly with a ballpoint pen, including amounts
8.  Have the customer sign the voucher while you hold the card. If you are suspicious the signature does not match, call the Authorisation Centre and select the 'Code 10' option
9.  Only give goods after authorization and transaction completion
10. Write authorization code on the voucher if given
11. If authorisation is not given, destroy incomplete voucher and ask for another payment method.
12. Return the card, the top copy of the voucher, and goods to the cardholder
13. Keep remaining voucher copies for processing and 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. Use the imprinter to take an imprint of your Banking Summary Card and the Banking Summary Voucher.
2. On the back of the white copy, list individual sales voucher amounts and calculate the total
3. On the blue copy, record the number and total value of sales and refund vouchers, calculating the net total (use a minus sign for negative values)
4. Sign and detach the white copy, organise it with sales vouchers in listed order, avoiding staples or clips.
5. Keep blue and yellow copies for record-keeping and bank reconciliation
6. Please send the white copies of the Banking Summary Voucher and paper vouchers within three working days to:

VPU Worldpay

Victory House

5th Avenue

Gateshead

NE11 0EL

United Kingdom

You can submit up to 200 vouchers with a Banking Summary Voucher. If your list of transactions will not fit on the back of the Banking Summary Voucher, 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

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

### 4.2.3  Reducing fraud and chargebacks

Most eCommerce sales are genuine. However, because the Internet is anonymous – you don't see the card or the shopper – some people see it as an easier 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 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. 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 (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

All eCommerce transactions must be authorised.

*Authorisation of a transaction does not guarantee payment. An authorisation only checks the availability of funds and that the card has not been reported lost or stolen at the time of the transaction. 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 is a security tool for verifying cardholder details in online eCommerce. It uses 3D Secure schemes like Mastercard Identity Check, Visa Secure, and American Express SafeKey, to confirm the cardholder's identity during online purchases.

Shoppers may be asked to enter a unique password or answer security questions at checkout, facilitated by their card issuer. It appears as a security prompt on your payment page, taking only seconds with minimal disruption to the sale process.

It enhances security by proving the cardholder's identity, reducing the risk of chargebacks due to fraudulent claims. Mastercard Identity Check is mandatory 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

39

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.

*Information about your business*

As a minimum, your website must clearly display:

- Your business name, website domain, full company name, incorporation/registered number, and physical and online addresses to ensure cardholders can identify you. Maintain consistent identity across all communications

- A customer service phone number (excluding mobile numbers) with country and area codes for dispute resolution. Include both domestic and international numbers if applicable. Use a direct email address for rapid contact, preferably for your customer service desk

- Your VAT registration number

- List any Trade Association memberships, including registration numbers and contact details, along with the code of conduct

- Details of any professional body memberships, including your professional title, the granting member state, and applicable professional rules with electronic access information

- Disclose merchant outlet location accurately before purchase completion to inform about fees, taxes, and shipping times

- The merchant outlet country on the checkout screen or within the checkout process webpages

*Information to provide before an order is placed*

- Product details: Describe products/services, guarantees, shipping practices, and export restrictions. Clearly state expected delivery times

- Pricing: Include total costs, shipping, handling, and taxes. Quote prices in agreed currency and clarify currency

conversion details

- Terms and Conditions: Provide easily accessible terms, conditions, and procedures for cardholder commitments in a storable format

- Returns Policy: Clearly state refund policy, including shipping, handling, and tax charges

- Cancellation Policy: Explain cancellation terms before payment. For free trials, obtain explicit consent for subscription, confirm details, and provide easy cancellation methods

- Payment commitment: Clearly indicate payment commitment when entering account number, with an option to cancel. Use account numbers only for payment

- Order Instructions: Provide clear order completion instructions and error correction methods

- Languages: Specify languages available for order completion

- Card Details Storage: Obtain formal agreement before storing card details for future use

- Card Scheme Logos: Display logos on the website at the point of cardholder interaction

***Information to provide after an order is placed***

- Error correction: Offer accessible methods to correct input errors post-confirmation

- Order acknowledgment: Send an email acknowledging order receipt promptly

- Confirmation: Provide durable confirmation including:

- Business name and address

- Description of goods/services

- Price, taxes, and delivery costs

- Payment and delivery arrangements

- Address for complaints

- Information on 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 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 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 the risks to your business, as 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 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 online card payments. 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.

