Clover™ Operating Guide
This Operating Guide forms part of your Merchant Agreement, so please read it carefully and keep it in a safe place for future reference. If you have any questions about our service or this guide, please contact us directly on the number below.

† Calls may be recorded. Calls cost 5p per minute, plus your phone company’s access charge.

Merchant Support Centre:

**0845 605 0615†**

Lines open 7am – Midnight, 7 days a week

This Operating Guide should be read in conjunction with the Merchant Conditions. 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.
1. Some Basic Rules - Page 6
   - You Must
   - You Cannot
   - Record Keeping
   - Storage of Cardholder Information

2. Things You Need to Know Before You Accept Card Payments - Page 7
   2.1 Payment card recognition - Page 7
      - Visa
      - Visa Credit Cards
      - Visa Electron
      - Visa Prepaid
      - Visa and Visa Electron Mini Cards
      - MasterCard
      - MasterCard Credit Card and Debit MasterCard
      - Maestro
   2.2 Commercial Cards - Page 10
      - Business Card
      - Corporate Card
      - Purchasing Card
   2.3 How to guard against fraud - Page 11
      - Preventing and Detecting Fraudulent Card Not Present Transactions
      - Preventing and Detecting Fraudulent Card Present Transactions
      - Counterfeit Cards
      - Delivery Warning Signals
      - Instruct Your Courier
      - Card Chip-Read/Swipe Failure
      - Returning Wanted or Recovered Cards
      - Reward Scheme
      - Other Important Fraud Considerations
   2.4 Card scheme requirements - Page 14
      - Payment Card Industry Data Security Standard (PCI DSS)
        - What is PCI DSS?
        - Why Comply with the PCI Security Standard?
        - Secure Data Storage
        - PCI DSS Requirements
        - Demonstrating Compliance with PCI DSS
        - Maestro Mandate

3. Accepting Card Transactions - Page 16
   3.1 Card Present Transactions - Page 16
      - Using Your Point of Sale Terminal
      - Manual Entry for Card Present Transactions
        - Non Chip Cards
        - Terminal Fallback
      - Contactless Transactions
        - What is a Contactless Transaction?
        - Accepting Contactless Card Payments
        - Authorisation and Code 10 Calls
          - Definition of Authorisation
          - Referrals
          - Code 10 Calls for Card Present Transactions
          - Refund Process
          - Purchase with Cashback
   3.2 Card Not Present Transactions - Page 19
      - Definition of Card Not Present
      - Card Not Present Transactions
      - Card Security Code
        - How You Must Treat the Card Security Code
      - Address Verification Service
      - Electronic Transactions
      - Authorisation Responses
      - Pre-Authorisation
      - Rules for Mail Order/Telephone Order Transactions
      - Recurring Transaction
        - VAU and ABU
        - Qualifying and Non Qualifying Transactions
   3.3 Internet Card Transactions - Page 25
      - Applying to Take Internet Card Transactions
      - Website Requirements
        - Order Page (basket)
        - Payment Page (check-out)
      - Verified by Visa and MasterCard SecureCode
      - Payment Service Provider
      - Receipt Requirements
      - Website Content
        - Merchant Details
        - Products and Pricing
        - Placing an Order
      - Payments and Refunds
      - Recurring Payments
      - Delivery and Guarantees
   3.4 Refund Process - Page 28
   3.5 Global Choice / Dynamic Currency Conversion - Page 29
   3.6 Multi-Currency & Cross Border Acceptance - Page 29
      - Permitted Merchant Outlet Location Countries
      - Available Funding and Settlement Currencies
   3.7 Bureau de Change - Page 30
4. General Procedures and Banking - Page 31
   4.1 Everyday procedures - Page 31
   - Banking Procedures
   - Fallback Paper Processing Procedures
     - The Sales Voucher
     - Completing a Sales Voucher
     - The Refund Voucher
     - Processing Refunds Using the Fallback Procedures
     - Completing a Refund Voucher
     - Preparing Vouchers for Submission
     - Submitting Vouchers
     - Refund Voucher Process
   
   4.2 Exceptional procedures - Page 34
   - Can I Pass Charges to My Customer?
   - Minimum Charging
   - Split Sales and Transactions
   - Alteration of Amounts

5. Chargebacks and Retrieval Requests - Page 36
   - Why Chargebacks Occur
   - Chargeback Reversal Procedure
   - Common Causes for Chargebacks
   - Retrieval Requests
   - To Help Reduce the Risk of Chargebacks

6. Payment of Debt - Page 38

7. Vehicle Rental Reservation Service - Page 39
   - Telephone Reservations
   - Fax or Mail Reservations
   - Internet Reservations
   - Reservation Confirmation
   - Your Cancellation Policy
   - No Show
   - Vehicle Collection
   - Estimated Authorisation
   - Pre-Authorisation
   - Delayed Charges
   - Accident or Collision
   - Accepting Split Sales
   - Refund Policy
   - Extended Hire
   - Disputed Transactions

8. Hotels, Lodging and Accommodation - Page 43
   - Advance Reservations
   - Telephone Reservations
   - Fax or Mail Reservations
   - Internet Reservations

9. Keeping Your Point of Sale Terminal Device Safe - Page 47

10. Changes to Your Business - Page 48
    - Change of Bank and/or Branch
    - Change of Address
    - Closure or Change of Ownership
    - Change of Business or Trading Name
    - Change of Legal Entity
    - Change of Products or Services Sold or Other Details
    - Changing Your Trading Terms
    - Other Changes Affecting Your Business
    - Changing Method of Taking Cards

11. Voicing Your Concerns - Page 50

12. Additional Information - Page 51
    - Stationery
    - Point of Sale and Display Material
    - First Data Merchant Solutions Artwork Guide
    - Emergencies & Disruptions

13. Useful Contact Information - Page 52
    - Authorisation Centre
    - Merchant Support Centre
    - PCI DSS Compliance Programme
    - First Data Global Leasing
    - Terminal Manufacturers
    - ClientLine
    - Global Choice – Dynamic Currency Conversion
    - American Express
    - Plusnet/Phoenix

14. Glossary - Page 53
SECTION 1: Some Basic Rules

1. Some Basic Rules

To get the most out of your service, it is important to follow some basic procedures that are strictly enforced by VISA® and MasterCard®.

You Must

→ Clearly display Card acceptance logos for your customers to see, for example VISA and MasterCard.
→ Ensure that any charges in respect of Credit Cards do not exceed the charges payable by you as detailed in your Application Form.
→ Provide a Sales Receipt for the Cardholder, to indicate that you have debited their payment card.
→ Include any taxes in the amount charged on Card Transactions, they may not be collected by you in cash.
→ Validate compliance with the Payment Card Industry Data Security Standard (PCI DSS). Please see Section 2.4 for further information.
→ Notify us of any changes to your business.

You Cannot

→ Levy charges in respect of the acceptance of Debit Cards.
→ Indicate that VISA and MasterCard or any other Association endorses your goods and services.
→ Establish procedures that discourage, favour or discriminate against the use of any particular Card.
→ Ask the Cardholder to supply any personal information, for example home or business telephone number, home or business address, or drivers licence number specifically for the payment card transaction, unless instructed by First Data Merchant Solutions.
→ Submit a Card Transaction or sale that has been previously subject to Chargeback.
→ Accept any direct payments from Cardholders e.g. cash/cheque for credit of the Card account. Only the card-issuing bank is authorised to receive such payments.
→ Process paper transactions (except when following the Fallback Procedures) Please see Section 4.1.
→ Accept Card Transactions on behalf of third parties.
→ Manually key payment Card Transactions into a Point of Sale Terminal when the Card details have been provided via an internet shopping cart.
→ Process Card Not Present Transactions without prior notice from the Cardholder.
→ Process Internet Card Transactions without prior agreement and designated internet facility.
→ Store sensitive card data.
→ Require, or indicate that you require, a minimum transaction amount to accept a valid and properly presented Card.

Record Keeping

In order to help us to defend potential retrieval requests and Chargebacks on your behalf, please retain and, if requested, provide copies of Card Transaction documents for a minimum of 24 months after completion of each Card Transaction.

A Card Transaction is only completed on the final delivery of goods or services.
→ Please supply all Sales Receipts and Refund Receipts requested by us within 14 calendar days. Strict time limits for the supply of this information are enforced by each of the Card Schemes.
→ When we request a copy of a Sales Voucher, the Card Issuer may only supply us with the Card Transaction date and Card Number. It is important that you store your Sales Receipts carefully and in date order, followed by the Card Number, to ease the retrieval process.
Storage of Cardholder Information
Do 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 value printed on the signature panel of the Card
→ Store only the portion of the customer’s account information that is essential i.e. name, account number and expiry date.
→ Store all material containing this information in a secure area in accordance with the PCI DSS.
Please see Section 2.4.
→ 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. After such time, destroy or purge all media containing obsolete transaction data with Cardholder Information.
→ PCI DSS rules apply if you (or your agent) store data electronically. Please see Section 2.4.

2. Things You Need to Know Before You Accept Card Payments

2.1 Payment Card Recognition

Visa
All Visa Cards have a Visa logo, holographic feature, ultraviolet feature and Card Security Code (CSC).
Not all Visa Cards are embossed or have a full account number or Cardholder name.

Visa Credit Cards

1. Visa Logo
   Always appears on the front of the Card, usually on the right-hand side.
2. Account Number
   Usually 16 digits and can be embossed or flat printed.
3. Holographic feature
   Features either a single dove or series of repeated doves in flight.
4. Ultraviolet feature
   Appears as a “V” or dove under ultraviolet light.
5. CSC
   Always appears on the reverse of the Card either on the signature panel or to the side. This security feature should be used to confirm online and telephone payments.
6. Cardholder name
   May appear as a name, generic identifier e.g. airline passenger or may be left blank.
7. Optional Chip
   Works together with the Cardholder’s PIN or signature to create more secure payment. Not all Visa Cards have a chip but you can accept them as normal using the magnetic stripe.
8. Issuer Identification
   This area is available for each Card Issuer to brand their cards.
SECTION 2: Things You Need to Know Before You Accept Card Payments

Visa Electron

1. Visa Electron Logo
   Always appears on the Card, usually on the right-hand side.

2. Account Number
   Usually appears as a 16 digit and can be embossed or flat printed.

3. Holographic feature
   Features either a single dove or series of repeated doves in flight.

4. Ultraviolet feature
   Appears as a “V” of dove under ultraviolet light.

5. CSC
   The CSC always appears on the reverse of the Card either on the signature panel or to the side. This security feature should be used to confirm online and telephone payments.

6. Cardholder name
   May appear as a name, generic identifier e.g. airline passenger or may be left blank.

7. Optional Chip
   Works together with the Cardholder’s PIN or signature to create more secure payment. Not all Visa cards have a chip but you can accept them as normal using the magnetic stripe.

8. ELECTRONIC USE ONLY
   A legend denoting ELECTRONIC USE ONLY appears on the front or back of the Card.

9. Issuer Identification
   This area is available for each Card Issuer to brand their Cards.

Visa Prepaid

Visa issue prepaid cards. These are loaded with funds and often given as gifts. They are not always personalised with a specific Cardholder name, but you can still accept them as you would any other Visa Card.

Visa and Visa Electron Mini Cards

These are miniature Visa and Visa Electron Cards, which carry the logos in a reduced size, positioned in either the bottom or top right of the Card.

A Visa mini dove hologram will feature on the back or front of the Visa Mini Card. However, this is optional on Visa Electron Mini Cards.

Other features include:
→ Signature Panel
   A signature panel will appear on the back of the Card.
→ Magnetic Stripe
   The magnetic strip 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 onto the signature panel.

→ Cardholder Photograph and Signature
A photograph of the Cardholder may appear either on the front or the back of the Card.

MasterCard™
MasterCard Cards are produced in many different designs and each Card identifies the Card Issuer.

MasterCard Credit Card & Debit MasterCard
All MasterCard Cards have the following security features:

1. MasterCard Logo
The MasterCard symbol of two interlocking globes and the MasterCard hologram together, surrounded by a retaining line, on the front of the Card.

2. Chip
Most Cards will carry an embedded chip, which works together with the Cardholders PIN or signature to create more secure payment.

