## Contents

1. **Introduction**
   - Basic Rules 4
   - Recordkeeping 5
   - Banking Procedures 5

2. **Before You Accept Card Payments**
   - How to Verify the Card 6
   - Commercial Cards 7
   - How to Guard Against Fraud 7

3. **Accepting Card Present (CP) Transactions**
   - Chip and PIN Enabled Cards 10
   - Contactless Transactions 10
   - Chip and Signature Cards 10

4. **Accepting Card Not Present (CNP) Transactions**
   - Card Security Code (CSC) 11
   - Address Verification Service (AVS) 12
   - Authorisation Responses 12
   - eCommerce Transactions 14
   - Pre-Authorisation 19
   - Referrals 19

5. **Purchases With Cashback** 20

6. **Refunds** 21

7. **Paper Vouchers**
   - Completing a Sales/Refund Voucher 22
   - Preparing/Submitting Vouchers for Submission 23

8. **Exceptional Procedures**
   - Can I Pass Charges to My Customer? 24
   - Split Sales and Transactions 24
   - Terminal Fallback 25
9. Chargebacks
   Common Causes of Chargebacks
   Retrieval Requests
   Chargeback Reversal Procedure

10. Other Services
    Vehicle Rental Services
    Hotels, Lodging, and Accommodations
    Dynamic Currency Conversion (DCC)
    Multicurrency and Cross-Border Transaction Acceptance
    Payment of Debt

11. Payment Card Industry Data Security Standard (PCI DSS)
    Becoming PCI Compliant
    Implications of Not Complying With PCI DSS
    Third-Party Obligations
    Secure Data Storage
    Demonstrating Compliance With PCI DSS

12. Keeping Your Point-of-Sale (POS) Device Safe
    Positioning Your POS Device

13. Qualifying/Non-Qualifying Transactions
    Card Present
    Card Not Present MOTO
    Card Not Present eCommerce

14. Voicing Your Concerns
    Complaints Team

15. Useful Contact Information

16. Changes to Your Business
Thank you for choosing First Data. This guide forms a part of your Merchant Agreement and contains the procedures that need to be followed regarding card acceptance. Please remember that all businesses that accept payment by credit and debit cards must follow the procedures set out by the card schemes, First Data as your acquirer, and the Payment Card Industry Data Security Standard (PCI DSS). These standards exist to protect you and your customers. It is important to follow some basic procedures that are strictly enforced by the card schemes.

**Basic Rules**

**You Must:**

- Clearly display card acceptance logos for your customers to see e.g., Visa®, Mastercard®, and Diners Club®
- Only accept the card types that you are entitled to take as specified in your Merchant Agreement
- Ensure surcharges added to card payments are displayed for the cardholder and are part of the transaction amount (i.e., cannot be charged separately)
- Include any taxes in the amount charged on card transactions
- Provide a sales receipt for the cardholder to confirm the amount debited from their payment card
- Validate your compliance with the PCI DSS (see Section 12)
- Never process any transactions for goods and services that do not directly relate to your business as specified in your Merchant Agreement
- Notify us of any changes to your business (see Section 17)
- Retain a copy of all sales and refund receipts for 18 months

**You Must Not:**

- Indicate that any card scheme endorses your goods and services
- Submit a card transaction that has been previously subject to a chargeback
- Accept card transactions on behalf of third parties
- Manually key a payment card transaction into a point-of-sale terminal when the card details have been provided via an internet shopping cart
- Process card transaction without the cardholder’s permission, if they are not present at that time
- Process eCommerce transactions, unless as specified in your Merchant Agreement
- Leave your terminal unattended (e.g., where fraudsters could have easy access)
- Store sensitive card data
Recordkeeping

› A card transaction is only completed on the final delivery of goods or services
› Sale and refund receipts should be stored in a secure area in accordance with the PCI DSS (see Section 12)
› Store only the portion of the customer’s account information that is essential (i.e., name, account number, and expiry date)
› You must not store the following under any circumstances:
  • Full contents of any data from the magnetic stripe or chip
  • Card Security Code (CSC) – the three-digit number displayed on the signature panel of the card
  • If requested by us, please supply all sales and refund receipts within 14 business days

Banking Procedures

Please follow the end-of-day banking procedures detailed in your Terminal User Guide to ensure you receive payment for all transactions. It is essential that all transactions be submitted for payment within two working days of being accepted.

Please note that if a transaction is submitted after two working days, the card issuer may reject the transaction, resulting in it being charged back.
Your Merchant Agreement with First Data states the card types you are allowed to accept. It is important that you and your staff understand how to recognise different card types to reduce fraud risk.

As the majority of the cards are processed as PIN verified or contactless, you will not be able to see the card. If signature verification is required, then you will need to ensure that the signature on the back of the card matches the signature provided by the cardholder.

Newly issued cards will have a card type printed on the front of the card. These will be Debit, Credit, Commercial, or Prepaid.

**Features Include:**

- **Magnetic Stripe**: The magnetic stripe will appear on the back of the card.
- **Card Security Code**: A three-digit Card Security Code will be displayed on the back of the card, either in the white area next to the signature panel or directly on the signature panel.
- **Cardholder Photograph and Signature**: A photograph of the cardholder may appear either on the front or the back of the card.

**How to Verify the Card**

- **Chip**: This works together with cardholder’s PIN or signature to create more secure payment, look for any visible damage.
- **Card Number**: This is usually (but not limited to) 16 digit number on the front or back of the card. It should be clear to read and in line.
- **Cardholder Title and Name**: These should be clear to read and in line. Check that the title printed/embossed on the card matches the gender of the customer presenting the card.
- **Signature Panel**: A card should be signed by the cardholder once received. If a transaction is taken in a way that requires signature verification, ensure that the signature on the back of the card matches the one provided by the customer. Check stripe for any visible damages or evidence of writing over a previous signature, etc.
- **Expiry Date/Valid-From Date**: Only some cards have a valid-from date, but all should have an expiry date. Ensure that the card is not presented to you after the expiry date and/or before the valid-from date.
- **Hologram**: The 3D image should move when the card is tilted. It can be located on the front or back of the card. Please note that some Visa Electron® cards do not have a hologram. On Visa cards, look for the flying dove; on Mastercard cards, look for the globe; and on Maestro® look for William Shakespeare’s head.
- **Card Security Code**: This code is typically located on the back of the card - on the signature panel or in the white box next to it.
Ultraviolet (UV) Features – Images under the UV light will show: on Visa, a flying dove; on Mastercard, the letters "M" and "C"; and on Diners Club International/Diners®, a circle with a vertical line in the middle. As with the hologram, some Visa Electron and Mastercard cards issued after October 2015 do not carry the UV image.

Card Scheme Logo – This should be clear and match the examples shown below:

![Card Scheme Logos]

Commercial Cards

Commercial cards bring specific benefits to business-to-business sales transactions. They look like any other Visa or Mastercard, although many have the description of the card’s function on the front of the card (e.g., Business Card, Corporate Card, and Purchasing Card).

How to Guard Against Fraud

There is a risk that exists with taking all types of transactions. This section outlines what we believe to be industry best practice that will help you to identify and reduce that risk. Remember that the best fraud prevention is well-trained staff. Please ensure that all staff accepting card payments on your behalf have read and understood the following procedures or any fraud prevention documents we may send you in the future. This will help reduce financial losses to your business and risk of chargebacks.

**IMPORTANT – Please note that an authorisation is not a guarantee of payment. It only confirms that there are enough funds to pay for the goods and that the card has not been blocked at the time of the transaction.**

Face-to-Face Transactions (Card Present)

Preventing and Detecting Fraudulent Face-to-Face Transactions

› Chip and PIN are the most secure types of transactions. As the cardholder will retain the control of the card when processing the transaction, you are not required to make visual checks of the card. You must, however, follow the instructions shown on the terminal.

› Despite the fact that nearly all cards in the U.K. are chip enabled, sometimes you will require the cardholder’s signature as a verification method. Please ensure that the person presenting the card is the genuine cardholder, and follow the prompts on your terminal.

Checking the Card

› Never key a card number into your terminal if both the card and cardholder are present. This may result in a chargeback to you.