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

website

## 4.3    Mail Order and Telephone Order payments

This section covers only Mail Order and Telephone Order (MOTO) sales. Find out more about taking online card payments 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

### 4.3.2   Reduce the risk of fraud

Most MOTO sales are genuine. As they are 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 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 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

43

- Chosen delivery address – if different from above
- Card Security Code (CSC) - three-digit code at the end of the signature strip (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.

### 4.3.4   The Data Protection Act 2018

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 register 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 refer to the Product Help Centre 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. (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 provided are exactly those they have registered with their card Issuer (i.e. as it will appear on their statement) to avoid an 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<br>22 High Street<br>Anytown<br>AB21 2BB | Mr A N Other<br>Flat 4<br>22 High Street<br>Anytown<br>AB21 2BB |
|---|---|
| You should key CSC: 696<br>Postcode numbers: 12<br>Address number: 22 | You should key CSC: 696<br>Postcode numbers: 12<br>Address numbers: 422 |

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

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

## What do the CSC/AVS responses mean?

After you have keyed in the CSC and AVS data, if 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 cannot be matched and where you should consider additional checks to reduce the risk of fraud. Please refer to Reducing fraud.

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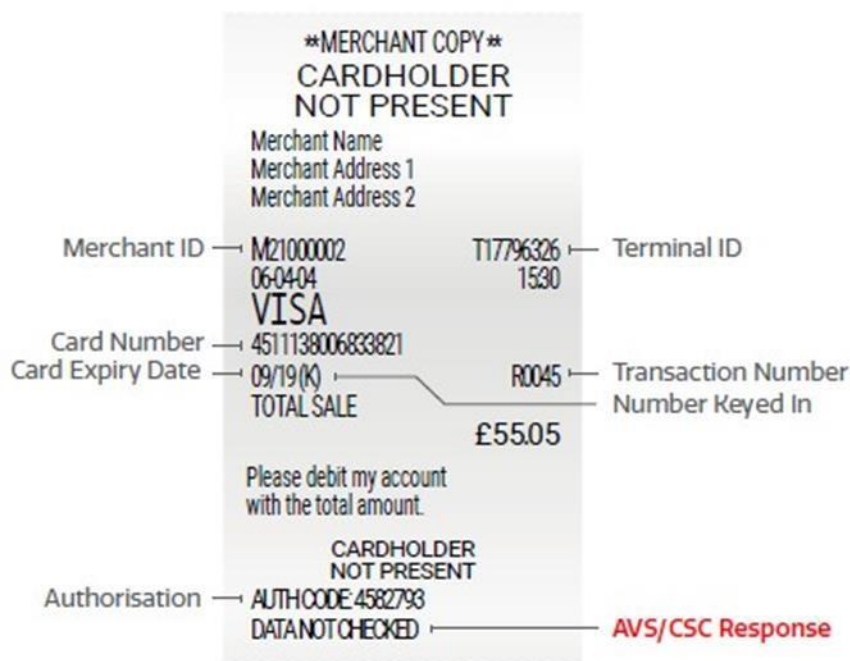
It's important to understand that these checks are an additional security measure. They can help you make an informed decision, but they are not a guarantee of payment.

The below tables shows CSC/AVS responses. However, 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 | `12 | |
|---|---|---|
| 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, if you are confident you can securely deliver goods/services to the address that has been verified. Delivery to a different address increases the risk associated with any CNP sale. Find out more in Reducing fraud. |

**worldpay**

| 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 | The transaction may be fraudulent or the cardholder has recently moved and not updated their details with their card issuer. The details may also have been taken down incorrectly or the cardholder address is abroad and we have been unable to verify with the card issuer.<br>Before going ahead, you should check the address details with your customer and be satisfied 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 | The transaction may be 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 be satisfied that they are the rightful cardholder.<br>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 numbers do not match | The transaction may be fraudulent. We recommend you do not proceed without further checks to be satisfied that the person offering the card is the rightful cardholder. For example, you should ask for additional ID, e.g. passport, driver's licence or utility bills. |
| Data not Checked | The card issuer has not been able to check the data | The card issuer may not support either of these security checks or their system is down. If this happens you need to decide based on the information you have, to be satisfied that the person offering the card is the rightful cardholder, before processing the transaction. |

### 4.3.7 Making an informed decision

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

These additional checks through your terminal also cannot confirm cardholder names. 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

49

Most cards are processed as chip and PIN or contactless and do not need you to see the card. 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 payment.

We recommend that all your staff know the process of 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 if 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 these security features. If you are suspicious for any reason, here are key details to check.