3. Expiry Date
Every MasterCard must have an expiry date. Some may also include an optional ‘Valid From’ date.

4. Cardholder name
May appear as a name, generic identifier e.g. airline passenger or may be left blank.

5. Embossed or printed account number
Embossed or flat printed, the account number can be up to 19 digits and the first digit is always the number 5.

6. Printed Bank Identification Number (BIN)
The four digit printed BIN number must appear below the account number and must match the first four digits of the embossed or printed account number. You must always check these numbers carefully to ensure they are the same.

7. Issuer Identification
This area is available for each Card Issuer to brand their Cards.

8. Magnetic stripe
The magnetic stripe holds information about the card and appears on the back of all Cards.

9. CSC
The Card Number or last 4 digits of the Card Number is printed on the signature strip on the back of the Card followed by the CSC (Card Security Code) which is a 3-digit number designed to provide extra security when conducting Card Not Present Transactions.
Maestro™

Maestro is a Debit Card brand owned by MasterCard and is issued in the UK and overseas.

Usually, Maestro Cards will carry the following details:

1. Maestro Logo
   The blue and red interlocking circles with the word “Maestro” printed across the centre in white.

2. Cardholder Number
   This can be between 12 and 19 digits long.

3. Cardholder Name

4. Expiry date

5. Signature Panel
   A signature panel will appear on the back of the Card.

6. Magnetic Stripe
   The magnetic strip will appear on the back of the Card. This may be printed with the word ‘Maestro’ in repeat pattern and may contain the last four digits of the Card Number, followed by the CSC.

Some may also contain the following:

→ Chip
→ Hologram
→ Cardholders title (for example, Mr, Mrs, Miss)
→ Start date
→ Card issue number
   This is the sequential number used to identify cards issued on the same account. It will be one or two digits only.

There are some differences in the way UK issued Maestro Cards and internationally issued Maestro Cards operate and it is very important that you follow this guide for all Maestro Cards you accept.

You must ensure that your staff are trained to accept Maestro Cards, and are familiar with these procedures.

For UK issued Maestro, transactions should be taken through your electronic Terminal and any amounts equal to or over your Maestro Floor Limit must be authorised. For internationally issued Maestro, all transactions must be authorised and your Terminal will recognise this. In the event of failed card read or swipe, please refer to the Terminal Fallback Procedures set out in Section 4.1.

If you accept Internet Card Transactions, you must be registered for MasterCard SecureCode, please refer to Section 3.3, before you can accept any Maestro or International Maestro Cards.

2.2 Commercial Cards

Commercial Cards bring specific benefits to business-to-business sales transactions. They look like any other Visa or MasterCard Card, although many have the description of the card’s function on the front of the Card, for example ‘Purchasing Card’.

There are three main types of Commercial Cards:

Business Card

→ Suitable for paying everything a small business needs for example stationery, office supplies, travel expenses etc.

→ Provides small businesses with a business payment method, an expense control mechanism and a cash management tool.

→ Available as charge and credit cards.

Corporate Card

→ Suitable for mid-sized to large companies for travel and entertainment expenses.

→ Provides management with the information to control expenditure and manage business expenses.
→ Enables companies to streamline the administration of expenses, saving time and money by reducing the cash handling and paper-based payments.

**Purchasing Card**

Purchasing Cards can be used to settle transactions in the usual way, however, they can also automate the paper invoice system and satisfy VAT reporting requirements.

→ Used by government departments, public sector bodies and large businesses.

→ Enables control and monitoring of expenditure and the provision of data and information to help improve cost management.

→ Allows reporting of reduced VAT rates.

→ Removes paper-based processes through electronic invoicing and provides a detailed breakdown of expenditure.

2.3 How to Guard Against Fraud

**Preventing and Detecting Fraudulent Card Not Present (CNP) Transactions**

→ Authorisation is not a guarantee of payment, it only confirms there are enough funds to pay for the goods and that the Card has not been blocked at the time of the transaction.

→ Fraudulent CNP Transactions are your liability as they are likely to be charged back to you.

→ Goods relating to a CNP Transaction should not be collected by the Cardholder. If the Cardholder wishes to collect the goods, then they must present the Card for payment at the time of collection. You should then cancel the CNP order and complete a Card Present Transaction.

→ Never dispatch goods to a third party, such as a friend, taxi driver, hotel or other temporary accommodation (except for goods such as flowers, as these are generally expected to be delivered to an address other than that of the Cardholder).

→ Be wary if the delivery/customer is overseas and products purchased are readily available in the customers’ local market.

→ 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.

**Ask yourself the following questions before the transaction.**

→ Why has this customer come to me?

→ Is the sale almost too easy; is the customer disinterested in price and details of the goods?

→ Are the goods of high value, ordered in bulk or easily re-saleable?

→ How does the sale compare with your average transaction, is the customer ordering multiple items, does the spending pattern fit with your usual customers?

→ Is this a new customer, does the caller match the Card, is the customer having problems remembering the address, or seem to be reading from notes, or is the customer being prompted by a third party?

→ Does the customer offer other Card Numbers if a transaction is declined?

→ Is the customer unwilling to provide a landline number?

→ What is the geographical location of the Card compared to the delivery address? Has the Card been issued overseas with the goods to go locally and vice versa? For example, if the billing address is an overseas address whilst the delivery address is in the UK.

→ Are you delivering multiple orders to the same address?
Assess your risk and perform extra checks to reduce the risks of fraud.

- Employ AVS/CSC checking (please refer to Section 3.2).
- Register and implement 3D Secure (please refer to Section 3.3).
- Implement third party fraud screening tools.
- Validate private telephone numbers through Directory Enquires and call customers back to confirm orders (not necessarily straight away).
- Check business customers against business directories or internet search engines.
- Validate private addresses against the Electoral Register, telephone directory or internet map searches.
- Avoid orders to overseas addresses unless you are confident that it is genuine. In the case of fraud, you will lose your goods and the shipping costs.
- Employ velocity checking; how often would you expect the same customer or the same card to be genuinely used over a specified period? Validate anything outside of these norms.

Preventing and Detecting Fraudulent Card Present Transactions

Please make sure that all staff accepting payment by Credit/Debit Cards on your behalf have read and understood the following guidelines in order to reduce the possibility of fraud.

Remember, these suggestions could help you in preventing fraudulent Card Transactions that could result in a Chargeback to you.

- If the appearance of the Card being presented or the behaviour of the person presenting the Card raises suspicion, you must immediately call the Authorisation Centre 0844 257 9400 and state “This is a Code 10 Authorisation”. Answer all of the operator’s questions and follow their instructions.
- Ask yourself; does the customer appear nervous/agitated/hurried?
- Are they making indiscriminate purchases? For example, not interested in the price of the item.
- The customer makes an order substantially greater than your usual sale e.g. your average Card Transaction is £40.00, but this Card Transaction is for £400.00.
- The customer purchases more than one of the same item (i.e. items that may be easily re-sold such as jewellery, video equipment, stereo equipment, computer games).
- The customer insists upon taking the goods immediately, for example, they are not interested in free delivery, alteration or if it is difficult to handle.
- The customer takes an unusual amount of time to sign and refers to the signature on the back of the Card.
- The customer takes the Card from a pocket instead of a wallet.
- The customer repeatedly returns to make additional orders in a short period of time causing an unusual sudden increase in the number and average sales Card Transactions value over a 1 to 3 day period.
- The customer tells you that he/she has been having problems with his/her Card for payment where multiple Card Transactions are subsequently declined but eventually an Authorisation is obtained for a lower amount. (Most genuine Cardholders know how much available credit they have.)
- Card Transactions are subsequently declined but eventually an Authorisation is obtained for a lower amount. (Most genuine Cardholders know how much available credit they have.)
- A fraudster may present more than 1 Card, often to find a Card that will be successfully authorised. If this happens, take particular care and also look out for Cards presented, issued by the same Card Issuer, where the Card Numbers are sequential or very similar. When in doubt, make a ‘Code 10’ Authorisation call to the Authorisation Centre.
- If you have an electronic Terminal and wish to reduce exposure to fraud you may request a reduction to your Terminal Floor Limit. Not only will this reduce fraud but it may also reduce Chargebacks due to invalid Cards. Please contact the Merchant Support Centre on 0845 964 5055† to arrange this reduction.
SECTION 2: Things You Need to Know Before You Accept Card Payments

Never accept an Authorisation Code from a customer. Authorisation must always be obtained via the correct procedures.

**Counterfeit Cards**
Most cases of counterfeit fraud involves ‘skimming’ or ‘cloning’, this is where the genuine data in the magnetic strip on one Card is electronically copied onto another Card without the legitimate Cardholder’s knowledge. This type of fraud can be identified by checking that the Card Number printed on the voucher is the same as that embossed on the front of the Card. If these numbers differ, call the Authorisation Centre immediately on 0844 257 9400 stating “This is a Code 10 Authorisation”.

The introduction of Chip Cards (Cards which contain a small micro chip) means that genuine Cards are less likely to fail at the Point of Sale, so the need to manually key enter Card details is reduced.

To help avoid receiving Chargebacks as a result of counterfeit fraud and disputed key entered Card Transactions, follow the guidelines provided in Section 3.1, Manual entry for Card Present Transactions.

**Delivery Warning Signals**
Here are some danger signs to look out for when arranging delivery of goods.

- Goods should not be released to third parties such as friends of the Cardholder, taxi drivers, chauffeurs, couriers or messengers. However, third party delivery of relatively low value goods such as flowers is appropriate.
- 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.
- Goods are to be delivered abroad.
- Don’t send goods to hotels or other temporary accommodation. Only send goods by registered post or a reputable courier and insist on a signed and dated delivery note.

**Instruct your Courier**
Make sure the goods are delivered to the specified address and not given to someone who ‘just happens to be waiting outside’. Instruct your courier to return with the goods if they are unable to effect delivery to the agreed person/address.

Do not deliver to an address, which is obviously vacant.

Obtain 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 0845 964 5055† for more details.
Always be particularly wary of:
- Demands for next day delivery.
- Alterations of delivery address at short notice.
- Phone calls on the day of delivery asking what time, exactly, the goods are due to be delivered.

**Card chip-read/swipe failure**
Please refer to Section 4 on Fallback Procedures.

**Returning wanted or recovered cards**
Please 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. If you are suspicious that the claimant is not the Cardholder, telephone the Authorisation Centre and state “This is a Code 10 Authorisation”. Only release the Card if you are satisfied that the claimant is the Cardholder.
Unclaimed Cards should be cut across the bottom left hand corner of the front of the Card and both parts attached to a letter. Please complete the form and send it to:
First Data Merchant Solutions Rewards Department,
PO Box 209,
Basildon,
Essex
SS14 9AA

A financial reward is not given in these circumstances.

**Reward scheme**

If you are worried about these or any other details, keep the Card and goods. Then telephone the Authorisation Centre immediately, stating “This is a Code 10 Authorisation”.

For further information, please see Section 4.1 Everyday procedures. A reward of £50 will normally be paid (at our discretion) to any Merchant who recovers a Card, when requested to do so by the Authorisation Centre.

**Other Important Fraud Considerations**

Remember – An Authorisation Code only indicates the availability of a Cardholder’s credit and that the Card has not been blocked at the time of the Card Transaction. It does not guarantee that the person using the Card is the rightful Cardholder.

Do not, under any circumstances, process Card Transactions for any business other than your own. Some fraudsters offer commission to process Card Transactions while they are awaiting their own Credit Card facilities. If you process Card Transactions on behalf of any other business/person, you will be liable for any Chargebacks, will be in breach of your Merchant Agreement and will put your own First Data Merchant Solutions service at risk.

Your Card Transactions must not involve any Card Issued in:
→ Your name or your account.
→ Or the partner in, or director or other officer of your business.
→ Or the spouse or any member of the immediate family or household of any such person detailed above.

Doing so will put your First Data Merchant Solutions service at risk and, in addition, First Data Merchant Solutions will have the right to process an entry to cancel the Card Transaction without notification.

### 2.4 Card scheme requirements

**Payment Card Industry Data Security Standard (PCI DSS)**

**What is PCI DSS?**

<table>
<thead>
<tr>
<th>Goals</th>
<th>PCI DSS Requirements – Validated by Self or Outside Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network</td>
<td>1. Install and maintain a firewall configuration to protect Cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of Cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Use and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to Cardholder data by business need-to-know</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to Cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>10. Track and monitor all access to network resources and Cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>12. Maintain a policy that addresses information security for all personnel</td>
</tr>
</tbody>
</table>
 zamanlı bi yazıyı okuyun.
SECTION 3: Accepting Card Transactions

3. Accepting Card Transactions

3.1 Card Present Transactions

Using your Point of Sale (POS) Terminal

Always follow the instructions shown in your Terminal User Guide supplied with your Terminal.