› Verify if the name on the card matches the signature. Remember to check the condition of the signature panel; if it looks damaged, it may be because the original signature has been covered over.

› If possible, check the spelling on the card and on the sales voucher
Compare the last four digits of the card number to that printed on the sales receipt. This check will allow you to identify a cloned card.

Check for the special mark on the card using a UV lamp. If you place the card under the lamp, you should see a hologram.

**Checking the Cardholder**

Look carefully for the following signals:

- The title on the card does not match the customer
- The customer seems nervous or hurried
- The customer insists upon taking the goods immediately (e.g., they are not interested in free delivery)
- The customer takes an unusual amount of time to sign and refers to the signature on the back of the card
- The customer repeatedly returns to make additional orders in a short period of time
- If a transaction is declined, the customer then requests a lower-value authorisation attempt

**Checking the Transaction**

- The customer makes an order substantially greater than you would normally expect

**Returning Wanted or Recovered Cards**

- Keep the card safely at your premises until the end of business on the day when the card was found
- If the cardholder returns to claim the card, obtain the claimant’s signature and compare this signature with that on the card
- Only release the card if you are satisfied that the claimant is the cardholder
- Unclaimed cards should be sent to: P.O. Box 280, Lowton Way, Hellaby, Sheffield, S98 1RU

**Card Not Present (CNP) Transactions – Mail Order Telephone Order (MOTO)**

CNP transactions are considered high risk, as you cannot check the card or the customer. Fraudulent CNP transactions are your liability, as they are likely to be charged back to you. Written agreement from First Data is needed to take this transaction type.

**Preventing and Detecting Fraudulent MOTO Transactions**

- Goods relating to a CNP transaction should not be collected by the cardholder. If the cardholder wishes to collect the goods, they must present the card for payment at the time of collection.
- Never dispatch the goods to anybody other than the cardholder, and be wary if the delivery/customer is overseas
- Be aware of "social engineering". Fraudsters may spend time building up credibility and then place a large order or make a request for goods or services outside of your usual trade, such as money transfers.
- To prevent MOTO fraud, look for:
  - A high-value order that can be easy to resell
  - First-time customers placing multiple orders
  - Multiple purchases of the same goods completed on the same card
  - Customers who are hesitant or make errors providing their personal information
  - Customers who are more interested in speedy delivery than the good’s price
Preventing and Detecting Fraudulent eCommerce Transactions

Signs to Look Out for Include:

› Multiple transaction attempts using the same, or similar, customer details or card numbers
› High-value purchases that are unusual for your business
› Mismatching of the Card Security Code (CSC) or Address Verification Service (AVS) check
› Mismatching combination of IP address, card issue country, and the billing currency
› An email address that bears no relation to the shopper’s name or makes no sense (e.g., “jfyfjlsur@gdyflg.com”)
› A request to bring forward the delivery date after the order has been placed
› A request to alter payments details
› Multiple deliveries to the same address
› A delivery country that is unusual for the purchase
› General inconsistency

Delivery Warning Signals

Here are some danger signs to look out for when arranging delivery of goods:

› Never dispatch the goods to anybody other than the cardholder, and be wary if the delivery/customer is overseas
› Insist that goods may only be delivered to the cardholder’s permanent address. If you agree to send goods to a different address, take extra care and always keep a written record of the delivery address with your copy of the card transaction details.
› Only send goods by registered post or a reputable courier, and insist on a signed and dated delivery note

Instructions for Your Courier

› Make sure the goods are delivered to the specified address and are not given to someone who "just happens to be waiting outside". Instruct your courier to return with the goods if they are unable to complete delivery to the agreed upon person/address.
› Do not deliver to an address that is obviously unoccupied
› Obtain a signed proof of delivery, preferably the cardholder’s signature
› If you have your own delivery service, consider training your driver to check the card. If you wish to do this, please contact the Fraud Department by phoning the Merchant Support Centre on 0345 606 5055 for more details.
Chip and PIN Enabled Cards

- Ask the cardholder to insert the card into the chip reader and enter the PIN, as prompted.
- Once the transaction is completed, the cardholder will be prompted to remove the card.
- Cardholders have three attempts to enter their PIN correctly before it is locked.
- If this happens, inform the cardholder and ask for an alternative method of payment.

Contactless Transactions

If the cardholder’s card or device (e.g., mobile) has been enabled for contactless, the process is as follows:

- Initiate the transaction as you would normally do using your terminal.
- Ask the cardholder to hold their contactless payment device within two centimetres of the contactless reader.
- Follow the terminal prompt to check that the transaction has been completed.
- As a further security measure, occasionally the cardholder will be prompted to insert the card and enter their PIN.

You cannot offer cashback on a contactless transaction.

Chip and Signature Cards

- Ask the cardholder to insert the card into the chip reader and follow the prompts on the terminal.
- Ask the cardholder to sign the receipt and check that it matches the one on the card being used.
A CNP transaction is when a card is not presented at the point-of-sale for eCommerce recurring transactions, such as mail/telephone orders, all of which must be authorised.

- Take extra care to ensure it is the genuine cardholder placing the order
- To defend any disputes, keep a record of any permission to debit the card, such as a recurring payment agreement or a call recording

To process a CNP transaction, you must obtain the following information:

- Card number
- Expiry date
- Card Security Code (except for mail order transactions)
- Cardholder’s full name and address
- Transaction amount
- Delivery address if different from the cardholder’s address

There are increased risks of chargebacks for CNP transactions as the cardholder and card are not present. If you choose to deliver goods to an address other than the cardholder’s address, you are taking additional risk.

Card Security Code (CSC)

The CSC is a three or four-digit code that appears on a debit or credit card. It is used as a fraud prevention tool in CNP transactions:

- The CSC is not retained in your terminal, if supplied through us
- If a customer provides written card details, you must ensure the details are securely deleted
- Card numbers and the CSC are valuable data; you must never record or accept copies of these
- CSC is not required for the following:
  - Reservations
  - Corporate and purchasing cards
  - No-show transactions
  - Cancellation refunds
  - Charges after checkout
  - Mail order transactions
CSC cannot be stored; it can be used for one transaction only. Once the transaction has been authorised, you must not keep a record of the CSC.

Address Verification Service (AVS)

AVS is available on cards issued in the U.K. and allows you to check the cardholder’s statement address with the card issuer to help reduce fraud. You need to ask the cardholder for the following information:

› Only the numbers in the postcode of the cardholder’s statement address
› Up to the first five numbers of the cardholder’s statement address

Your terminal will prompt you to enter the numbers in the three stages below:

<table>
<thead>
<tr>
<th>Cardholder’s Address</th>
<th>Card Security Code</th>
<th>Postcode Numeric</th>
<th>Address Numeric*</th>
</tr>
</thead>
<tbody>
<tr>
<td>55 South Street, Any Town, Any County SS17 1BL</td>
<td>000 or 1234</td>
<td>171</td>
<td>55</td>
</tr>
<tr>
<td>Flat 3, 21 North Street, Any Town, Any County LM5 7LT</td>
<td>000 or 1234</td>
<td>57</td>
<td>321</td>
</tr>
<tr>
<td>The Cottage East Lane, Any Town, Any County SS12 3BL</td>
<td>000 or 1234</td>
<td>123</td>
<td>Bypass*</td>
</tr>
<tr>
<td>Apt 62, 2190 West Road, Any Town, Any County LM45 1LT</td>
<td>000 or 1234</td>
<td>451</td>
<td>62219</td>
</tr>
</tbody>
</table>

*When a customer address includes only a house name, you may bypass this prompt by pressing the ENTER key.