*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

## 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.

> *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 when 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*



51

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**

It 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 and 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**

We have added a list of card scheme logos that you can download here. Please see *Manually Adding the Card and Payment Method logos* under *How to add card logos to your 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
- Visa – a flying dove
- Maestro (UK-issued) – William Shakespeare
- Visa Electron – 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 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.

*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 useful to help reconcile your accounts.

**Useful support articles**

- How do I Use Worldpay Dashboard for Reconciliation?

- What is the difference between monthly and daily billing?

## 4.5.1   Accessing your invoice

We can provide your invoice by post or online, depending on your preference. Merchants registered with Worldpay Dashboard can access their invoice online. The invoice can be downloaded in PDF format, and you can print it out if needed. In addition, Worldpay Dashboard offers access to transaction and settlement data including card sale trends and analytics. Merchants not registered with Worldpay Dashboard will receive 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 invoices, use the Manage Account pages on Worldpay Dashboard to turn on this feature.

### 4.5.2 Settling your invoice

**Daily billing**

If your account is billed daily, you will receive your funds from transactions daily, and any transaction charges, chargebacks, and refunds will also be deducted daily from your transaction funds.

Daily billed merchants can access a Daily Invoice **and** a monthly summary in their Monthly Statement.

- **Daily Invoices** are generated each day you've transacted and made available two days later. They show a summary of transactions and charges for that day. If no transactions are processed, a daily invoice won't be generated
- **Monthly Statements** are generated monthly with a summary of all daily invoices and any applicable charges for the month

**Monthly billing**

If your account is billed monthly, you will receive funds in full from your transactions daily. The transaction charges from Worldpay will then be calculated and invoiced monthly.

Your monthly invoice will include the transaction charges and any other miscellaneous account charges from the previous month (e.g., you'll receive an invoice in March showing charges for February).

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 to 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.

You can find more details on the differences between monthly and daily billing [here](here).

### 4.5.3 Premium Transaction Charges

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

## 4.6     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 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.

> *Never store your cardholder's Card Security Code (CSC). The CSC may be used*
> *for the first transaction, it 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: 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 use 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 – offer your customers the option to transact in your local currency, or one of the other 24 currencies supported by Worldpay, directly through your new terminal(s) at the point of sale
- 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 via telephone 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 an agreement(s) with us to process MOTO transactions and eCommerce (if you accept bookings online).

### Hotel Services - Cards you can accept for guaranteed reservations

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

You cannot accept:

- Maestro
- Visa Electron

### Hotel Services - Details you need from the cardholder when making a guaranteed reservation

- 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

### The Data Protection Act 2018

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.

### Hotel services - Information you must 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.

### Hotel services - When 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

### Hotel services - 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

*Hotel services - If the accommodation has been overbooked*

If a guest has made a guaranteed reservation and 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.

*Hotel services - 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

*Hotel services - 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 important to follow the correct procedure carefully to reduce the risk of chargebacks.

***Hotel services - Cards you can accept for express checkout***

- Mastercard

- Debit Mastercard

- Visa

- Visa Debit

- JCB

- Diners/Discover

You cannot accept:

- Maestro

- Visa Electron cards

***Hotel services - Using 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

***Hotel services - 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. For information on processing pre-authorised transactions visit the Product Help Centre.

- 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

### Hotel services - 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 via Product Help Centre
- If the top-up authorisation is declined, you will need to contact your customer and ask them for another method of payment

### Hotel services - Delayed or amended charges

You may need to process extra charges or change the amount agreed due to other costs incurred. These are referred to as delayed or amended charges.

For hotel stays, room charges including food and beverages may be subject to delayed or amended 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.

Card schemes do not allow merchants to process a delayed/amended charge for any damage incurred during a cardholder's stay.

### Hotel services - 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.

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 added security of pre-authorising payments before the customer takes the vehicle away.

### Vehicle Rental Services- 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.

### Vehicle Rental Services- Information you must 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, there are two things you need to do before they take the vehicle away with them.

1. 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

2. 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

> *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 by visiting the [Product Help Centre](#).
  - 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 by visiting the [Product Help Centre](#)

Maestro cards do not support pre-authorisation requests.