Although Chip and PIN Cards are the most common in the UK, you must continue to accept all types of MasterCard and Visa Cards.

Some customers may not have a Chip and PIN Card e.g. customers from overseas and some customers with disabilities.

You should not attempt to guess whether the customer’s Card is a Chip and PIN Card or requires a PIN or signature, simply process the card in the terminal and follow the prompts on the screen.

Manual entry for Card Present Transactions

A vast majority of your Card Transactions will be chip read or swiped through your POS Terminal. You will find that Chip and PIN Card will not usually fail, if you key enter or revert to the magnetic strip on a Chip and PIN Card, it is possible that the issuer will decline the transaction. Specifically face-to-face transactions taken on a Maestro Card must not be key entered. The issuer will decline the transaction. If the transaction is declined, follow the terminal prompts, which may direct you to speak to our Authorisation Centre. You should follow their instructions and only return the Card to the customer if you are not asked to retain it.

Non-Chip Cards (excluding Maestro Cards and Visa Electron Cards)

1. After 3 unsuccessful attempts to swipe the Card, your Terminal will indicate that it has not been possible to read the magnetic strip on the reverse of the Card.
2. You must manually key enter the Card details in accordance with your Terminal User Guide, ensuring they have been entered correctly.
3. Once you have key entered the Card Transaction details, ask the customer to sign the Terminal Sales Receipt in the normal manner.
4. If the Cardholder indicates that they are suffering recurring ‘card read’ problems it would be helpful to suggest that it may be wise to contact their Card Issuer to advise them of the problem. If you feel that there may be a problem with your Terminal, please contact your Terminal supplier helpline or the Merchant Support Centre.
5. In the unlikely event the Card Transaction is disputed it may be subject to Chargeback as the Card details have been key entered, key entering Card details into your terminal does increase the chances of Chargeback.

Terminal Fallback

With the introduction of Chip and PIN and Maestro, you need to be aware of the fallback procedure where the problem is with the Terminal or PIN Pad and not the card. This guide shows you the action you need to take.

A manual fallback Card Transaction must be completed in all events where your Card payment terminal is inoperable (with the exception of Maestro Cards and non-embossed Electronic Use Only for which an alternative payment method should be requested).
You should contact your Terminal supplier helpdesk immediately to report any faults. A representative will endeavour to resolve the problem remotely, or failing this, will arrange for a new electronic 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 2 to 4 working days.

Contactless Transactions

What is a contactless transaction?

Otherwise known as Visa PayWave and MasterCard PayPass, it is a contactless transaction process that uses radio waves to exchange data between a reader and an electronic tag attached to an object. This allows Cardholders to wave their Card in front of contactless payment terminals without the need to physically swipe or insert the Card into a POS device.

Accepting Contactless Card Payments

Sales - The value of any single transaction is limited to £10.
Refund – These are not permitted. All refunds must be carried out as a Chip and PIN Transaction.
Failed transactions – if you are unable to process a contactless transaction, revert to standard transaction acceptance, i.e. Chip and PIN.
Security – on occasion, you may be requested to process a contactless transaction as Chip and PIN. This is a security measure to ensure the genuine Cardholder is in possession of the Card.

### Authorisation and Code 10 calls

#### 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.

Authorisation must be obtained at the time of the transaction. If you have an electronic POS device, an Authorisation request should be automatically generated. You should not proceed with the Transaction when your request for Authorisation is declined. It is your responsibility to ensure that all Transactions are authorised.

#### Referrals

Sometimes you may be prompted by your Terminal to call for Authorisation. This is called a referral. A referral is when a Card Issuer requests that First Data Merchant Solutions 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 process. Generally, it will be necessary for the Cardholder to come to the telephone. You should follow the instructions given by the authorisation operator. At the end of the call, a decision will be provided to you.
SECTION 3: Accepting Card Transactions

For Authorisation, please telephone:
0844 257 9400
Lines open 24-hours a day, 7 days a week

Code 10 calls for Card Present

If you suspect something is wrong, or the Card checks you make show inconsistencies, then you must telephone the Authorisation Centre on 0844 257 9400, PRIOR to swiping the Card through the Terminal and state that "This is a Code 10 Authorisation". Then follow their instructions.

‘Code 10’ Authorisation applies in the following circumstances:

→ The Card Number embossed on the front of the Card is different from the one printed on the signature strip on the back of the Card
→ The Cardholder’s signature differs from that on the Card
→ The title on the Card does not match the customer
→ The signed name is not the same as that embossed on the front of the Card
→ The word ‘void’ is visible on the signature strip or there is any indication that the strip has been tampered with
→ There has been any attempt to disguise or amend the signature
→ The Card is unsigned
→ There is no ‘flying V’ or ‘offset MC’ on the Card being presented
→ The hologram is damaged or missing
→ The Card has been mutilated in any way
→ You have a reason to be suspicious about the sale, the Card or the customer
→ The amount of the Card Transaction is significantly higher than normal for your business
→ Your Terminal requests that you call the Authorisation Centre

Hold on to the Card and goods and telephone the Authorisation Centre immediately – you should not call the Police unless instructed to do so by the Authorisation Centre.

When you make a ‘Code 10’ Authorisation call, have the following details ready:

→ The Cardholder Number
→ The Card issue number (if applicable)
→ Your First Data Merchant Solutions number
→ The exact amount of the Card Transaction, in pounds and pence
→ The Card expiry date

Say to the Operator: "This is a Code 10 Authorisation"

This will alert the Authorisation Centre and you will be asked the relevant questions, most of which will require "Yes" or "No" answers (to avoid difficulty or embarrassment if the customer is waiting close by).

The operator may instruct you to call the Police or advise you that the Police have been notified. Police involvement is not always necessary – please do not contact the Police unless instructed to do so.

Reward: There is normally a £50 reward (at our discretion) to any First Data Merchant Solutions Merchant for Card recovered.

Purchase with Cashback

You must have received written notification from First Data Merchant Solutions that you are permitted to offer "Purchase with Cashback". Cashback may only be offered where the customer receives goods or services as well as cash.

Here are some simple tips for dispensing Cashback:

1. Not every customer is eligible to receive Cashback with their Card – it is a service on the Cards and it depends on whether the customer’s bank permits this service. Do not attempt to guess whether the customer’s bank permits this, simply process the Card through your Terminal and follow the prompts on the screen.
2. Only dispense Cashback when using an electronic terminal, not a manual imprint machine.
3. Only dispense Cashback to customers who make a purchase with their Card.
4. Only dispense up to the maximum Cashback amount confirmed in your written notification from First Data Merchant Solutions.

5. Key in the purchase and Cashback separately.

6. Follow the prompts on the screen, it will tell you whether the purchase with Cashback has been approved. Depending on your POS facilities, either you or your customer will handle the Card.

---

3.2 Card Not Present Transactions

**Card Not Present**

A Card Not Present Transaction is when a Card is not presented at the point of sale. Examples of Card Not Present Transactions include mail order/telephone order, internet and recurring payments.

**Card Not Present Transactions**

Provided you have received written notification from First Data Merchant Solutions, you may accept a Card Not Present Transaction from a Cardholder who wishes to pay using VISA, MasterCard and Maestro.

You must not accept International Maestro Cards for Card Not Present Transactions except where the transactions are taken through Secure E Commerce.

When accepting a Card Not Present Transaction, please take extra care to ensure it is the genuine Cardholder who placed the order. Record in writing, all details of the Card Not Present Transaction and if conducted by telephone the time and date of the conversation. You may be asked to produce this or the Cardholder’s authority for a Card Not Present Transaction if the Card Not Present Transaction is disputed at a later date. If feasible, you should obtain and keep a copy of the Cardholder’s signature on file authorising you to process the Card Not Present Transaction.

**Important**

Under no circumstances can goods paid by mail or telephone be handed over the counter to, or collected by, your customer.

If a Cardholder wishes to collect the goods, then he/she must attend your premises in person and produce his/her
SECTION 3: Accepting Card Transactions

Card. You should cancel the Card Not Present Transaction and perform a new Card Present Transaction. You must not release goods to a third party or anyone who suggests they have been sent by the Cardholder to collect the goods. For example, a taxi driver.

To process a Card Not Present Transaction, you must obtain the following information:

- Card Number
- Expiry date
- Card Security Code
- Cardholder’s full name and address
- Transaction amount
- Delivery address if different to the Cardholder’s address

You must obtain authorisation for the transaction. Please note: Authorisation from the Card Issuer is not a guarantee of payment.

There are increased risks of Chargeback for Card Not Present Transaction as the Cardholder and Card are not present. Please note: If you choose to deliver goods to an address other than the Cardholder’s address, you are taking additional risk.

Card Security Code (CSC)

All businesses that accept payment by Credit and Debit Cards must follow the procedures set out by the Card Schemes, First Data Merchant Solutions as your Acquirer and the Payment Card Industry Data Security Standard (PCI DSS). These standards exist to protect you and your customers from Card fraud.

All customer and payment card information must be handled in a secure manner. You must ensure you know how to treat payment Cards and data appropriately.

A key piece of information on any Credit or Debit Card is the CSC, also known as the Card Verification Value (CVV). The CSC is printed on the reverse of the Card within the signature strip, after the Card Number and is used as a fraud prevention tool.

For all MasterCard, Visa and Maestro Cards, the code is the 3 digit number that follows directly after the Card Number as indicated. For American Express Cards the CSC is a 4 digit number and appears above the embossed Card Number on the front of the Card, in the near future those 4 digits will be moved to the signature strip on the reverse of the Card.

Your Terminal is designed to ensure the CSC is not retained.

If a customer sends Card details by email, you must ensure the email is securely deleted. Card Numbers and the CSC are valuable data and you must never write them down. You must not request or accept photocopies of the front or back of the Card, for any reason.

How You Must Treat the Card Security Code

There are only two scenarios in which you will need to request the CSC:

1. During a Card Not Present Transaction
   For example, if you accepting payments over the telephone or via email for an advance booking prepayment or deposit.

2. The Card is present, however your Terminal cannot read the Card details In this scenario, you will need to follow the prompts on the Terminal, which may require input of the CSC.

Once the transaction has been authorised, you must not keep record of the CSC.

Taking a Reservation: the CSC is not required for reservations

The Card details you are required to collect to guarantee a reservation/booking:

- The Card Number (do not ask for the CSC)
- The expiry date
- The Cardholder’s name, as it appears on the Card
- The Cardholder’s billing address, telephone number and email address (if applicable)

Overbookings: alternative accommodation at your hotel’s expense

You must ensure all data from the Card used to make the original booking is securely deleted (please refer to
Section 8. Hotels, Lodging and Accommodation for further information).

Corporate and Purchasing Cards: the CSC is not required

The CSC is not required for payment authorisation on these Cards, even for Card Not Present Transactions.

No show transactions: the CSC is not required

If a guest fails to arrive and has not cancelled their reservation, you are entitled to charge for one night’s accommodation, plus applicable tax (please see Hotels section for further information). Once you have processed the transaction, send a copy of the receipt with “No Show” written on the signature panel, along with your terms and conditions to the Cardholder at their billing address. The CSC is not required.

Cancellation refunds: the CSC is not required.

A complete refund of a guest's deposit is required if a reservation is cancelled before the deadline specified in your bookings terms and conditions (please see Hotels section for further information).

Charges after check-out: the CSC is not required.

This is when a guest is billed for additional charges discovered after they have checked out, for example, room service or bar charges. Provided your guest signs your terms and conditions of booking, the CSC is not required when processing these extra charges.