Authorisation Responses

If there are available funds and the card has not been reported lost or stolen, one of the standard responses shown below will be received. Please remember:

› The final decision to accept the payment or not is yours
› You are responsible should a transaction be confirmed as invalid or fraudulent even if the data matches and an Authorisation Code is issued
› AVS/CSC does not protect you from a chargeback. AVS and CSC responses do not consider whether there are sufficient funds or even if the card is lost or stolen. You can still get a positive AVS/CSC match on a declined transaction.
<table>
<thead>
<tr>
<th>Response</th>
<th>Definition</th>
<th>Action to Take</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Matches/Data Matched</td>
<td>Both the AVS and CSC match the card issuer’s records.</td>
<td>As long as you have been issued an Authorisation Code and are satisfied that the transaction is genuine, then unless there are other suspicious circumstances, you are likely to want to go ahead with this transaction. As with all CNP transactions, payment is not guaranteed, and you bear the risk if the transaction is disputed.</td>
</tr>
<tr>
<td>Data Non-Match/Data Not Matched</td>
<td>Both the address and postcode details do not match the card issuer’s records.</td>
<td>This indicates this could be either a fraudulent transaction or the details have been entered incorrectly. We recommend that you not proceed unless further checks are made to verify the cardholder and the delivery address provided.</td>
</tr>
<tr>
<td>CSC Match Only</td>
<td>Either house number or postcode does not match the card issuer record.</td>
<td></td>
</tr>
<tr>
<td>AVS Match Only</td>
<td>Both address and postcode match but not the CSC.</td>
<td></td>
</tr>
<tr>
<td>Not Checked</td>
<td>The CSC and AVS have not been checked.</td>
<td>You will have to make a decision based on the information you have. We recommend further checks be made before going ahead with the transaction.</td>
</tr>
</tbody>
</table>

For more information about AVS and CSC, please contact our Merchant Support Centre on 0345 606 5055†.

An authorisation with or without confirmation of AVS/CSC information does not guarantee payment. If fraud subsequently occurs, you will be liable for the chargeback.

**Rules for CNP Transactions**

When the cardholder places the order, you must obtain an authorisation, and when the goods or services are ready to be delivered, the transaction should be processed. The authorisation is valid as follows:

- **Visa** – The transaction amount must be within 15% of the authorised amount, and the goods must be shipped within 31 days. Otherwise, a second authorisation is required

- **Mastercard and Diners Club** – The transaction amount must equal the authorised amount, and the goods must be shipped within 30 days. Otherwise, a second authorisation is required
**eCommerce Transactions**

You must make an application to take eCommerce transactions with First Data, even if you have an existing Merchant Agreement.

On approval, a new First Data merchant number will be issued. This is solely for the purpose of acceptance of eCommerce transactions for the business described within the new application form.

All eCommerce transactions are regarded as "Card Not Present Transactions" and are taken at your own risk. In the case of a dispute, we retain the right under the Merchant Agreement to charge back any eCommerce transactions irrespective of whether or not an Authorisation Code is obtained.

**Website Requirements**

The details below should not be considered as a comprehensive list of the information that you may be required to provide on your website under applicable legal requirements, and they should not be seen as a form of legal advice. You should obtain your own legal advice on the content and activities carried out on your website.

You should ensure that your website, its contents, and any activities related to it, such as marketing, are in accordance with all local legal requirements and regulations.

You must also comply with the requirements of all data protection legislation. Where you process personal data on your website, include a Privacy Policy that cardholders are required to agree before providing any personal data on your website.

You need to ensure that your website provides some basic information about your business so that the online shopper can easily identify you. It also needs to display contact details (landline telephone number and correspondence or email address) so that any customers who wish to contact you to resolve a dispute can do so. You should also clearly state the physical location of your business and a statement detailing under which legal jurisdiction your business operates before the transaction is completed. Any trade association membership, professional bodies that you are registered with, as well as VAT registration number (if applicable) should also be provided.

The order page on your website, whether provided by a third-party or created by you, must be PCI (Payment Card Industry) compliant and collect at least the following details:

- Cardholder’s full name
- Cardholder’s email address
- Cardholder’s billing address and postcode
- Delivery address

**Payment Page (Checkout)**

Providing cardholders with sufficient information about their purchases is very important so that they have a good idea of what is on offer. You should ensure that you provide a description of the following:

- The products and the services as well as total cost (showing any additional cost such as applicable tax, packaging, delivery charges, etc.)
- Your Terms and Conditions, including your return and cancellation policy
- Instructions on how to complete their order
The payment page on your website, whether provided by a third-party or created by you, must be PCI DSS compliant and collect at least the following:

- Transaction amount
- Card type e.g., the card types detailed in your Merchant Agreement
- Customer’s card number
- Card expiry date
- CSC

**Payments and Refunds**

- Cardholders should be provided with clear information on all payment options and clear instructions on how to pay
- Cardholders should be informed of their cancellation, refund, replacement, and complaint rights at the time of purchase
- Receipts should be provided with the goods on delivery

**Receipt Requirements**

You must provide a cardholder receipt by email and/or post that contains the following:

- Partial cardholder account number – for eCommerce transactions, please note that the cardholder account number, Card Security Code (CSC), and expiry date must not appear on the transaction receipt (this is a PCI DSS requirement)
- Unique transaction identifier – to assist in disputes, you should assign a unique identification number to the transaction and display it clearly on the transaction receipt:
  - Cardholder name
  - Transaction date
  - Transaction amount
  - Transaction currency
  - Authorisation Code
  - Description of merchandise or services
  - Merchant name
  - Website address

Best practice is to provide your customers with an acknowledgement of their purchase, prompting them to either print or save this document for their own records.

**Verified by Visa and Mastercard SecureCode**

These are industry-wide initiatives introduced to combat internet fraud, commonly known as cardholder authentication. Cardholders who register for this service with their card issuer will be required to use a personal PIN or password at the time of the transaction to confirm they are the genuine cardholder. Verified by Visa and Mastercard, SecureCode operates on your website and interacts with both the customer and their card issuer. The whole process takes a few seconds, and the online shopper is unlikely to be inconvenienced by it.
Payment Services Provider (PSP)

You must be set up with the First Data eCommerce gateway (or a third-party PSP) if you want to accept eCommerce transactions. Please note, third-party PSPs must be PCI DSS compliant and accredited with First Data to submit eCommerce transactions to us. Your chosen PSP will be able to advise you of relevant costs, setup times, and how their systems integrate with your website.

Security

You must ensure that card details are captured and stored securely in accordance with PCI DSS requirements. Card details should be encrypted and protected by a firewall. Never send full card details via email as this is not a secure method for data transfer.

Delivery and Guarantees

› Delivery dates/times should be clearly stated and agreed upon with the cardholder. If it is not possible to deliver on the agreed upon date/time, another delivery should be arranged. If this is not possible, the cardholder should be offered a refund.
› You should capture both the billing address details and delivery address details
› In the event of a non-delivery, it is the merchant’s responsibility to prove receipt of the goods by the cardholder
› Apart from deposits, full payment for goods and services must not be debited from a cardholder’s account until goods have been dispatched or the service provided. Should you wish to be able to take deposits on goods and services, you must get agreement from First Data for this before any deposits are taken.

Recurring and Instalment Transactions

› **Recurring Transaction** – A payment for goods or services that are received over time, e.g., insurance or subscription
› **Instalment Transactions** – A regular payment against a single purchase, e.g., car or loan. Written agreement from First Data is needed to take these transaction types.

<table>
<thead>
<tr>
<th>Recurring Transaction</th>
<th>Instalment Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>The cardholder must consent to periodic charges for recurring merchandise or services at the time of the first transaction. This permission must include at least all of the following in writing and must be provided to the cardholder:</td>
<td>You must provide, and the cardholder must consent to, the merchandise or services and all of the following in writing, at the time of the first transaction:</td>
</tr>
<tr>
<td>› Transaction amount</td>
<td>› Terms of service</td>
</tr>
<tr>
<td>› Fixed dates on or intervals at which the recurring transactions will be processed</td>
<td>› Timing of delivery to cardholder</td>
</tr>
<tr>
<td>› Duration for which cardholder permission is granted</td>
<td>› Transaction amount</td>
</tr>
<tr>
<td>› Cancellation and refund policies</td>
<td>› Total purchase price</td>
</tr>
<tr>
<td>You must retain the cardholder’s permission for the duration of the recurring merchandise or services.</td>
<td>› Terms of future payments, including the dates and amounts</td>
</tr>
<tr>
<td></td>
<td>› Cancellation and refund policies</td>
</tr>
</tbody>
</table>
A recurring transaction amount must not include:

- Partial payment for merchandise
- Services purchased in a single transaction
- Finance charges

An instalment transaction amount must be less than the total price of the merchandise or services purchased and may include interest charges.