***Vehicle Rental Services- 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 via [Product Help Centre](#)

- Do not include charges for damages or insurance deductibles in the payment. These charges need to be processed separately as delayed or amended charges

**Vehicle Rental Services - If the customer cancels/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

**Vehicle Rental Services - 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 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

***Vehicle Rental Services - 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

***Vehicle Rental Services - Disputes (including chargebacks)***

**Visa cards transactions**

If a Visa card transaction dispute arises, you must provide us with specific documents within the indicated timeframe to avoid a chargeback debit to your bank account. Required documents include:

- **Notification letter**: A dated copy sent to the cardholder about delayed or amended charges
- **Rental agreement**: A copy of the original agreement
- **Repair estimate**: Cost estimate from a legal repair provider in local currency
- **Fines documentation**: Proof of billing for parking or driving fines, excluding processing or excessive unpaid fine charges
- **Accident report**: Relevant civil authority report (if applicable)
- **Cardholder agreement**: Signed documentation showing cardholder liability, with signature on the same page as terms and conditions
- **Vehicle registration**: All documents must match the correct vehicle registration number
- **Insurance policy**: A copy of the rental company's insurance policy and rental agreement showing cardholder's consent for insurance deductible responsibility
- **Additional liability documentation**: Any other proof of cardholder liability for damages

Failure to provide these documents will result in a chargeback debit.

**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**

If 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.

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, we will not be able to defend a dispute on your behalf and a chargeback debit will be processed to your bank account

### 4.6.3 Bureau de Change

If you operate as a bureau de change, you can offer your customers 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 an 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

69

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.

## 4.6.4 Tax free shopping

Tax  free  shopping  enables  travelers  outside of Europe  to receive  a VAT refund  on goods  over  £30 which  they buy in the UK and  take home. International   shoppers  are  increasingly  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 may be disputed by the cardholder or card issuing bank, if goods are not received, or a transaction was not recognised or authorised.

Worldpay 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  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  the right  process  has  not  been  followed,  for  example,  if you have  taken  payment  above your  floor  limit without  obtaining  valid  authorisation.  Or when  you take an eCommerce  transaction  without cardholder  authentication  (e.g.  Visa Secure  or Mastercard  Identity  Check),  and  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.

**Chargebacks Dispute Process**

The chargeback dispute process is outlined in the below diagram. As your acquirer we'll always act on your behalf during this process, but if you don't respond to our request for information in time or card scheme rules were breached, the transaction may be debited from your account

1. Cardholder initiates a dispute for a transaction with their card issuing bank (e.g NatWest, Barclays etc).

2. The card issuing bank (Issuer) sends the funds back to Worldpay (Acquirer) to investigate further.

3. Worldpay receives the chargeback, then resolves where possible with the Issuer directly or forwards on to the Merchant (Worldpay customer) for further supporting evidence.

4. Merchant receives chargeback and accepts debit or provides supporting evidence to Worldpay to defend the chargeback.

Cardholder     Issuer     Acquirer     Merchant

7. Cardholder receives the dispute resolution information and may be credited or rebilled for the item in question

6. Issuer independently reviews the supporting evidence and a chargeback outcome is reached. Merchant advised of outcome by written communication.

5. Worldpay receives the supporting information from the Merchant and if provided within the time frames will represent to the Issuer.

## 4.7.1   Why chargebacks happen

Here are some common reasons for chargebacks. 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 their knowledge or states that they do 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 or 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 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 – 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. 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 and have the customer agree to any resolution agreed. Proving the content of a telephone conversation is extremely difficult as card schemes do not accept recordings of telephone conversations as evidence.

The cardholder does not always have to physically return the goods to you for a chargeback to be correctly raised.

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 contact you directly?

You and your customer may come to an agreement to issue a refund, but this will usually be before 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, as a response to the card issuer is still required.

- If the customer 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, 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 important to respond by the date given or timescales specified.

- We set response times 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 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.

Following all correct procedures does not guarantee that you will succeed in disputing a chargeback. The technology we use is designed to ensure that chargeback enquiries are resolved efficiently with minimum disruption to your business.

## 4.8    Merchant location

A Worldpay merchant 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...................................................................................78

# 5 Authorisations and referrals

## 5.1 Making a referral call

If you have an electronic terminal, the authorisation check is typically automatic. Your terminal may 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.

*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 the 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 you have accurately entered the code 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 via the Product Help Centre about keying the code.

### 5.1.3 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

- 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. Check any new card carefully. Find out about Reducing fraud

### 5.1.4    Transaction changes after authorisation and before processing

Sometimes you need to amend 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 only applies if the transaction had been processed. Find out more in Refunds

### 5.1.5    Split transactions

You must not split the sale into two (or more) separate amounts on one card 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.