Address Verification Service (AVS)

This service allows you to check the numerical part of the Cardholder’s postcode and statement address with the Card Issuer. AVS is available on all MasterCard, Visa, Maestro and American Express Cards issued in the UK. It has been delivered in the effort to reduce Card Not Present fraud. You will need a small amount of information from the Cardholder:

- Card Security Code (the last 3 digits on the signature strip of the card)
- The numbers in the Cardholder’s postcode
- Up to the first 5 numbers of the Cardholder’s address

You will need to ask the Cardholder for their address as it is recorded by their Card Issuer and input the relevant numbers shown in the examples detailed in the table 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</td>
<td>000 or 1234</td>
<td>171</td>
<td>55</td>
</tr>
<tr>
<td>Any Town</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any County</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SS17 1BL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flat 3</td>
<td>000 or 1234</td>
<td>57</td>
<td>321</td>
</tr>
<tr>
<td>21 North Street</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any Town</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any County</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LM5 7LT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Cottage</td>
<td>000 or 1234</td>
<td>123</td>
<td>Bypass*</td>
</tr>
<tr>
<td>East Lane</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any Town</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any County</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SS12 3BL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apt 62</td>
<td>000 or 1234</td>
<td>451</td>
<td>62219</td>
</tr>
<tr>
<td>2190 West Road</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any Town</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any County</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LM45 1LT</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Your Terminal will prompt you to enter the numeric digits in the three stages shown.

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

Do not store the Card Security Code after the transaction has been authorised.
**Electronic Transactions**

These extra security measures should not make any difference to the speed it takes to authorise a transaction electronically.

If you are using an electronic Terminal to process your Card Not Present Transactions, your Terminal will automatically call the First Data Merchant Solutions Authorisation Centre as normal.

The introduction of the electronic CSC/AVS Service is designed to eliminate the need for Card Not Present ‘code 10’ Authorisation calls in normal circumstances, however, if you are suspicious then you should undertake a ‘code 10’ Authorisation call to further verify the transaction.

**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. It is your decision whether or not you wish to progress a Card Not Present Transaction. Please remember that you remain responsible should a transaction be confirmed as invalid or fraudulent, even if the data matches and an Authorisation Code is issued.

The final decision on whether or not to accept a payment is still up to you, as CSC/AVS 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 CSC/AVS match but 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>This means that both the AVS and CSC match the Card Issuer’s records</td>
<td>As long as you have been issued with an Authorisation Code, and you are satisfied that the transaction is genuine, unless there are other suspicious circumstances that concern you, you are likely to want to go ahead with this transaction. Although, as with all Card Not Present Transactions, payment is not guaranteed and you bear the risk if the transaction is disputed at a later date.</td>
</tr>
<tr>
<td>Data Non Match / Data Not Matched</td>
<td>The CSC and one or both of the address details do not match the Card Issuer’s records</td>
<td>This is possibly a fraudulent transaction. It could also mean that the details have been noted incorrectly. We recommend you don’t proceed unless further checks are made to verify the Cardholder and the delivery address provided.</td>
</tr>
<tr>
<td>CSC Match Only</td>
<td>Only the CSC matches and either one or both of the address details do not match the Card Issuer’s records</td>
<td>The address must match the details recorded by the Card Issuer. It is possible that the transaction is fraudulent. It could also mean that the Cardholder has changed address and not informed their Card Issuer, or the Card Issuer does not support AVS. This could also simply mean that the details have been noted incorrectly and should be verified again with the Cardholder.</td>
</tr>
<tr>
<td>AVS Match Only</td>
<td>Both address and postcode match, or just the postcode in cases where the address has a house name rather than a number. However the CSC does not match.</td>
<td>This could be a fraudulent transaction. However, the Cardholder may have provided an incorrect CSC by mistake. It could also mean that the details have been noted incorrectly. You may wish to verify the CSC again before taking any further action. Beware of repeated attempts by the Cardholder to guess the CSC.</td>
</tr>
<tr>
<td>Not Checked</td>
<td>This means that neither CSC or AVS have been checked.</td>
<td>This may be because the Card Issuer does not support either service, or their system is down. In these circumstances you will have to make a decision based on the information you have. We recommend further checks are made before going ahead with the sale.</td>
</tr>
</tbody>
</table>
SECTION 3: Accepting Card Transactions

For more information on CSC and AVS please contact our Merchant Support Centre on 0845 964 5055†.

IMPORTANT – authorisation, with or without confirmation of AVS/CSC information does not guarantee payment. If fraud subsequently occurs the merchant is liable for the Chargeback.

Pre-Authorisation
This is only permitted in certain circumstances. Visa and MasterCard allow pre-authorisation for car rental, hotel, internet and mail/telephone order merchants only. More information about pre-authorisation for car rental and hotels can be found in Sections 7 and 8.

Rules for Card Not Present Transactions
For goods to be delivered by mail/telephone order or through an E Commerce Merchant should obtain authorisation on the day the Cardholder contacts them to place the order. When the goods or services are ready to be delivered, the transaction should be processed. The Authorisation is valid if the final transaction amount is within 15% of the authorised amount.

If shipping goods more than 7 days after the original Authorisation request, a second Authorisation should be obtained.

Recurring Transaction
If you and a Cardholder agree that more than one transaction is to be made on a regular basis for the cost of goods or services, then the transaction is a Recurring Transaction.

You must make an application to take Recurring Transactions with First Data Merchant Solutions, even if you have an existing Merchant Agreement.

To take Recurring Transactions, the following must be adhered to:
→ Use a dedicated Merchant Number exclusively for Recurring Transaction business. No other transactions should be processed on this Merchant Number
→ All Recurring Transactions must be flagged Card Not Present
→ 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)

Please note Recurring Transactions are not permitted on Maestro Cards.

The initial transaction in which the Cardholder provides their Card details for recurring payments must be undertaken on the standard Merchant Number for your business. All subsequent transactions must be submitted on a Recurring Transaction Merchant Number.

Where the Cardholder initially provides their Card details over the Internet, you must submit the first transaction as an Internet Card Transaction and all subsequent as Recurring Transactions.

You may use an existing E Commerce (Internet Card Transaction) Merchant Number for the initial transaction and you don’t need to have a specific E Commerce Merchant Number purely for the initial transaction of a recurring payment.

All subsequent transactions must be submitted on a Recurring Transaction Merchant Number.

You may use an existing Recurring Transaction Merchant Number for subsequent Recurring Transactions initiated over the internet and do not need to have a specific Recurring Transaction Merchant Number purely for subsequent transactions initiated over the Internet.

Written permission from the Cardholder is required to undertake Recurring Transactions. This can be submitted in writing or electronically to allow periodic billing to their account for recurring goods or services over a period of time (no more than one year can be between each transaction). The written request must at least specify:
→ The transaction amounts or unspecific amount
→ The frequency of recurring charges
→ The duration of time for which the Cardholder’s permission is granted.
SECTION 3: Accepting Card Transactions

Examples of business types where Recurring Transactions are appropriate are:

- Insurance
- Membership
- Subscriptions

You must ensure:

- The Cardholder understands the ongoing nature of the commitment they have undertaken
- The Cardholder will always know at least 14 days before the event how much is due to be debited from their account and when

To comply with the requirement you must comply with the following guidance on Advance Notice:

1. Where you are using a Recurring Transaction authority or acknowledgement which does not specify both the due date of any debit and the amount to be debited, you are required to give individual advance notice to your customers of:
   - The amount to be debited from their account
   - The date when the amount due will be debited from that account

2. Advance notice must be given in all cases when the amount and/or date of the debit are to change.

Please note when advising a Cardholder of the amount and date of their first payment, it is acceptable to advise them that no further advance notice will be given if the amount due to be debited changes solely because of the alteration in the application rate of any statutory levy, such as VAT or insurance premium tax.

3. Advance notice will not be required when a direct action by the Cardholder requires you to initiate a specific claim on their account. This action must provide sufficient information to determine the amount and date of the debit.

4. Where the amount due is to be debited infrequently, i.e. at intervals longer than one year, you are required to notify the Cardholder at least 14 days before the debit is due.

You must ensure that debits made comply with the terms of the authority given by the Cardholder and are timed to ensure that the debit appears on their account no later than 7 Business Days after the agreed date.

When received, you must ensure that instructions to cancel are actioned immediately to ensure that no more debits are made after receipt. You should note statutory notice, such as is published on the appointment of a liquidator or receiver, is deemed to be constructive advice of cancellation.

If First Data Merchant Solutions request a copy of the Recurring Transaction, you must respond to this request within 10 days of the request being received. Failure to supply a copy upon request may result in a debit being disallowed and charged back.

Please note such requests may be originated up to six years after the last debit is made.

**VAU and ABU**

Visa and MasterCard provide services that allow a merchant to verify Card details prior to a Recurring Transaction being presented.

Visa Account Updater (VAU) and MasterCard Account Billing Updater (ABU) maintain databases that consist of participating issuer card information. These databases enable merchants to validate that a recurring payment authorisation has not been cancelled and the Card Number and expiry date they hold for their customer are current.

An exchange of data files takes place between the merchant, First Data Merchant Solutions and the Card Schemes. Further information is available on request.

**Qualifying / Non Qualifying Transactions**

As part of your Merchant Agreement you may be assigned Qualifying and Non Qualifying Merchant Service Charge, which support Visa and MasterCard rules that require transactions to be submitted quickly and accurately to reduce the risk of fraud. If so, you will be categorised based on your method of Card Acceptance at the time of signing. This may subsequently be updated with our written agreement. These categories are explained below.

**Transactions taken exclusively in a face to face environment (tier 05)**

Qualifying Transactions are face to face chip Transactions which are submitted for processing within two Business Days of the Transaction.
SECTION 3: Accepting Card Transactions

A Non Qualifying Transaction rate may be applied when:
- your customer pays with a Visa Business Debit card
- a transaction is taken as CNP

Transactions taken in a face to face environment and/or Mail & Telephone Order (tier 15)
Qualifying Transactions are face to face Chip & Pin and mail/telephone transactions that capture the Card’s CSC number, which are submitted for processing within two Business Days of the transaction.

A Non Qualifying Transaction rate may be applied for mail/telephone transactions when:
- your customer pays with an EU or International MasterCard or Maestro Card
- your customer pays with an International Visa Card
- your customer pays with a Debit MasterCard Card
- a transaction does not capture the Card’s CSC number

Transactions taken in an E Commerce environment (tier 16)
Qualifying Transactions are 3D Secure enabled E Commerce transactions submitted for processing within two Business Days of the transaction.

A Non Qualifying transaction rate may be applied to:
- all mail/telephone transactions
- all ‘face to face’ transactions
- all Recurring Transactions
- Visa consumer charge Cards
- MasterCard World Signia and World Cards

3.3 Internet Card Transactions
All Internet Card 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 Chargeback any Internet Card Transactions irrespective of whether an Authorisation Code is obtained.

Applying to Take Internet Card Transactions
You must make an application to take Internet Card Transactions with First Data Merchant Solutions, even if you have an existing Merchant Agreement.

On approval a new First Data Merchant Solutions Merchant number will be issued, this is solely for the purpose of acceptance of Internet Card Transactions for the business described within the new application.

Website Requirements
Order page (basket)
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:
- Cardholders’ full name;
- Cardholders’ email address;
- Cardholders’ billing address and postcode;
- Delivery address.

Payment page (checkout)
First Data Merchant Solutions is able to accept and process, on your behalf, Internet Card Transactions made with the following Card types:
- Visa;
- MasterCard;
- Maestro;
- Electron;
SECTION 3: Accepting Card Transactions

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 details:

→ Transaction amount;
→ Card type box, (for those Card types detailed in your Merchant Agreement, e.g. Visa);
→ Customers’ Card Number;
→ Card expiry date;

**Verified by Visa and MasterCard SecureCode**

These are industry wide initiatives introduced to combat Internet fraud, commonly known as 3D Secure. Cardholders who register for this service 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 operate on your Website and interact with both the customer and their Card Issuer. The Cardholder signs up for the extra security features with their Card Issuer.

Note – MasterCard Secure Code and Verified by Visa must be present on your website in order to accept Internet Card Transactions by Visa, MasterCard and Maestro Cards.

→ When shopping online, the Cardholder selects their goods/services and proceeds to the payment page.
→ The Cardholder enters their Card number. If registered for Verified by Visa or MasterCard SecureCode, the Cardholder will see a pop-up screen from their Card issuer asking for their password.
→ The Card issuer verifies the password.
→ The Transaction is completed, having verified the identity of both the Merchant and Cardholder.

For further information on these services, contact the Merchant Support Centre on 0845 964 5055†.