Authorisation is required for each individual recurring transaction.

Authorisation is required for each individual instalment transaction. If a request for a subsequent payment is declined, you must notify the cardholder in writing and allow the cardholder at least seven days to pay by other means.

A merchant must not process an initial instalment transaction until the merchandise or services have been provided to the cardholder.

You must provide an online cancellation procedure if the cardholder’s request for merchandise or services was initially accepted online.

You must not complete a recurring transaction beyond the duration expressly authorised by the cardholder or if it receives either a cancellation notice from the cardholder or a decline response.

If the cardholder cancels within the terms of the cancellation policy, you must provide to the cardholder both of the following within three business days:

- Cancellation of refund confirmation in writing
- Credit transaction receipt for the amount specified in the cancellation policy

Visa Account Updater (VAU) and Mastercard Account Billing Updater (ABU) must be implemented to pre-validate card details prior to the submission of a recurring transaction (please see VAU and ABU section for further information).

VAU and ABU are not available for instalment transactions.

If you do not process a recurring or instalment transaction at the time of entering into the agreement with the cardholder, you must:

- Submit an account number verification transaction authorisation
- Identify the account number verification transaction as a recurring or instalment transaction in the authorisation
- Contact your Payment Service Provider (PSP) to enable account number verification transaction authorisation
VAU and ABU

Visa and Mastercard provide services that allow a merchant to verify card details prior to a recurring transaction being submitted.

Visa Account Updater (VAU) and Mastercard Account Billing Updater (ABU) maintain databases that consist of participating issuer card information. These databases enable merchant to validate that a recurring payment agreement has not been cancelled and that the card number/expiry date is valid. Further information is available on request.

Instalment Transaction

Instalment transactions work in a similar way to recurring transactions, with the exception of instalment transactions that represent a single purchase, with payment occurring on a schedule agreed upon between a cardholder and merchant (e.g., loan/car/debt repayment transactions over a set period of time).
An authorisation must be obtained at the time of the transaction. You should not proceed when your request for authorisation is declined. Multiple authorisation attempts following a decline are not permitted. Please remember that it is your responsibility to ensure that all transactions are authorised in accordance with your Merchant Agreement.

**Authorisation**

Authorisation is a check that is undertaken with the card issuer to confirm if they will approve the transaction. Authorisation from the card issuer is not a guarantee of payment.

**Pre-Authorisation**

If you do not know the final amount for which you will submit the transaction, you should be sending an estimated authorisation request. An estimated authorisation amount should be used when your customer is booking a room/vehicle/equipment, and you are not sure if there will be additional charges to be applied later. Estimated authorisation may also be used where orders for goods are placed and multiple items within the order will be dispatched separately. Please remember always to advise the cardholder of the amount you are pre-authorising as these funds will be unavailable on their account.

**Referrals**

A referral occurs when a card issuer requires First Data to contact them prior to providing a response to an authorisation request. This may be prompted by an unusual spending pattern for the cardholder or a large value that triggers the issuer’s fraud detection rules. Your terminal will prompt you to call for authorisation in this instance. Generally, it will be necessary for the cardholder to come to the telephone to answer some security questions. You should follow the instructions given by the authorisation operator. At the end of the call, if authorisation is granted, you will be issued with a code to key into your terminal.

For authorisation, please telephone: 0344 257 9400; lines are open 24 hours a day, seven days a week.
Purchase with cashback allows your customers to request cashback when purchasing goods using their debit card. Written agreement from First Data is needed to take this transaction type. The following rules apply:

- Can only be to customers who make a purchase with their card
- Must be via an electronic terminal, not a manual imprint machine
- Must not exceed the maximum cashback amount confirmed in your written notification from First Data
- Enter the purchase and cashback amounts separately, as prompted by your terminal
- Cashback can be offered on Visa Debit, Visa Electron, Maestro, and Debit Mastercard issued in Europe only
- Follow the terminal prompts; they will tell you whether the purchase with cashback has been approved
You are only permitted to make a card refund when the original sale was on the same card. The refunded amount will be credited to the cardholder’s card and debited from your account.

When processing refund transactions:

› You must check that the card presented for the refund is the same one used for the original sale
› You should never make a refund on the card where the original sale was made by cash or cheque
› You should never make a refund by cash or cheque where the original sale was on a card
› You should never make a card refund for an amount higher than the original sale
If you are unable to use your card terminal for sales and refund transactions, follow the procedures below. The paper vouchers contain the following copies:

- Merchant/Top copy – you must retain this for 18 months from the date of the card or last recurring card transaction (to defend a disputed transaction)
- Processing/Middle copy – you must post this to First Data
- Cardholder/Bottom copy – this is the record of the card transaction to be given to the cardholder

Please note the voucher for a sale is printed with black text, whereas the voucher for a refund has red text and is clearly marked “refund voucher.”

**Completing a Sales/Refund Voucher**

1. Fully complete all the information fields on the voucher
2. Do not mark copies with pencil or paper clips as these can transfer through the carbons and obscure details
3. Check that the details are clear on all three copies to avoid the risk of a chargeback
4. If you make a mistake, you must complete a new sales/refund voucher and destroy the old one
5. For a sale, ask the cardholder to sign the sales voucher, and check that the signature matches the one on the back of the card presented. Failure to do so may result in a chargeback.
6. For a refund, you must sign the refund voucher
7. For both a sale and a refund, you must telephone the Authorisation Centre on 0344 257 9400 for an Authorisation Code for each sale/refund and write the code provided on the sales/refund voucher
8. You cannot alter the sales/refund voucher once you have the authorisation code in order to avoid the risk of a chargeback

The sales voucher must always be completed in pounds sterling (£), unless you have made arrangements with First Data to accept different currencies. An example of a correctly completed sales voucher is shown below:
Preparing/Submitting Vouchers for Submission

You must complete the merchant summary voucher to submit your sales/refund vouchers, retaining the top and middle copies and submitting the bottom copy for processing.

› Fully complete all the information fields on the voucher, including your merchant number and business name
› Do not submit more than 200 vouchers on one merchant summary voucher
› All vouchers must be posted to First Data at Parseq, Lowton Way, Hellaby, South Yorkshire, S66 8RY. This copy is electronically processed. Therefore, please do not fold, damage, pin, or staple, and ensure that the necessary details are clearly recorded.
› To avoid an increase in your processing charges, these must be received by us no later than three business days from the transaction date
› If you do not submit your vouchers within this timescale, the card issuers may reject the card transactions, even though you may otherwise have followed the proper authorisation procedures, and/or you may be subject to a surcharge and/or a chargeback

Warning: Do not submit vouchers when the card transactions have already been processed through an electronic terminal. If in doubt, please telephone the Merchant Support Centre on 0345 606 5055.
Can I Pass Charges to My Customer?

Surcharging is permitted in accordance with local law. If you indicate a price to a cardholder that is not applicable to all methods of payment, then before you accept the card transaction, you must display a statement explaining any methods of payment to which the indicated price does not apply, including the difference in price either as an amount or a percentage:

› For all payments made in-store, or by telephone, you must inform the customer of the charge amount before they authorise the card payment
› For payments in-store you must clearly display a statement regarding any surcharges at the point-of-sale
› For card not present (CNP) payments, you must display a statement explaining the charges on your website, catalogues, advertisements, and any other forms
› Any surcharge amount must be included in the transaction amount and not collected separately
› You must comply with any legal requirements limiting the amount you can charge and what you must tell your customers about the charge. It is your responsibility to check these requirements yourself. Please contact your local Trading Standards Office or equivalent body if you need further information.

Split Sales and Transactions

There may be occasions when a cardholder will request to split payments between several cards, or between a card and cash or cheque.

If several cardholders wish to split the transaction amount into small amounts in order to pay a proportion of a bill, this is permitted; for example, in a restaurant when individuals pay their own bill or a proportion of the total bill. You are permitted to split the total bill between each cardholder.