### 5.1.6    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 allows pre-authorisations for all transactions. Pre-authorisations expire 31 days following the date they were submitted.

For Visa cards, authorisations differ per sector. An approval response to an estimated or initial authorisation and any subsequent incremental authorisations will expire:

- 31 days after the initial estimated authorisation for cruise lines, hotel/lodging and car/vehicle rental merchants
- Seven days after the initial estimated authorisation for other rental merchants, trailer parks and campgrounds

For Card Not Present otherwise not specified, the approval response will be valid for seven days from the 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**

**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, 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' above

**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**) – 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 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 (CSC)' above.

**Card Verification Value (CVV or CVV2)** – refer to 'Card Security Code (CSC)' above.

**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 process whereby a card issuer can dispute part or all of the value of a transaction on behalf of the cardholder via your acquirer, e.g. 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** – 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 Due Diligence (CDD)** – a regulatory practice that requires the periodic re-verification of customer account information, to support best practice and protect against financial service industry fraud practices.

**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 online. 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 online access must have a firewall to prevent outsiders from accessing internal private data resources.

**Floor limit** – an amount agreed between Worldpay and our merchant 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, 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 online. Formerly known as Mastercard SecureCode.

**Merchant ID (MID)** – see 'Customer Number' above.

**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 (online) 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. 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)** – full magnetic stripe data, CAV2/CVC2/CVV 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 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.

**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 online-facing IP addresses that check for unknown

vulnerabilities  in your network.

**W**

**Worldpay Dashboard –** an online platform where you can manage your Worldpay account and examine your business information from card sales, settlements, invoices and much more

**Worldpay Product Help Centre** – an online platform where merchants can access articles and videos with in-depth how-to guides and FAQs. This content can also be found in the help search in Worldpay Dashboard, so you can find relevant support quickly based on the page or section you are viewing.

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

**3**

**3D Secure** – see <u>Cardholder  authentication</u>.

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    Key contact details

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 merchants:  0345 760 0500*
ROI merchants: 1800 700 100
International merchants: [International.helpdesk@fisglobal.com](mailto:International.helpdesk@fisglobal.com)

**Authorisations – Card Not Present transactions**

UK merchants: 0345 760 0530*
ROI merchants: 1 800 700 300
International merchants: [International.helpdesk@fisglobal.com](mailto:International.helpdesk@fisglobal.com)

**Name and Address checks**

UK merchants: 0845 300 7929
ROI merchants: 1 800 700 300

## 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 merchants:  0345 761 6263* (Text phone users may call 18001 0845 3003889*)
ROI merchants: 1800 242 636
International merchants: [International.helpdesk@fisglobal.com](mailto:International.helpdesk@fisglobal.com)

*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 Worldpay's approved supplier below.

UK merchants:   0800 289 666 (Freephone)
ROI merchants: 0  0800  9899  2000

**eCommerce helpdesk - Existing eCommerce merchants**

UK merchants:   0330  333  1233
ROI merchants: 1870  366  1233

**Sales**

UK merchants:   0115 828 4034
ROI merchants: 1800 800 117

**Other ways to contact us**

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

Contact Worldpay in writing to:
Worldpay

Gateshead Card Centre Victory

House

5th Avenue

Gateshead

NE11 0EL

United Kingdom

# 8    About this guide

## 8.1    Document control

| Version | Change  description | Date |
|---------|---------------------|------|
| **1.0** | First  version | October  2019 |
| **1.1** | Update to Section 4.2.8 – 'Information to be given before an order is placed'. | June 2023 |
| **1.2** | Brand review<br>Update to Section 4.1.1 – 'Point of Sale requirements and display material'.<br>Update to Section 3.2.2 – 'Transaction Monitoring'<br>Update to Section 4.1.2 – 'Call costs'<br>Update to Section 4.6.2 – 'Our other services'<br>Update to Section 6 – 'All the jargon explained alphabetically'<br>Update to Section 7 – 'All the Contact details you need' | July 2024 |
| **1.3** | Brand  review | September 2024 |
| **1.4** | Quarterly brand and content review | January 2025 |
| **1.5** | Interim update to align with MOI Key facts document | February 2025 |
| **1.6** | Quarterly brand and content review | June 2025 |
| **1.7** | Quarterly brand and content review | September 2025 |
| **1.8** | Quarterly brand and content review. Date update. | December 2025 |

## 8.2  Legal

©2026 Worldpay and/or its subsidiaries. All Rights Reserved.