**Payment Services Provider (PSP)**

To take Internet Card Transactions you will need to use a PSP. First Data Merchant Solutions require that you use a fully hosted solution by your chosen PSP. This means having your card payment application hosted on the PSP’s secure servers. If you choose the secure hosted option, the Payment Card Industry Data Security Standard (PCI DSS) validation requirements for E-Commerce merchants are greatly reduced.

PCI DSS is a set of requirements, endorsed by the Card Schemes, Visa, MasterCard and American Express, governing the safekeeping of account information and applies to all merchants that store, processes or transmits Cardholder data.

The PSP you choose must be PCI compliant and be accredited with First Data Merchant Solutions to submit Internet Card Transactions to us. Your chosen PSP will be able to advise you of relevant costs, set up times and how their systems integrate with your Website.

Details of PSPs currently submitting Internet Card Transactions to us can be provided on request.

Any fees charged by the PSP will be in addition to the Merchant Services Charge (MSC) on your Internet Merchant Number.

**Receipt Requirements**

You must provide a Cardholder receipt and it must contain at least the following information:

→ Concealed Cardholder Account Number; For Internet Card Transactions, the Cardholder account number, Card Security Code (CSC) and expiry date must not appear on the transaction receipt. This is a PCI DSS requirement to ensure that Card details are protected from compromise;
→ Unique Transaction Identifier; To assist in dispute resolution between the Cardholder and Merchant, 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.
SECTION 3: Accepting Card Transactions

You can choose to send a separate email message to the Cardholder containing this required information, or send a physical receipt in the mail or both. To minimise Cardholder enquiries, you are encouraged to send an online acknowledgement of the Internet Card Transaction. When this online acknowledgement is sent, you should include a statement encouraging the Cardholder to either print or save this document for their own records.

Website content
Set out below are details that should be included in the content of your Website.

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

You should ensure that your Website, its content 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, and where you process Personal Data on your Website, include a Privacy Policy that Cardholders are required to agree to before providing any personal data on your Website.

Merchant details
Full details about your company should be provided on your Website, these should include:

- The registered company or LLP name and address, registration number and VAT number (if applicable). If you are not a company or LLP you must indicate that you are a sole trader or a partnership and the address where the business is located;
- Details of any trade register or similar register available to the public in which you are registered and details of any professional body with which you are registered together with a reference to the applicable professional rules and means to access them. You should make sure you have determined what details are required to be given under relevant regulations;
- A correspondence and email address, as well as a customer services contact, i.e. telephone and fax numbers;
- The physical location of your business, (including your country of domicile);
- A statement detailing under which legal jurisdiction your business operates.

Products and pricing

- All products or services on offer should be clearly described/illustrated so that the Cardholder has a good idea of what is on offer;
- Any limits to product availability should be clearly stated. This includes all costs, such as taxes, including import duty, packaging and delivery charges;
- If appropriate and wherever possible, the Cardholder should be provided with the order details and the total cost of purchase, including any additional charges as noted above. The Cardholder should also be informed of the period for which the offer remains valid.

Placing an order

Where a Cardholder places an order through your Website you must (unless the recipient is a business and you have both opted out of these requirements):

- Provide details of the different technical steps to conclude the contract and whether the contract will be kept by you and accessible to the Cardholder;
- Acknowledge receipt of the order to the Cardholder without undue delay and by electronic means;
- Make available to the Cardholder appropriate, effective and accessible, technical means allowing him to identify and correct errors prior to placing the order;
- Provide information on any relevant codes of conduct to which you subscribe and how these can be consulted; and
- Make available to the Cardholder any applicable terms and conditions in a way that allows him to store and reproduce them.
SECTION 3: Accepting Card Transactions

Payments and refunds
- The Cardholder should be provided with clear information on all payment options and clear instructions on how to pay;
- The Cardholder should be informed of their cancellation rights and their rights to a refund, and/or replacements at the time of purchase/and the conditions for exercising the cancellation rights;
- A refund information page should also be provided with clear contact details;
- Receipts should be provided with the goods on delivery;
- The Cardholder should be provided with details of how and to whom a complaint can be made including an address.

Recurring Payments
Internet Merchants are able to accept an electronic record (such as email) from a Cardholder with permission enclosed for the Merchant to periodically charge the Cardholder for Recurring Transactions. This record can be retained for the duration of the services. A copy of the record must be provided to the Card Issuer/Card Acquirer upon request. The phrase "recurring transaction", details of the frequency of debits and the period for which debits are agreed, must be included on the receipt issued to the Cardholder.

If you are considering offering an online sign-up for Recurring Transactions, you must provide an easy online cancellation procedure to the Cardholder. Such procedures must be as simple and as accessible as those of the original sign-up process.

Delivery and guarantees
- Delivery dates/times should be clearly stated and agreed with the Cardholder. If it is not possible to deliver on the agreed date/time, another delivery should be arranged. If this is not possible, the Cardholder should be offered a refund;
- You should capture both billing address details and delivery address details, where these differ;
- In the event of non-delivery, it is the Merchant's responsibility to prove receipt of the goods by the Cardholder;
- Guarantee terms and details should be clearly stated. The Cardholder needs to be aware that this will in no way affect their statutory rights. The name and address of any insurer backing the guarantee should be provided.

Apart from deposits, full payment for goods and services must not be debited from a Cardholder's Account until the 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 Merchant Solutions for this before any deposits are taken.

3.4 Refund Process
1. If you wish to provide a Refund, the Refund Card Transaction must be completed using the same Card as that used for the original sale.
2. You should never make a Refund to a Card where the original sale was made by cash or cheque.
3. You should never make a Refund to a Card where there has been no sale transaction.
4. Failure to observe the procedures in this section could lead to your funds being withheld pending further investigation.
5. You must enter the Card into the Chip Card reader, PIN Entry Device or swipe it. If your Terminal is unable to read the card you must manually key enter the Card Number.
6. Where the original Transaction was PIN verified, you may need the Cardholder to enter their PIN in order to process the Refund. This will depend on the type of Terminal you use; please refer to your Terminal User Guide, otherwise you should sign the Terminal Sales Receipt, and make a note of the exchange and/or return of any items.
7. If Authorisation was obtained for the original Card Transaction, or your Terminal indicates that manual Authorisation is required, you must telephone the Authorisation Centre. Maestro Card Transactions will make an automated Refund Authorisation call based on the same parameters that were used for the sale, so a manual call is not required.
8. You may only perform a Refund agreed on the telephone or in correspondence if you are able to manually key enter Card Transactions. Please refer to the manual key entry procedures in your Terminal User Guide.
SECTION 3: Accepting Card Transactions

3.5 Global Choice™ / Dynamic Currency Conversion

Global Choice™ provides you with the ability to offer overseas Visa and MasterCard Cardholders the option to pay for goods or services in their own currency.

The price of goods and services will be shown to the Cardholder in UK Sterling and in their own currency, along with the exchange rate used. Exchange rates held in your terminal are updated automatically.

You must

→ Inform the Cardholder that Global Choice™ 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 Global Choice™ by default;

Receipt requirements

The Global Choice™ transaction receipt must show the following

→ 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;
→ Exchange rate used to determine the Cardholder currency transaction amount;
→ Total transaction amount charged by you in the transaction currency, followed by the words “Transaction Currency”; and
→ 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;
  - That the currency selected by the Cardholder is the transaction currency; and
  - Indicate that the Global Choice™ is conducted by you.

Separate written approval for Global Choice™ acceptance must be obtained from First Data Merchant Solutions.

3.6 Multi-Currency & Cross-Border Transaction Acceptance

Allows you to operate across several European countries and centralise your payment Card processing arrangements.

Separate written approval for Multi-Currency and Cross-Border acceptance must be obtained from First Data Merchant Solutions.

Permitted Merchant Outlet Location Countries

The merchant outlet location is either the physical premises where a transaction is completed or an electronic commerce or mail/telephone order transaction, where all the following occur:

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

Cross-Border acceptance is permitted within the following European countries:

- Andorra
- Austria
- Belgium
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Gibraltar
- Greece
- Greenland
- Hungary
- Ireland
- Israel
- Italy
- Latvia
SECTION 3: Accepting Card Transactions

- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Monaco
- The Netherlands
- Norway
- Poland
- Portugal
- San Marino
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- United Kingdom
- Vatican City

Available Funding and Settlement Currencies
Transactions can be accepted in any currency and settled to you in either Great British Pound (GBP), Euro or US Dollar (USD). You can also receive settlement in any of the currencies below, provided the transaction currency is the same.

- Great British Pound
- Euro
- US Dollars
- Australian Dollars
- Canadian Dollars
- Swiss Franc
- Japanese Yen
- Norwegian Krone
- Swedish Krona
- Denmark Krone
- Hong Kong Dollar
- New Zealand Dollar
- South African Rand

3.7 Bureau de Change
If you wish to operate a Bureau de Change, you will need to have another First Data Merchant Solutions merchant services account and First Data Merchant Solutions’ prior agreement to accept this type of Card Transaction.

You will be required to submit a new application for a Bureau de Change service provided by First Data Merchant Solutions, even if you have an existing First Data Merchant Solutions service.

Please contact our Merchant Support Centre on 0845 964 5055† to discuss your application. Lines are open 8am-9pm, Monday to Saturday.

When your Bureau de Change account is approved, you will be issued with a new Merchant Number. This number must be used for Bureau de Change sales only.

Security Check Procedures
In addition to Chip and PIN verification, you are required to follow specific security checks, which you must adhere to for every Bureau de Change transaction. Failure to complete this process may lead to a Chargeback for which you would be liable.

→ Review identification to verify the Cardholder’s identity.

→ If photographic identification is presented you must ensure the Cardholder resembles the person depicted in the photograph.

→ On the front of the receipt you retain, record the description of the identification i.e. driving licence, passport etc and include the serial number displayed on the identification. Additionally, if a photo is present also 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 4 digits must be recorded on the front of the transaction receipt to validate they have been checked.

Any fee to be charged and is included within the total transaction value must be disclosed to the customer (Cardholder) prior to completing the transaction.

If you wish to discuss obtaining a Bureau de Change service, please contact our Merchant Support Centre on 0845 964 5055†. Lines are open 8am-9pm, Monday to Saturday.

4. General Procedures and Banking

4.1 Everyday Procedures

Banking procedures
Please follow the end-to-end banking procedures detailed in your Terminal Operating Guide to ensure you receive payment for all transactions. It is essential that all transactions are submitted for payment within 2 working days of being accepted.

Please note that if a transaction is submitted after 2 working days, the Card Issuer may reject the transaction, resulting in it being charged back.

Fallback Paper Processing Procedures
If your terminal malfunctions or if you have a power or telephone network failure you may have to use the Fallback Procedures and complete transactions using a manual Sales Voucher. This process must be Sterling (£) transactions only unless you have made arrangements with First Data Merchant Solutions to accept different currencies.

The Sales Voucher
The Sales Voucher contains the following copies:

9. Merchant’s Copy: (top copy) a copy of the Card Transaction for your records. A copy of the Card Transaction must be produced to First Data Merchant Solutions should it be requested, and therefore must be kept for at least 24 months from the date of the Card Transaction or for a Recurring Transaction at least 24 months from the date of the last Card Transaction forming part of the Recurring Transaction. If you are unable to produce a copy of the Card Transaction within the requested timescale then the item may be subject to a Chargeback.

10. Processing Copy: (middle copy) a copy must be posted to First Data Merchant Solutions, PO Box 5653, Southend on Sea, Essex, SS2 6SU. This copy is electronically processed, therefore please do not fold, damage, pin or staple, and ensure the necessary details are clearly recorded.

11. Cardholder’s Copy: (bottom copy) a record of the Card Transaction to be given to the Cardholder.

Completing a Sales Voucher

1. Place the Sales Voucher on a firm surface

2. Using a ballpoint pen carefully and clearly write:
   - the Card Number across the top left hand of the Voucher;
   - the Card start date and expiry date directly beneath the Card Number;
   - the Cardholder’s name directly beneath the start date and expiry date;
   - give brief details of the goods/services purchased;
   - your 15 digit merchant number;
   - your business name;
   - your business address;
   - date of transaction;
   - amount of transaction

3. Do not mark copies with pencil or paper clips, as these can transfer through the carbons and obscure details.

4. Check that all details are clear especially on the processing copy of the Voucher set. If the detail is not clear, a Chargeback may occur. If you make a mistake, please complete a new Sales Voucher and destroy the old one.