However, if one cardholder requests that you split a transaction amount between several cards (e.g., where the cardholder may not have sufficient funds on one card), you should proceed as follows:

› Only conduct the transaction if you are not suspicious of the transaction or the person presenting the card
› Ensure that all cards presented are issued with the same cardholder name
› Follow the normal card acceptance procedures as detailed in Section 3
› First Data recommends that you only split a transaction over more than one card when it is a card present (CP) transaction and each transaction is verified by either chip and PIN or signature (as requested by the terminal)

Warning: If a sale transaction is declined, you should not then split the sale over multiple smaller transactions as this could indicate fraudulent activity and result in a chargeback.
## Terminal Fallback

If it is impossible for the terminal to read the chip on the card or if the terminal has a malfunction, you should contact your terminal supplier help desk immediately to report the fault. A representative will try to resolve the problem remotely or, failing this, will arrange for a new terminal to be sent to your premises on the next working day, provided the fault is reported prior to 16:00. This does not include premises situated in the Highlands and Islands, where replacement may take two to four working days. In the interim, follow the guidelines below:

<table>
<thead>
<tr>
<th>Card Type</th>
<th>Revert to Chip and Signature</th>
<th>Revert to Magnetic Stripe</th>
<th>Revert to Plan Key</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maestro and Visa Electron and electronic-use-only cards unable to read magnetic stripe</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
<td>Seek alternative payment method</td>
</tr>
<tr>
<td>Diners Club and Discover® Cards</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Mastercard chip-enabled card. Unable to read chip.</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Seek alternative payment method</td>
</tr>
<tr>
<td>All other card types; chip cards, PIN not enabled. Unable to read chip.</td>
<td>N/A</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>All other card types; chip-and PIN-enabled cards. PIN pad fault. Unable to accept PIN entry.</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>All other card types; magnetic-stripe cards only. Unable to read magnetic stripe.</td>
<td>N/A</td>
<td>N/A</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

You are liable for swiped or key-entered chip-card transactions that are proven to be fraudulent.
A chargeback occurs when a card issuer raises a disputed transaction on behalf of the cardholder. The following section describes the procedures that you should follow, together with suggestions that will help you reduce the risk of chargebacks being debited to your merchant account.

Remember, you may be liable for a chargeback in some circumstances, even if you obtained authorisation for a card transaction.

A cardholder or the card issuer has the right to question/dispute a card transaction. A dispute can normally be raised up to 180 days after the card transaction has been debited to the cardholder’s account. Retaining your sales and refund receipts (see Section 1) will help you respond to this.

A cardholder disputes a transaction because they do not recognise the description on their card statement as it may not match the name of your business (see Section 4).

It is a card scheme requirement that if you are predominantly trading as a mail or telephone order business, a contact telephone number rather than location must be included in the transaction description (e.g., The mail order shop 01234 567890); for eCommerce transaction, the transaction description should include a reference to your website address and a contact telephone number or mail address. This provides the cardholder with the ability to verify the transaction with you rather than disputing it with their card issuer (see Section 4).

You can change the description that appears on the cardholder statements by contacting our Merchant Support Centre on 0345 606 5055†.

Common Causes of Chargebacks

The most common causes for chargeback are:

- A fraudulent mail, telephone, or eCommerce transaction
- You do not respond in time to a request for a copy of the transaction (retrieval request)
- The card was not valid at the time of the transaction (this could be before the valid date or after the expiry date)
- Authorisation was not obtained
- The signature on the transaction receipt does not match what is on the card
- The goods or services provided were not as described, were defective, or were not received
Retrieval Requests

In many cases, before a chargeback is initiated, the card issuer requests a copy of the sales voucher via a “retrieval request”. Once a retrieval request is received, we will respond by sending a copy of the card transaction, if available.

Where you hold electronic sales receipts or terminal sales receipts for electronically processed card transactions, it is your responsibility to respond to all retrieval requests received within 14 calendar days of our initial request. You are responsible for retaining and providing copies of sales receipts and any refund receipts for a minimum of 18 months from the original card transaction date. If First Data does not receive a clear, legible copy of the sales receipt on time, you may be subject to the chargeback simply by failing to meet the card scheme timescale.

Chargeback Reversal Procedure

When a chargeback is received, we will debit the disputed amount from your account and contact you with details of the card transaction together with the information/documentation we require from you and the deadline by which we require it.

If the information provided is sufficient to warrant a reversal of the chargeback and is within the applicable timescale, we will attempt to defend the chargeback. However, reversal is contingent upon acceptance by the card issuer under the applicable card schemes guidelines. If the chargeback is successfully reversed, the card issuer has the right to present the chargeback a second time, and your merchant account will be debited again if you have not complied fully with the terms of your Merchant Conditions and this Operating Guide. We will do our best to help you defend a chargeback. However, due to the short timeframes and supporting documentation necessary to successfully (and permanently) reverse a chargeback in your favour, we strongly recommend the following:

› Ensure card transactions are completed in accordance with the terms of your Merchant Conditions and this Operating Guide
› If you do receive a chargeback, send us the requested documentation within the required timescale
› Whenever possible, contact the cardholder directly to resolve the inquiry/dispute but still comply with the request for information in case this does not fully resolve the matter
Vehicle Rental Services

If you are a vehicle rental company or a third-party that accepts guarantee rental reservation, using pre-authorisation when taking card payments will add additional security to the transactions because the card will be checked before the customer takes the vehicle. Please remember that the pre-authorisation from the card issuer is not a guarantee of payment. It is only a check that the card has not been reported lost or stolen and that there are sufficient funds at the time of the transaction. Written agreement from First Data is needed to take this transaction type.

Please read the guidelines below carefully to understand regulations and risks associated with taking vehicle-rental-service card payments.

Information to Obtain from the Cardholder

- Name of the person making the reservation
- Telephone number
- Name of person(s) requiring the vehicle
- Expected collection date and time
- Number of days of expected vehicle hire
- Card number
- Card expiry date
- Cardholder name
- Cardholder billing address
- Card Security Code (only for telephone and eCommerce transactions)

You should discuss and agree with the terms of hire. This should include, but is not limited to, hire rates, cancellation and no-show policy, and procedures, along with any additional charges that may be applied, such as damages or parking tickets.

Procedure for Completing Vehicle Rental Transaction

Pre-Authorisation

You can pre-authorise the transaction before the car rental period begins. It allows you to estimate the final transaction amount, gain authorisation, and reserve the funds before the hired vehicle is returned. The estimation should be based on the intended rental period, rental rate, and applicable tax and mileage rate. Please remember that the estimation cannot include potential vehicle damage.

Your Terminal User Guide should provide instructions of how to perform the pre-authorisation. Ensure that your customer understands that the pre-authorised amount will be deducted from the available funds on the card. You should process the payment AFTER the vehicle is returned. The payment should not include any additional
charges such as vehicle damage. These charges should be processed separately. The Authorisation Code received for an approved pre-authorisation should be used to complete the transaction. If the final bill is more than the pre-authorised amount, you must obtain another authorisation code for the difference, with the exception of Visa, where the bill can be within 15% of the authorised amount.

**Cancellation Policy**

Please note that whilst you may have a cancellation policy within your Terms and Conditions (which you must clearly communicate to your customer), you must not charge any cancellation fee if the cardholder cancelled the reservation in accordance with the outlined procedures.

Within your cancellation period, you must not require cancellation notification of more than 72 hours to the scheduled collection time and date of the booking without penalty. If the cardholder makes a reservation within 72 hours of the scheduled pick-up date, the cancellation deadline must be no earlier than 6 p.m. at the address of the scheduled pick-up date.

If a reservation has been properly cancelled in accordance with the communicated cancellation policy, you are required to provide the cardholder with a cancellation code and advise them to retain it for their records. You must then send a written confirmation of the cancellation to the cardholder within five business days.

**No-Show Policy**

If the cardholder does not turn up within 24 hours of collection time and they did not cancel the reservation in accordance with your Terms and Conditions, you may charge the customer for the maximum value of the one-day rental. To do so, you will need to perform a card not present (CNP) transaction, writing “No Show” on the receipt, and send a copy of a no-show receipt to the billing address provided at the time of booking.