5. Retain the Card and check the Card details carefully. Ask the Cardholder to sign the Voucher. When the Sales Voucher is signed, check that the signature matches that on the Card. Failure to do so may result in a Chargeback.
6. You must telephone the Authorisation Centre for an Authorisation Code for each Card Transaction where the Card details are handwritten. If the operator authorises the Card Transaction, write the code in the space provided on the Sales Voucher.

7. You may also wish to alert the Authorisation Centre by making a ‘Code 10’ Authorisation call if you suspect something is wrong (refer to the Authorisation and Code 10 Section), for example:
   - the Card appears unusual or has been tampered with;
   - the customer is acting suspiciously;
   - the amount of the Card Transaction is significantly above normal for your type of business;

8. When you are satisfied that everything is in order, hand the Cardholder the bottom copy of the Sales Voucher and their Card.

9. Once the Cardholder has signed the Sales Voucher and left, do not alter the copies in any way. If there are subsequent queries or disputes, the Cardholder’s copy will normally be treated as correct.

10. The Sales Voucher must always be completed in Pounds Sterling (£) unless you have made arrangements with First Data Merchant Solutions to accept different currencies.

**The Refund Voucher**

The Refund Voucher consists of 3 parts all printed in red; a top copy for your own records, a middle copy for banking, and a bottom copy for the Cardholder.

Refund Vouchers should be completed with all details in the same way as Sales Vouchers. You should then sign the completed Refund Voucher. Make a brief note on the Refund Voucher regarding the exchange and/or return of any items.

**Processing Refunds using the Fallback Procedures**

- If goods are returned by a Cardholder and exchanged for goods of the same price, no action is required.
- If you wish to provide a Refund, the Refund transaction must be completed using the same Card as that used for the original Card Transaction.
- Never return cash to a customer who originally paid using his/her Card or cheque.
- Never make a Refund using a Card where the original Card Transaction was made by another method of payment, for example cash or cheque.
- If the Card Transaction is to be refunded in full, you must prepare a Refund Voucher or Card Refund Data for that amount.
- Never accept money from a customer in connection with processing a Refund to the Cardholder’s Account.

**Completing a Refund Voucher**

If you wish to complete a refund using the Fallback Procedures, you must follow the steps below:

1. Check the Card.
2. Complete a Refund Voucher:
   - Place the Refund Voucher on a firm surface.
   - Using a ballpoint pen, carefully and clearly write:
     - the Card Number across the top left hand of the voucher;
     - the Card start date and expiry date directly beneath the Card Number;
     - the Cardholder’s name directly beneath the start date and expiry date;
     - give brief details of the goods/services purchased;
     - your 15 digit merchant number;
     - your business name;
     - your business address;
     - date of Refund;
     - amount of Refund;
     - date of original purchase.

Remember: Never make a Refund using a Card where the original Card Transaction was made by another method.
of payment, for example cash or cheque.

3. You must telephone the Authorisation Centre for an Authorisation Code for each refund transaction where the Card details are handwritten. If the operator Authorises the Refund transaction, write the code on the Refund Voucher.

4. You must sign the Refund Voucher.

5. Once you have completed all the above steps, return the Card to the Cardholder together with any original receipt and a signed copy of the Refund Voucher. If the cost of the replacement item differs from the returned item, a Refund for the original item should be completed on the same Card as the original Card Transaction. A new sale should be completed for the new Card Transaction and authorisation obtained.

If a Refund is agreed on the telephone or in correspondence with the Cardholder, you should complete the Refund Voucher in the manner above. You should also write CARD NOT PRESENT REFUND or CNP REFUND in the signature box.

**Preparing Vouchers for Submission**

When submitting your Vouchers for processing you must complete the Merchant Summary Voucher. The Merchant Summary Voucher is in 3 parts. The yellow top copy and white middle copy are the Merchant copies, and the bottom white copy is the copy to be sent for processing.

Using a ballpoint pen, carefully and clearly:

1. write your merchant number and business name on the top of the front of the Voucher;

2. list the amount of each Sales Voucher and Refund Voucher and the total in the spaces provided on the back of the Merchant Summary Voucher;

3. prepare a separate listing if there is insufficient space on the Merchant Summary Voucher;

4. please do not use staples, pins or paperclips;

5. do not submit more than 200 Vouchers on one Merchant Summary Voucher;

6. complete the front of the summary set (the Merchant Copy):
   - enter the total number of Sales Vouchers and total amount
   - enter the total number of Refund Vouchers and the total amount
   - enter the net total amount by deducting Refund Vouchers from Sales Vouchers;

7. detach the bottom copy and assemble the documents in the following order:
   - Merchant Summary Voucher (processing copy);
   - Separate listing, if used;
   - Sales Vouchers (in the same order as listing);
   - Refund Vouchers (in the same order as listing);

8. retain the 2 top Merchant copies of the Merchant Summary Voucher and keep with your copy of the Sales Vouchers;

If you have insufficient Sales Vouchers against which to offset the Refund Voucher(s) please follow the instructions below:

Complete a Merchant Summary Voucher in the normal manner and enter the details of the Refund(s). The value of the Refund(s) should be enclosed by brackets, preceded by a minus sign, to clearly indicate that the total is a negative value. The value of the Refunds will subsequently be debited to your bank account.

**Submitting Vouchers**

All Vouchers must be posted to First Data Merchant Solutions, PO Box 5653, Southend on Sea, Essex, SS2 6SU and must be received by us no later than 3 Business Days from the transaction date.

It is important that you post the Vouchers within the timescales given. If you do not, 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.

You must retain copies of all Merchant Summary Vouchers, Sales and Refund Vouchers for at least 24 months from the date of the Card Transaction or for a Recurring Transaction at least 24 months from the date of the last Card Transaction forming part of the Recurring Transaction. This will assist you in checking your Merchant Statement.
SECTION 4: General Procedures and Banking

and resolving any possible Chargebacks. If you are unable to produce a copy of the Card Transaction, you may be subject to a Chargeback. It is also essential that copies are retained in case any Merchant Summary Vouchers or Sales Vouchers are lost in the post.

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 0845 964 5055†.

4.2 Exceptional Procedures

Can I pass charges to my customer?

In the United Kingdom, if you accept Cards as defined by the Credit Cards (Price Discrimination) Order 1990 you may impose a surcharge on Transactions using a Credit Card within the United Kingdom.

If you indicate a price to a Cardholder, which is not a price applicable to all methods of payment accepted by you, 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.

Surcharging is not permitted on Debit and Prepaid cards (please refer to Section 1).

You must make it clear to your customers and ensure they are informed of any surcharges before the initiation of the transaction.

- For all payments, you must ensure that your advertising makes clear that any prices stated are for payments other than by Card
- 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 your surcharges at each public entrance to your premises and at each Point of Sale. You must also inform the Cardholder of the difference in price for the Card Transaction (either as an amount or a percentage) when they present the Card
- For Card Not Present payments made by mail, telephone or online, you must display a statement explaining the charges in your catalogue, advertisements and the order form.

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.

Minimum Charging

You must not set a minimum transaction limit on Credit and Debit Card Transactions if your customer has a valid and properly presented Card.

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.

It is important for you to understand when you can and cannot split a transaction.

1. 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. To prevent future disputes, ensure each Cardholder agrees to the amount they will pay and process separate transactions for each Card. Each transaction must be verified by the Cardholders PIN or signature, as prompted by the terminal. Please provide each Cardholder with a copy of the transaction receipt applicable to the agreed amount (which may or may not include gratuity) by the Cardholder.

2. If one Cardholder requests you to split a transaction amount between several Cards (perhaps issued by different Card Issuers) you may proceed as follows:
   - Only conduct the transaction if you are not suspicious of the transaction or the person presenting the Card
   - Ensure all Cards presented are issued with the same Cardholder name
   - Follow the normal Card acceptance procedures as details in Section 3.

This type of request may occur when accepting a large value transaction where the Cardholder may not have sufficient funds on one Card. First Data Merchant Solutions recommend you only split a transaction over more
than one Card when:
- It is a Card Present Transaction.
- You ensure each Card presented is either issued by a different bank or is a different Card type from the same bank. It is unlikely that the Cardholder would have more than one Card issued by the same bank and the same Card type
- You process each transaction by either chip-read or magnetic strip (as per Terminal prompts)
- Each transaction is verified by either Chip and PIN or signature (as requested by the Terminal)
- Each transaction is authorised
- The Cardholder agreed to the amount charged to each Card and is given a receipt for each transaction, which shows the amount charged to each Card.

3. You must not split transaction amounts for the same Cardholder into smaller amounts. For example, if Authorisation is declined on a transaction, do not split it into smaller amounts in an attempt to gain Authorisation. If you attempt to split a sale, any transaction may be charged back. First Data Merchant Solutions will not be able to defend you from such Chargebacks.

**Alteration of Amounts**

- You must not alter the transaction amount without the Cardholder’s consent.
- If you have a gratuity facility on your terminal, you must ensure the Cardholder has agreed for any gratuity to be added to the bill.
5. Why Chargebacks Occur

A Chargeback is an unpaid Card Transaction returned to us by the Card Issuer. The following section describes the procedures which you should follow together with suggestions which 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. Such requests can be received up to 180 days after the Card Transaction has been debited to the Cardholder’s Account and in some circumstances, beyond 180 days.

One of the main reasons a Cardholder disputes a transaction is because they do not recognise the description on their Card statement, as it may not match the name of your business.

It is a Visa and MasterCard 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; for example The Mail Order Shop 01234 567890. This provides the Cardholder with the ability to verify the transaction with you, rather than disputing with the Card issuer.

The same applies to Internet Card Transactions; the transaction description should include reference to your website address and a contact telephone number or email address.

You can change the description that appears on the Cardholder statements by contacting our Merchant Support Centre on 0845 964 5055†.

**Chargeback Reversal Procedure**

When a Chargeback is received from a Card Issuer we will normally debit your Merchant Account and advise you accordingly, with details of the Card Transaction together with the information/documentation required from you. We will also tell you the latest date by which you must reply with the information/documentation required. If the information provided is:

- sufficient to warrant a reversal of the Chargeback; and
- within the applicable timeframe;

We will defend (reverse) the Chargeback if possible but reversal is contingent upon acceptance by the Card Issuer under Visa/MasterCard guidelines. A reversal is not a guarantee that the Chargeback has been resolved in your favour. If the Chargeback is 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 to defend a Chargeback. However, due to the short timeframes and the 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, investigate and send in the appropriate documentation within the required timeframe
- 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.

**Common Causes of Chargebacks**

The most common causes for Chargebacks are:

- A fraudulent mail, telephone or Internet Card Transaction. Please refer to Section 2.3 for further information
- You did 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)
- The sale amount exceeded your Floor Limit and authorisation was not sought, for whatever reason
- The signature on the transaction receipt does not match what is on the Card
- A transaction was taken on a Card that should only be used in a ATM (Automated Teller Machine)
- If two or more Card Transactions were taken for one sale over the Floor Limit (split sale) and authorisation was not received
If the goods or services provided were not as described, defective or not received
A transaction was completed on behalf of a third party who could not process the transaction themselves. This is laundering and is in breach of your Merchant Agreement

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 from the Card Issuer, 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 from First Data Merchant Solutions 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. For Recurring Transactions, this increases to at least 24 months from the date of the last Card Transaction forming part of the Recurring Transaction.

If First Data Merchant Solutions does not receive a clear legible copy of the Sales Receipt within 14 calendar days of the initial request you may be subject to a Chargeback. The potential liability remains with you if the item is not supplied in time and you may become liable for Chargeback simply by failing to meet the payment scheme timeframe. Chargebacks for 'non-receipt of requested item' cannot be reversed unless the requested documentation is provided within 14 calendar days of the initial request.

To Help Reduce the Risk of Chargebacks
To help protect your business against fraud, First Data Merchant Solutions recommend that you use a Chip and PIN-enabled Terminal. Chip and PIN terminals help establish that a Card is genuine and the person using the Card is the owner. The chip makes it difficult for a fraudster to counterfeit or copy the Card, while the PIN makes it harder for a criminal to use a lost or stolen Card. Because the Cardholder authorises a transaction by keying in a four-digit PIN known only by them, the risk from forgery is greatly reduced.

Ensure all Card Transactions are processed correctly according to the Card type.
Only accept Cards you have an agreement to process.
Unless you are aware of the possible risks, do not accept mail, telephone or Internet Card Transactions. If you see an increase in these types of transactions, please contact us to ensure you have the correct Merchant Agreement in place.
Retain copies of all transaction records. You may be asked to provide evidence of a transaction in order to resolve a dispute. Failure to do so may result in a Chargeback. You must keep all receipts for a minimum of 18 months, in the case of a recurring transaction this increases to 24 months.
To avoid disputes, which could lead to Chargebacks, display a limited returns policy on your receipts and at the point of sale.
Remember to follow your instincts. If something about a Card, the customer or the transaction itself does not seem genuine, make a Code 10 call to our Authorisation Centre. Please remember 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.

Except if the debt is considered uncollectible, for example if the payment is to a collection agency or in an attempt to recover funds for a dishonoured cheque, you may accept a Card to collect or refinance an existing debt.
SECTION 6: Payment of Debt

6. Payment of Debt

Mortgage and Loan Payments
You may accept Visa Debit and Visa Electron Cards for the payment of mortgages and loans. However, during the transaction you must:

→ Obtain Authorisation
→ Complete the transaction as a purchase
→ Write the type of payment made on the receipt, i.e. "Loan" or "Mortgage"
→ On the signature line of the receipt, write "Instalment Transaction".

You must not add any surcharges to the transaction, unless local law expressly requires that a Merchant be permitted to impose a surcharge. Any surcharge amount, if allowed, must be included in the Transaction Amount and not collected separately.
7. Vehicle Rental Reservation Service

If you are a Vehicle Rental Company or a third-party booking agent that accepts Cards to guarantee rental reservations, First Data Merchant Solutions have created this best practice guide to detail the correct procedures to deal with Chargebacks.

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.

**Telephone Reservations**

As telephone reservations are Card Not Present Transactions, you should take as many details as possible to verify the authenticity of the Cardholder, for example:

- The name of the caller
- Their telephone number (NOT a mobile number)
- The name of the person(s) requiring the vehicle
- The expected collection date and time
- The number of days they expect to hire the vehicle
- The Card Number of the Card to be used
- The Card expiry date
- The Cardholder’s name
- The Cardholder’s billing address
- The Card Security Code (the last 3 digits on the signature stripe on the back of the Card or the last 3 digits in the box adjacent to the signature panel).

You should discuss and agree the hire rate and obtain the caller’s consent to your cancellation policy. This must be clearly explained to the customer. Once the order has been confirmed, please send the Cardholder the following in writing:

- Your terms and conditions and cancellation policy
- Reserved vehicle rental rate
- Currency of the transaction
- Name and address of the location the vehicle is to be collected from

The reservation confirmation to the Cardholder can be by mail, fax or email.

You must also inform the Cardholder that a No Show Transaction up to the value of one day’s rental at the reserved vehicle rental rate will be billed to the Cardholder if the Cardholder has neither:

- Collected the vehicle within 24 hours of the collection time, or
- Properly cancelled the reservation in accordance with the communicated cancellation policy

If you wish to bill a No Show Transaction, you must confirm, in writing, as part of the reservation confirmation, the value and currency of the fee that will be billed to the Cardholder.

**Fax or Mail reservations**

Fax and mail reservations should contain the same information as required for telephone reservations, however without the Card Security Code. Within the reservation, the Cardholder should also confirm they accept your terms and conditions.

You should call the Cardholder to confirm the reservation and provide confirmation in writing, together with a copy of your terms and conditions and cancellation policy.

**Internet Reservations**

When taking reservations on the Internet, we advise that you use the same procedures and precautions as those taken by telephone. This will also include that the Cardholder confirms their acceptance of your terms and conditions; this can be via a tick box.

First Data Merchant Solutions requires that your website uses 3D Secure. Please see Section 3 for further details.
SECTION 7: Vehicle Rental Reservation Service

Reservation Confirmation
When a customer uses your vehicle rental reservation service, you must supply the Cardholder with a confirmation code and advise the Cardholder to retain it in case of a dispute. You must also provide a written confirmation containing the following information:

- Cardholder name,
- Cardholder Account Number (truncated to only display four digits)
- Card expiration date
- Confirmation code
- The address the vehicle is to be collected from
- Hours of operation of the collection and return outlet
- Cancellation policy and procedures

You must ensure that the Cardholder is advised at the time of making the reservation that a confirmation receipt is available on return of the rented vehicle. This confirmation receipt confirms the mutually agreed condition of the rented vehicle upon return.

Your 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 may not charge any cancellation fee to the Card used for the vehicle reservation. If you do, First Data Merchant Solutions will be unable to defend you from any subsequent Chargeback.

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 6pm 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 5 business working days.

No Show
If the Cardholder does not turn up, having failed to cancel their vehicle hire, your terms and conditions may entitle you to charge the customer. However, you may not charge any cancellation fee to the Card used for the vehicle reservation. If you do, First Data Merchant Solutions will be unable to defend you from any subsequent Chargeback.

Vehicle Collection
When your customer comes to collect their hire vehicle ask to see their Card and ask them to read your terms and conditions and sign the rental agreement. Carry out the visual check to ensure the Card is genuine, (see Section 2 for further details).

In case there are any additional or delayed charges, do not ask the Cardholder to sign the Transaction Sales Receipt. The Cardholder must agree to be charged additional or delayed charges if they occur.

If possible, take payment by processing a Card Present Transaction (please see Section3, Accepting Card Transactions). If payment has already been obtained, ensure an imprint of the Card is taken on the vehicle rental agreement as proof that the Cardholder has consented to the Card payment.

Estimated Authorisation
An Estimated Authorisation allows you to estimate the final transaction value, obtain Authorisation and reserve payment while the vehicle is on hire. The estimate should be based on:

- The Cardholder’s intended rental period
- The rental rate and applicable tax
- Mileage rates

The estimated authorisation cannot include potential vehicle damage.

You cannot estimate authorisation with Maestro Cards.
As Estimated Authorisation is only valid for the length of the vehicle rental, for any extended rental periods, we recommend that you close the customers account after 14 days and bill them fortnightly.

At the end of the vehicle hire agreement, if the bill is within 15% of the estimated authorisation amount, you can use the code provided. However, you will need to gain a final Authorisation Code if:

- The final transaction amount is above your floor limit and you have not obtained a previous Authorisation
- There is more than 15% difference between the final bill and the Pre-Authorisation amount
- The Cardholder is paying by Visa Electron and the final bill is more than the sum of all the Estimated Authorisation you have previously gained for the vehicle hire period.

**Pre-Authorisation**

Pre-authorisation are those Card Transactions for which you can seek authorisation prior to the debiting of the Cardholder Account. It allows you to estimate the final transaction amount, gain Authorisation and reserve the funds before the hired vehicle is returned. This is, however, not supported for Maestro Cards. For Maestro Cards, we recommend full payment for the expected value when the vehicle is collected. If the Cardholder decides to reduce the length of hire, you can provide a Refund.

Authorisation will be valid for the length of the hire term. If the Cardholder decides to extend the hire period, First Data Merchant Solutions recommend that you do not allow your customers to hire a vehicle for more than 2 weeks without settling their bill. You should ask customers wishing to extend their hire to more than 2 weeks to pay the current total due, preferably by the Cardholder in person, and bill every 2 weeks.

At the end of the hire agreement, if the final bill is 15% more than pre-authorised amount, you must get a further pre-authorised code for the remaining rental period.

**Delayed Charges**

For you to process a delayed charge, for example 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.

To support the delayed charges, you must supply the customer with any additional documentation. For example, for a traffic violation:

- A copy of the rental agreement
- Document violation
- The licence number of the rented vehicle
- The law violated and, if applicable, a copy of the accident report
- Notice of the amount charged

Upon return of the vehicle, you must provide the Cardholder with a written confirmation of all of the following:

- The visible damage status of the rented vehicle upon return. If there is no visible damage, this must be clearly stated on the written confirmation and you must not process a delayed or amended charge transaction for any visible damage to the rented vehicle.
- The fuel status of the rented vehicle upon return. If there are no extra fuel charges, this must be clearly stated on the written confirmation and you must not process a delayed or amended charge transaction for extra fuel.
- The date and time of the return. If there are no extra rental charges as a result of extended time, this must be clearly stated on the written confirmation and you must not process a delayed or amended charge transaction for the extra day’s rental.

**Accident or Collision**

In an event of an accident or collision, you may charge Visa Cardholders for the damages to the vehicle. You must provide a written confirmation containing the details of the damage, the cost of the damage and the currency in which the cost of the damage will be charged to the Cardholder within 10 Business Days of the return date of the rented vehicle.

For delayed and amended charges relating to damages, where you have written to the Cardholder, the
SECTION 7: Vehicle Rental Reservation Service

Cardholder may, at no cost to the Car Rental Company, provide written confirmation of an alternative estimate for the cost of the damage. This must be within 10 Business Days of receipt of original written confirmation detailing the cost of the damage from you.

You and the Cardholder may come to an agreement on the cost of the damage before processing the transaction. If an agreement is not reached between you and the Cardholder for the cost of the damage, and if you process the delayed charges, the Cardholder retains the right to dispute the transaction.

To apply additional charges to a MasterCard, you must obtain a separate Cardholder signed authority by processing a Card Present Transaction. If the charge is disputed at a later date, this will be required as proof that the Cardholder authorised the additional charge.

Accepting Split Sales

There may be occasions when a customer requests a payment to be split between Cards, cash or cheques in order to share the costs. Although this is acceptable, there is a high number of Chargebacks as a result of them. You must always obtain Authorisation and always inform the Authorisation operator at the start of the call that the transaction is part of a split payment. You must only process one transaction per Card.

Please note Authorisation from the Card Issuer is not a guarantee of payment.

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 to the same Card as 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.

Extended Hire

First Data Merchant Solutions recommend that you do not allow your customers to hire a vehicle for more than 2 weeks without settling their bill. You should ask customers wishing to extend their hire to more than 2 weeks to pay the current total due, preferably by the Cardholder in person.

If the current bill is 15% more than the pre-authorised amount, you must get a further pre-authorised code for the remaining rental period.

Disputed Transactions

If at a later date, a Transaction is disputed, it is vital to show that the Card was present and authorised.

Common reasons for a disputed transaction include:

→ Vehicle reservations made using a Card obtained by a fraudster who never arrives to collect the vehicle. In this instance, it is likely that the fraudster is only using your reservation system to check that the Card they are using is valid with funds available. Therefore, it is likely that the Cardholder will only become aware of this when they receive their statement with your No Show charge included.

→ Not replying to Card Issuer requests for information. The Card Issuer is entitled under Card Scheme Rules to request details of any Transaction. This may include copies of the final transaction, showing that the Card was present and authorised by the Cardholder. Please ensure that you reply to Card issuer requests within 14 days. Failure to do so may result in a Chargeback.
8. Hotels, Lodging and Accommodation

First Data Merchant Solutions have created this best practice guide to detail the correct procedures to take when accepting Cards within the hotel industry. Failure to follow this guide may result in unnecessary Cardholder queries and complaints, and possible Chargebacks.

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.

Advance Reservations

Wherever possible, the person requiring accommodation or lodging should be asked to make the reservation themselves. However, for practical reasons, you may need to accept reservations from third parties, for example secretaries acting on behalf of their bosses.

Telephone Reservations

As telephone reservations are Card Not Present Transactions, you should take as many details as possible to verify the authenticity of the Cardholder, for example:

→ The name of the caller
→ Their direct dial telephone number (NOT a mobile telephone number)
→ The name of the person(s) requiring the accommodation/lodging (if not the caller)
→ Their expected arrival date and time
→ The number of nights they are expected to stay
→ The Card Number of the card to be used for the charges
→ The Card expiry date
→ The Cardholder’s name
→ The Cardholder’s billing address
→ The Card Security Code (the last three digits on the signature strip on the back of the Card or the 3 digits in the box adjacent to the signature panel).