**Refund Policy**

If you operate a no-refund policy, this must be made clear to the cardholder when discussing the reservation. If you do agree to refunds, you must credit them to the same card as the one used to make the reservation. Where a charge is made to a card in error, the reversal must be applied to the card within 30 calendar days. Do not refund by cash or other payment methods as this could result in chargebacks.

**Delayed Charges**

For you to process a delayed charge (e.g., damage to the vehicle, fuel, insurance fee, parking tickets, excessive mileage, etc.), the cardholder must have given their consent by signing the rental agreement and agreeing to your Terms and Conditions. Any delayed charges must be processed within 90 days of the original transaction date, and you must obtain further authorisation. These charges must be submitted as a separate transaction with “signature on file” clearly visible. The cardholder must be notified in writing of any delayed charges.

**Providing Evidence to the Cardholder**

Before you process any additional charges, you need to inform your customer and provide evidence to support the claim. You need to provide:

- Details of the violation
- Time and place of the violation
- The law violated and, if applicable, a copy of the accident report
- A copy of parking tickets
- The license number of the rental vehicle
The amount of the charge

A copy of the rental agreement

Evidence that the cardholder read the Terms and Conditions agreeing to responsibility to pay any additional charges

Proof that the car was damaged, had a shortage of fuel, etc. on return

**Car Rental Damage – Visa Cardholders**

- You need to provide written confirmation to the cardholder within 10 business days from the return of the vehicle advising of the damage and the cost
- Within 10 business days from receiving written confirmation, the cardholder has the right to provide an alternative estimate for the cost of repairing the damage. A cardholder has the right to raise a chargeback if the agreement is not reached and the additional charges are debited.
- You need to wait 20 business days before processing the delayed/additional charges

**Car Rental Damage – Mastercard Cardholders**

To apply additional charges to a Mastercard, you must obtain a separate cardholder-signed authority by processing a card present (CP) transaction. If the charge is disputed at a later date, this will be required as proof that the cardholder authorised the additional charge.

Processing transactions differently may result in a chargeback and, therefore, losses to your company. As in all other cases, we will try to defend a chargeback. We may ask you to provide us with:

- A copy of the rental agreement, stating vehicle rental period
- A copy of the document signed by the cardholder agreeing to accept responsibility for the delayed charges
- A copy of the original notification you have sent to the cardholder informing them about the charges
- A proof of cost estimation
- A proof of law validation, such as a parking ticket, a speeding ticket, etc
- Any supportive documentation, such as police reports, insurance policy of the rental vehicle, etc., demonstrating cardholder liability

Not receiving requested documentation on time may prevent us from defending the dispute and may result in a debit to your account.

**Hotels, Lodging, and Accommodations**

**Advanced Reservations**

To be able to take advanced reservations, you will need to have an agreement with First Data to process MOTO and eCommerce transactions. Wherever possible, the cardholder requiring accommodation or lodging should be asked to make the reservation. However, for practical reasons, you may need to accept reservations from third parties, such as secretaries acting on behalf of their managers. Advanced reservation allows your customers to book a room in advance. As you will obtain the card details, you will be able to charge the cardholder if they do not turn up or do
Information to Obtain from the Cardholder:

- Name of the person making the reservation
- Telephone number
- Name of person(s) who will be using the room
- Expected arrival date and time
- Number of days of expected stay
- Card number
- Card expiry date
- Cardholder name
- Cardholder billing address
- Card Security Code (only for telephone and eCommerce transactions)

If the booking is for corporate purposes, you should also collect the following information:

- The caller’s name and position in the company/organisation
- The name of the company/organisation
- The company/organisation switchboard telephone number

You should discuss and agree to the room rate and obtain cardholder consent to your cancellation and no-show policy. This must be clearly explained to the customer.

Advanced Deposits

Please note: If you take advanced deposits for a room reservation, under card scheme regulations, this is the only amount you can debit the customer. You will also forfeit your right to charge one night’s no-show payment. If you operate a no-refund policy, you must make it perfectly clear to the cardholder at the time of the reservation. Any refunds must be made to the card used for the original booking. You must not refund by cash, cheque, or other means.

Once you and the cardholder have agreed on the deposit, please inform the cardholder of the following:

- Room rate (including tax)
- Amount of advanced deposit that will be billed on the card (which must not exceed the cost of 14 nights’ accommodation)
- Explain that the deposit will be deducted from the final bill
- Explain that the accommodation will be held for the period covered by the advanced deposit

No Show or Invalid Cancellation

If the reservation is not done in accordance with your cancellation policy (late cancellation) or if the customer does not show up, you may charge one night’s stay. To do so, you will need to perform a card not present (CNP) transaction and send a copy of the final bill to the billing address provided at the time of booking.

Guest Arrival/Check-In

Upon arrival of your guest, request to see the card with which the booking was made, and ask them to complete a registration form. If you wish to charge additional services/items to the guest’s room, such as newspapers and bar charges, your registration form must clearly show this.
Pre-Authorisation

Pre-authorisation allows you to estimate the final bill and reserve funds on the card for that amount whilst your guest is staying with you. We recommend that you obtain full payment upon check-in for the expected number of nights of the stay. The cardholder’s total charges can be estimated based on:

› Expected length of stay
› Room rate (including tax)
› Estimated miscellaneous charges

Please advise the cardholder how much you have pre-authorised as this will reduce the amount of funds they have available on their account. The pre-authorisation helps protect you from fraudulent card use and confirms if the cardholder’s account is valid and has sufficient funds available. Authorisation from the card issuer is not a guarantee of payment.

Departures/Checkout

When the cardholder wishes to check out, calculate the final bill amount and compare this with the pre-authorisation. If the final bill is more than the pre-authorised amount, you must obtain another authorisation code for the difference, with the exception of Visa, where the bill can be within 15% of the authorised amount.

Express Checkout

You may want to offer your customer the option to leave the key and check out without waiting for the bill. If you decide to offer your guest an express/priority checkout service (the card is no longer present), be aware that you may not be able to defend you from a chargeback if a cardholder later denies any transactions.

If the cardholder requests priority checkout, at check-in you must:

› Record the card number, expiry date, and cardholder name
› Inform the cardholder of your policy regarding any charges discovered after checkout
› Give the cardholder a priority checkout agreement to complete. When the cardholder returns the agreement, ensure that:
   • It is signed
   • It includes the mailing address
   • The card number on the checkout agreement matches the card number on the pre-authorisation

Upon checkout, you must complete the transaction for the total charges incurred during the cardholder’s stay. If the final bill is more than the pre-authorised amount, you must obtain another authorisation code for the difference, with the exception of Visa, where the bill can be within 15% of the authorised amount.

Extended Stays

Those requiring longer stays should be asked to pay the current total due. You can ask for their card, or you can use the card details provided during check-in. However, please be aware that there is a risk that this amount could be disputed at a later date if no signature or PIN is obtained.

Pre-authorisations are not supported for Maestro cards. We recommend that you obtain full payment for the expected number of nights of the stay. If the cardholder decides to check out early, simply provide a refund.

If the bill is more than 15% above the pre-authorised amount or Mastercard is being used, you must obtain another authorisation code for the remainder of the stay.
Additional Charges

Please remember that any additional charges following checkout must be processed within 90 days from the date of departure. You will need to write on the transaction receipt "Signature on File" and send a copy to the cardholder’s address given to you at the time of reservation.

Additional Checks

In some circumstances (depending on country-specific scheme processing regulations), you will be required to ask the cardholder for secondary proof of identification:

› Ask the cardholder to provide a second form of identification. This should be a passport or a full driving licence.
› Check that the photograph of the document resembles the person who presented it to you and that there are no visible changes to the picture that may indicate the document is not genuine.
› Check that the second identification document is not out of date and that it shows the cardholder’s signature
› On the front of the receipt, record the description of the identification (e.g., driving license, passport, etc.) and include the serial number displayed on the identification. Additionally, if a photo is present, annotate the receipt with "Photo Card Presented", which proves the cardholder’s identity was verified by photograph.
› The first four digits of the card number (if present) are printed immediately below the card number. These first four digits must be recorded on the front of the transaction receipt to validate that they have been checked.

Remember

› Never process Maestro cards
› You must always obtain an authorisation
› Never proceed with a transaction if the cardholder is unable to provide an acceptable second form of ID as these transactions may be charged back to you and debited from your account
› Any fees to be charged must be included within the total transaction value and disclosed to the cardholder prior to completing the transaction
› It is your responsibility to undertake the additional identity checks

Dynamic Currency Conversion (DCC)

DCC provides you with the ability to offer overseas Visa and Mastercard cardholders the option to pay for goods or services in the currency in which their card is issued. The price of goods and services will be shown to the cardholder in pounds sterling (£) and in their own currency, along with the exchange rate used. Exchange rates stored in your terminal are updated automatically.

You Must:

› Inform the cardholder that DCC is optional
› Not impose any additional requirements on the cardholder to have the transaction processed in the local currency
› Not use any language or procedures that may cause the cardholder to choose DCC by default
Receipt Requirements

DCC transaction receipts must show the following:

› The currency symbol of the local currency of your outlet
› The transaction amount of the goods or services purchased in the local currency of your outlet
› The exchange rate used to determine the cardholder currency transaction amount
› The total transaction amount charged by you in the transaction currency, followed by the words “Transaction Currency”
› A statement, easily visible to the cardholder, that specifies the following:
   • The cardholder has been offered a choice of currencies for payment, including the local currency of your outlet
   • The currency selected by the cardholder is the transaction currency
   • The DCC is conducted by you. Written agreement from First Data is needed to take this transaction type.

Multicurrency and Cross-Border Transaction Acceptance

This functionality allows you to operate across several European countries and centralise your payment card processing arrangements. Written agreement from First Data is needed to take these transaction types.

Permitted Merchant Location Countries

The merchant location is either the physical premises where a transaction is completed or an eCommerce or MOTO transaction in which all the following occur:

› There is a permanent establishment through which transactions are completed. In the absence of a permanent establishment, a merchant who provides only digital goods must use the country where the principals of the company work.
› The merchant holds a valid business license for the merchant location
› The merchant has a local address for correspondence and legal process
› The merchant outlet pays taxes relating to the sales activity

Available Funding and Settlement Currencies

Transactions can be accepted in any currency and settled to you in British Pounds Sterling (GBP), Euro (EUR), or U.S. Dollars (USD). You can also receive settlement in any of the currencies below, provided the transaction currency is the same:

› GBP
› EUR
› USD
› Australian Dollar
› Canadian Dollar
› Swiss Franc
› Japanese Yen
› Norwegian Krone
› Swedish Krona
› Danish Krone
› Hong Kong Dollar
› New Zealand Dollar
› South African Rand

If you are interested in expanding your business by offering this service to your customers, please contact our Merchant Support Centre on 0345 606 5055†.
Payment of Debt

You may accept Visa Debit, Visa Electron, and Mastercard cards for the payment of mortgages and loans. However, during the transaction you must:

› Obtain authorisation, providing additional data. For more information, please contact our Merchant Support Centre on 0345 606 5005.

› Complete the transaction as a purchase flagged as instalment payment

› Write the type of payment made on the receipt (e.g., "Loan" or "Mortgage")

› On the signature line of the receipt, write “Instalment Transaction”
Payment Card Industry Data Security Standard (PCI DSS)

This standard is managed by the Payment Card Industry Security Standards Council set up by the payment card brands (Mastercard, Visa, American Express®, Discover, and JCB®). PCI DSS outlines the minimum security requirements to help businesses handle payment information securely. The card brands require that any business accepting cards for payment of goods or services must be compliant with the PCI DSS.

Becoming PCI Compliant

To report your PCI DSS compliance for your business, you need to identify and complete the appropriate self-assessment questionnaire. Securing your business requires the following steps:

› Analyse your business practice and processes
› Research the appropriate security solutions for your business
› Implement and maintain security solutions

Central to this is that you protect your customers’ payment card data. You must make sure that you have security controls in place at all times to maintain your compliance. Your customers trust you to keep their information safe; you need to repay that trust with compliance, at the very least.

PCI DSS Requirements As Set Out by the Card Schemes

1. Build and maintain a secure network
2. Install and maintain a firewall configuration to protect cardholder data
3. Do not use vendor-supplied defaults for system passwords and other security parameters
4. Protect cardholder data
5. Protect stored data
6. Encrypt transmission of cardholder data across open public networks
7. Maintain a vulnerability management program
8. Use and regularly update antivirus software or programs
9. Develop and maintain a secure system and applications
10. Implement strong access control measures
11. Restrict access to cardholder data by business need-to-know
12. Assign a unique ID to each person with computer access
13. Restrict physical access to cardholder data
14. Regularly monitor and test networks
15. Track and monitor all access to network resources and cardholder data
16. Regularly test security systems and processes
17. Maintain an information security policy
18. Maintain a policy that addresses information security for all personnel
Implications of Not Complying With the PCI DSS

Not being compliant with the PCI DSS can leave your business at risk of a data breach and related costs. Most people do not realise that these can be quite substantial and can include card scheme fines and card replacement costs.

Other factors include loss of customer confidence and damage to the reputation of your business, not to mention your business being open to lawsuits and audits. You may also be subject to non-compliance fees.

Third-Party Obligations

You are responsible for making sure that all third-party service providers that come into contact with your customers’ cardholder data are compliant with the PCI DSS at all times. This may include any web-hosting provider, software application provider, PSP, processing bureau, vendor, etc. used by your business. If these third parties could impact the ways that you process card payments, then they must be compliant with the PCI DSS. Remember, their compliance status directly impacts your compliance status.

Secure Data Storage

It is potentially much easier for a hacker to break into a business network than it is for a burglar to break into a business location. Any stored payment card data must be encrypted, as set out by the PCI DSS. Storing unencrypted card data electronically is strictly prohibited. If you have to store data to process card transactions, then you must do so securely. This could relate to any stored data, be it paper copies, digital or electronic files, and audio or voice recordings.

If you can demonstrate that storing your customers’ card data is necessary for your business, then you must have a process in place to do so securely. The only data that you are allowed to store includes:

› The long card number and expiry date
› Passwords, pass phrases, and any other unique card data supplied as part of the card payment
› The name, address, description of the purchase, amount, and any other detail that may identify the customer and their purchases

You may not, under any circumstances, store certain types of data. This includes:

› The CVV2, also called the Card Security Code (CSC), which is displayed on the back of the card, in or next to the signature panel
› The CVV number, which is contained in the magnetic stripe
› The CVV number, which is contained in the chip
› The contents of the magnetic stripe, also called Track 2 Data
› The customer’s PIN, which is contained in the magnetic stripe (PIN Verification Value – PVV)
**Demonstrating Compliance With PCI DSS**

You must show that you are compliant by reporting annually. To make reporting your compliance as easy as possible for you, we have provided you with the First Data PCI DSS Compliance Program. You will receive your personal access details and instructions for logging in by letter.

<table>
<thead>
<tr>
<th>STEP 1</th>
<th>STEP 2</th>
<th>STEP 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>› Log into the online portal</td>
<td>› We will help you to understand how to protect your business</td>
<td>› You will be asked to confirm and validate all of your responses and any tasks that you may have to undertake</td>
</tr>
<tr>
<td>› We will ask you a few questions</td>
<td>› This will help you understand and identify areas of your business that might be at risk</td>
<td>› PCI DSS refers to this as your Attestation of Compliance (AoC)</td>
</tr>
<tr>
<td>› These questions focus on how your business is set up to handle credit and debit card payments</td>
<td>› You will be taken through the security assessment that matches your business type, including any scanning, if needed</td>
<td></td>
</tr>
<tr>
<td>› Using dynamic profiling, we will only ask questions that are relevant to your business to figure out your security risk level</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Make sure that you answer the questions accurately as this determines the method of validation you must undertake. Whether you need to self-evaluate using our online portal or need to submit a Report on Compliance (ROC), which requires a Qualified Security Assessor, the First Data compliance program will direct you through both methods. Once you have finished your reporting, remember that PCI DSS compliance is an ongoing process. In order to maintain compliance, maintenance task reminders may be sent to you throughout the year. You must make sure that you validate your compliance on an annual basis. We will send you reminders in advance of your renewal date.
Keeping Your Point-of-Sale (POS) Device Safe

Chip and PIN has significantly reduced fraud; however, POS devices will continue to be targeted by criminals wanting to commit fraud. You must take care to ensure that no one, other than an authorised engineer, has the opportunity to tamper with your POS device.

Criminals use stolen card and PIN details to produce fake magnetic swipe cards for use abroad, where chip and PIN is not used, or for use in cash machines. A criminal may pose as an engineer to gain entry to your POS device. They may try to replace certain components of your device with bogus parts fitted with data capture devices or insert a pinhole camera to photograph card and PIN detail. They may even try to replace the whole device with one that is already equipped with data capture equipment.

Please note: A legitimate engineer will never visit your premises without contacting you first. This may be via the terminal vendor or an employee from First Data. Never disclose your merchant number or your terminal details to anyone else.

Recommendations:

- Do not allow anyone other than a legitimate engineer or a direct employee of First Data to remove your terminal from your premises
- In the event you suffer a communication failure in your premises, the terminal will store up to five transactions until it is next able to go online. Although this poses minimal risk, a criminal may try to steal your POS device to extract any data stored. A PIN stand secured to your countertop is a good deterrent against theft, although these must allow access in accordance with the Disability Discrimination ACT 1995.
- A criminal may try to force or bribe a staff member to allow them access to the POS device in order to fit a data capture device
- Your staff should be trained regularly on POS security and must report any incident they feel is a threat to the device
- You should carry out some simple checks on a daily basis to ensure that your POS device has not been tampered with
- Check that your device is not damaged
- Check that no additional stickers are on the device that were not attached at the time of installation
- Ensure that your POS device has not been modified and that there are no additional components that were not there previously

If you detect anything suspicious with your POS device, do not use it and report it immediately to our Merchant Support Centre on 0345 606 5055.
Positioning Your POS Device

You must consider cardholder privacy when positioning your POS device:

› The POS should be placed in a position where the cardholder cannot be observed whilst entering their PIN details
› The POS must not be positioned directly in view of CCTV cameras
› If a PIN shield is provided with your POS, it should be used
As shown in your Merchant Agreement Charges Schedule, your transactions may incur a non-qualifying charge. Depending on the type of card used and how you take the payment, your transactions will be categorised as either qualifying or non-qualifying.

**Card Present**

**Qualifying Transactions Are:**
- Chip-and-PIN, contactless, and swiped transactions submitted for processing within two business days of the transaction

**Non-Qualifying Transactions Are:**
- Payment with a Visa Business Debit Card
- A card not present (CNP) transaction

**Card Not Present MOTO**

**Qualifying Transactions Are:**
- MOTO transactions that capture the Card Security Code (CSC) submitted for processing within two business days of the transaction

**Non-Qualifying Transactions Are:**
- Transactions that do not capture the card’s CSC number
- Payment with an EU or International Mastercard or Maestro Card, Mastercard Reward, World Elite or World Cards, Debit Mastercard
- Payment with a Visa Business Debit Card or International Visa Card

**Card Not Present eCommerce**

**Qualifying Transactions Are:**
- 3D secure enabled eCommerce transactions submitted for processing within two business days of the transaction

**Non-Qualifying Transactions Are:**
- MOTO, Face-to-Face (Card Present) or Recurring Transactions
- Payment with a Visa Consumer Charge Card
- Payment with Mastercard World Signia and World Cards
First Data is authorised and regulated by the Financial Conduct Authority (FCA). If you have reason to complain, we will take a balanced and fair view of the situation and take whatever action is necessary to resolve your complaint.

The Financial Services and Markets Act 2000 lays down a standard procedure that we follow to handle all complaints. You can contact our Client Service Team as follows:

**Complaints Team**

P.O. Box 280, Lowton Way, Hellaby, Sheffield, S98 1RU or
Telephone: 0345 606 5055†, 8 a.m.–9 p.m. Monday–Saturday, or contact us at UKSolutionsHelp@firstdata.com

We take all complaints seriously. Whilst many can be dealt with straight away, some take more time to investigate. The FCA gives us eight weeks to resolve all complaints, but if you are not happy with the outcome, please contact us explaining what you think we can do to put it right. If you remain dissatisfied after we have tried to put things right, you can ask The Financial Ombudsman to look at your case for free. They can be contacted at:

- **Address**: The Financial Ombudsman Service Exchange Tower, London E14 9SR
- **Telephone**: 0800 023 4567 or 0300 123 9123
- **Email**: complaint.info@financial-ombudsman.org.uk
- **Website**: www.financial-ombudsman.org.uk
Useful Contact Information

**Authorisation Service**
Tel: 0344 257 9400 or 01268 823 130 (Open 24 hours, seven days a week)

**Merchant Support Centre**
For any queries about your First Data service, please call 0345 606 5055† (open 8 a.m.–9 p.m., Monday–Saturday). Alternatively, write to us at: P.O. Box 280, Lowton Way, Hellaby, Sheffield S98 1RU.

**PCI DSS Compliance Program**
For queries regarding your PCI DSS Compliance status, please call the PCI DSS Help Desk on 0330 808 1606† (open 9 a.m.–5 p.m. Monday–Friday)

**First Data Global Leasing**
For queries regarding your terminal lease, please call First Data Global Leasing on 0345 841 2442† (open 9 a.m.–5 p.m. Monday–Friday) or email FirstDataGlobalLeasing@firstdata.com

**Terminal Manufacturers**
Clover Support Tel: 0345 605 0615 (open seven days a week, 8 a.m.–9 p.m.) or email UKCloverSupport@firstdata.com.
Spire, Verifone, Ingenico, and First Data Terminal Helpdesk Tel: 0345 606 5055† (open 8 a.m.–12 p.m. Monday–Saturday; 9 a.m.–5 p.m. on Sunday and bank holidays).

**Business Track®/ClientLine®**
For queries, please call the Help Desk on 01268 567 128 (Open 8 a.m.–9 p.m. Monday–Saturday)

**Dynamic Currency Conversion**
For queries regarding DCC, please call the Merchant Support Centre on 0345 606 5055† (open 8 a.m.–9 p.m. Monday–Saturday)

**American Express®**
For queries regarding American Express, please call the American Express Help Desk on 01273 675 533 (open 8 a.m.–6 p.m. Monday–Friday; 9 a.m.–5 p.m. on Saturday)

**Stationery**
Stocks of stationery (e.g., sales, refund and merchant summary vouchers and deposit envelopes) can be ordered by calling the Merchant Support Centre on 0345 606 5055†

**Point-of-Sale and Display Material**
Point-of-sale material is available by telephoning the Merchant Support Centre on 0345 606 5055†
Changes to Your Business

It is vital that you keep us updated with any material changes to your business, including (but not limited to):

› Bank details (e.g., account number, sort code, branch address)
› Contact names, phone numbers (landline and mobiles), email addresses, and website addresses
› Legal entity of the business and/or trading name
› Business closure (including outlets) or change of ownership (e.g., changes to the directors or directors names, changes to voting control or shareholding)
› Products or services your business provides and/or for which it takes card payments
› Methods by which you take card payments
› New and/or additional outlets
› Any insolvency event affecting your business, any arrangement with creditors, or any financial difficulties

Please notify us immediately of any changes by email at UKcustservice@FirstData.com or in writing to First Data, P.O. Box 280, Lowton Way, Hellaby, Sheffield S98 1RU. Please quote your Merchant Identification Number.
This Operating Guide forms part of your Merchant Agreement, so please read it carefully and keep it in a safe place for future reference. All capitalised terms used in this Operating Guide and not otherwise defined in this Operating Guide shall have the meanings set out in the Merchant Conditions.

**Merchant Support Centre:**

0345 606 5055†

Lines open 8 a.m.–9 p.m. Monday–Saturday

†Telephone calls may be recorded for security purposes and monitored under the quality control process.