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 the room rate and obtain the caller’s consent to your cancellation policy. This must be clearly explained to the customer. Once the reservation has been confirmed, please inform the Cardholder of the following:

→ The room rate (including tax)
→ The hotel’s address
→ The Cardholder’s name as it appears on the Card
→ The confirmation code for the guaranteed reservation (advise them to keep this for future reference)

Fax or Mail Reservations

Fax and mail reservations should contain the same information as required for telephone reservations, however without the Card Security Code. Within the reservation, the Cardholder should also confirm the acceptance policy.

You should call the Cardholder to confirm the reservation and also provide confirmation in writing, together with a copy of your terms and conditions and cancellation policy.

Internet Reservations

When taking reservations on the Internet, we advise that you use the same procedures and precautions as those taken by telephone. This will also include that the Cardholder confirms their acceptance of your terms and conditions; this can be via a tick box.
First Data Merchant Solutions requires that your website uses 3D Secure. Please see Section 3 for further details.

**Advanced Deposits**

Please note if you take advanced deposits for a room reservation, under the Visa and MasterCard rules, 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:

- The room rate (including tax)
- The 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 advance deposit
- Provide your address and telephone number
- The confirmation code of the reservation (advise the Cardholder to keep this for future reference)

Maestro cards are acceptable only when the Cardholder is present. All Maestro Card deposits must be processed electronically using the magnetic stripe or embedded chip.

**Cancellation Policy**

Please note that whilst you may have a cancellation policy within your terms and conditions, you must ensure this is clearly understood by the Cardholder when the room reservation is made. You must ask if they accept the policy and to confirm this. All cancellation deadlines must be no earlier than 72 hours before the guest is expected.

Should the Cardholder cancel in accordance with your cancellation policy, you should:

- Provide the Cardholder with a cancellation code, advising them to keep a record for future reference.
- Write “cancelled” on the reservation form and record the cancellation code
- Provide a written cancellation note, including the following information:
  - The Card number (this must be truncated so that only the last four digits are shown)
  - The Card expiry date
  - The Cardholder’s name as it appears on the card
  - The cancellation code

**Guest Arrivals/Check-In**

When your guests arrive, request to see the Card that the booking was made with 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.

**No Show**

If a Cardholder fails to cancel their room reservation, in accordance with your cancellation policy, you are entitled to charge for one night’s accommodation, plus applicable tax. For this, you can use the Card given at reservation.

Once you have processed the transaction, send a copy of the receipt with “No Show” written on the signature panel, along with your terms and conditions to the Cardholder at their billing address.

If however, the Cardholder later claims that they did not make the room reservation then a Chargeback may still occur.

Please note you may offer to reserve accommodation for a customer using a Maestro Card, however please be aware that you cannot debit the Card for one night’s stay if they do not arrive.
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. However, it is not supported for Maestro Cards. We recommend that you obtain full payment upon check-in for the expected number of nights stay. If the Cardholder decides to check out early, you can provide a refund.

The procedure for seeking Authorisation of estimates allows you to estimate the final transaction amount and receive the protection of an Authorisation before the guest checks out.

The Cardholder’s total charges can be estimated based on:
→ The expected length of stay
→ The room rate (including tax)
→ The estimated miscellaneous charges

At the time of Pre-Authorisation, the Cardholder will be required to input their PIN number to confirm they are the genuine Cardholder. Please advise the Cardholder how much you have Pre-Authorised, as this will reduce the amount of funds they have available on their account. You should reassure the Cardholder that this PIN is being used only to verify that the genuine Cardholder is present and that their Card is not being debited at this time. The Authorisation of estimates helps protect you from fraudulent Card use and confirms if the Cardholder’s account is valid and has sufficient funds available. 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.

Departures/Check-Out

When the Cardholder wishes to check out, calculate the final bill amount and compare this with the total amount of authorised estimates.

If the final bill is within 15% of the Pre-Authorised amount, there is no need for further authorisation, you can process the transaction by using the code given at Pre-Authorisation.

However, if the final bill is more than 15% above the Pre-Authorised amount, you must obtain another Authorisation Code for the difference.

Express /Priority Check-Out

If you decide to offer your guest an express/priority check-out service (Card no longer present), please be aware that we may not be able to defend you from a Chargeback if a Cardholder later denies any transactions.

If the Cardholder requests priority check-out, at check-in you must:
→ Record the Card Number, expiration date and Cardholder Name on the sales draft
→ Inform the Cardholder of your policy regarding any charges discovered after check-out
→ Give the Cardholder a priority check-out agreement to complete. When the Cardholder returns the agreement, ensure that:
  - It is signed
  - It includes the mailing address
  - The Card Number on the check-out agreement matches the Card Number on the Authorisation of the estimate.

Upon check-out, you must complete the sales draft by entering the total charges incurred during the Cardholder’s stay, including restaurant, telephone and miscellaneous charges. Compare the final bill amount with the total amount of authorised estimates.

If the final bill is within 15% of the Pre-Authorised amount, there is no need for further Authorisation, you can process the transaction by using the code given at Pre-Authorisation.

However, if the final bill is more than 15% above the Pre-Authorised amount, you must obtain another Authorisation code for the difference.

Extended Stays

First Data Merchant Solutions strongly recommend that you do not allow stays of more than two weeks without asking your guests to settle their bill.

Those requiring longer stays should be asked to pay the current total due. You can ask for their Card, or you can
SECTION 8: Hotels, Lodging and Accommodation

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.

If the bill is more than 15% above the Pre-Authorised amount, you must obtain another Authorisation code for the remainder of the stay.

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

Disputed Transactions
If a transaction is later disputed, it is important for you to show that the Card was present and authorised (where required).

The most common reasons for a disputed transaction are:
1. Reservations made using a Card obtained by a fraudster who never arrives at the hotel.
   In this instance, it is likely that the fraudster is only using your reservation system to check that the Card they are using is valid with funds available. It is therefore likely that the Cardholder will only become aware of this when they receive their statement with your “No Show” charge included.
2. Not replying to requests for information.
   Under Card Scheme rules, the Card Issuer is entitled to request details of any transaction. This may include copies of the final transaction, showing that the Card was present and authorised by the Cardholder. Please ensure that you reply to Card Issuer requests within 14 days. Failure to do so may result in a Chargeback.

Requests for Information and Notification of Chargebacks
If First Data Merchant Solutions advise that a Cardholder is disputing a charge, always ensure you supply the correct information to help us defend the dispute.

If the dispute is over an express/priority check-out where no signature was obtained, please send:

→ a copy of the transaction receipt captured at check-in, proving the Card was present and pre-authorisation was carried out
→ a copy of your registration showing the Cardholder’s signature and acceptance of the charge for the agreed length of stay etc.

If the dispute is over charges levied since the Cardholder checked-out, for example mini-bar charges or breakfast on their last day, please send a copy of the transaction receipt with “Signature on file” written in the Cardholder signature box. Please also send a copy of your registration showing the Cardholder’s signature and their acceptance of additional charges that may be made to their account.
9. Keeping Your Point of Sale Device Safe

The introduction of Chip and PIN has significantly reduced fraud; however, Point of Sale (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 swipe magnetic swipe cards for use abroad, where Chip and PIN is not used or to 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 Merchant Solutions. Never disclose your merchant number or your Terminal details to anyone else.

- Do not allow anyone other than a legitimate engineer or a direct employee of First Data Merchant Solutions 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 counter top 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

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:

- Is there any physical damage to your POS device?
- Are there any stickers on the device that were not attached at the time of installation?
- Does your POS device appear to have been modified, are there any additional components that were not there previously?

If you detect anything suspicious with your POS device, do not use it and report immediately to our Merchant Support Centre on 0845 964 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 overlooked 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.
SECTION 10: Changes to Your Business

10. Changes to Your Business

It is vital that you keep First Data Merchant Solutions apprised of any material changes to your business. Where we request in this section that you notify us of changes in writing, then you should write to us at First Data Merchant Solutions Customer Service at the address set out in Section 13 or as we may otherwise notify you. It is particularly important that you advise us of the following changes:

Change of Bank and/or Branch

You must contact the Merchant Support Centre immediately on 0845 964 5055† if your bank account details have changed. If you do not advise us there will be a delay in funds reaching your account. Changes to bank account details must be confirmed in writing. We will also require a new Direct Debit mandate.

Change of Address

You must advise First Data Merchant Solutions immediately and confirm in writing if you change your business or trading address.

Closure or Change of Ownership

Your First Data Merchant Solutions service is not transferable to anybody under any circumstances without the prior written approval of First Data Merchant Solutions. If you are selling or closing your Business or there is any material change to the nature, size or scope of your Business you must confirm this in writing to First Data Merchant Solutions. If the purchaser of your Business wishes to use First Data Merchant Solutions, a new account may have to be opened that reflects the new ownership and we reserve the right to make our usual pre-contract enquiries. If you fail to advise us that you no longer own the Business you will continue to be liable for any liabilities that the subsequent owner(s) generate.

You must also advise us immediately of:
→ Any changes to directors, partners or to the other officers of your Business
→ Any change of voting control in you or your parent company
→ Any sale or other disposal of all or any material part of your assets

Change of Business or Trading Name

If you are changing the business or trading name of your Business then you must advise First Data Merchant Solutions in writing.

Change of Legal Entity

If you are changing the legal status of your Business, for example, from sole trader to limited company status, adding a partner to your Business or if a partner leaves, you must advise First Data Merchant Solutions in writing.

Change of Products or Services Sold or Other Details

When you apply for merchant services from First Data Merchant Solutions, you give us the various product details that your business sells and we categorise your account accordingly. These details, including your anticipated average sale value, are important in terms of the ongoing risk assessments that First Data Merchant Solutions regularly undertake.

Therefore, it is important that you advise us, in writing, if the nature of your Business changes, for example, a change of product or service or if you expand into an additional line of Business, different to your own existing Business. You must also advise us in writing if any of the other details that you have provided to us change, whether in your application or otherwise. If you fail to advise us you may find that proceeds from sales transactions are withheld pending our investigations and reassessment of risk.

Changing Your Trading Terms

You must advise First Data Merchant Solutions immediately if you make any changes to your trading terms, for example, any changes to your Refund policy, or to the terms and conditions issued to your customers, or to the delivery timeframes you have previously indicated to us.
Other Changes Affecting Your Business
You must advise us immediately if any of the following events occur:
→ Any Insolvency Event affecting your Business
→ You make any arrangement with creditors
→ You experience any financial difficulties

Changing Method of Taking Cards
If you would like to change your method of taking Cards – for example from Card Not Present processing to face to face Card acceptance or from taking Card Present Transactions to processing through the Internet or accepting Transactions in a Card Not Present environment, you must first obtain written authority from First Data Merchant Solutions. Failure to do so will invalidate your Merchant Agreement, and you will be liable for any Chargebacks.

The address to write to is:
First Data Merchant Solutions
Janus House,
Endeavour Drive,
Basildon,
Essex
SS14 3WF
11. Voicing Your Concerns

First Data Merchant Solutions are authorised and regulated by the Financial Conduct Authority (FCA). Every step is taken to ensure you are satisfied with the services you receive from First Data Merchant Solutions. However, 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 which we aim to meet in the handling of all customer complaints:

You can contact the First Data Merchant Solutions Customer Care Team by writing to:

Janus House,
Endeavour Drive,
Basildon,
Essex SS14 3WF

or

Telephone: 0845 964 5055†, Mon-Sat, 8am - 9pm
Email: FDMSComplaints@firstdatacorp.co.uk

We take all complaints seriously. Many issues can be dealt with straight away, but some do take a little time to investigate thoroughly. If this happens, we get a specialist from our Customer Care Team to resolve the issue. The FCA gives us eight weeks to resolve all complaints.

If for any reason you are not happy with the outcome please contact us explaining what you think we can do to put it right.

If you are still not happy after we’ve tried to put things right you can ask the ombudsman to look at your case for free. They can be contacted at:

The Financial Ombudsman Service
South Quay Plaza,
183 Marsh Wall,
London E14 9SR

or

Telephone: 0800 023 4567
Email: complaint.info@financial-ombudsman.org.uk

The Finance & Leasing Association

This association may provide a conciliation service for certain types of complaint relating to finance and leasing agreements, if First Data Merchant Solutions’ internal procedures have failed to resolve matters:

The Compliance Manager
Finance & Leasing Association,
Imperial House,
15-19 Kingsway,
London WC2B 6UN

or

Telephone: 0207 836 6511
Fax: 0207 420 9650
Email: info@fla.org.uk
12. Additional Information

Stationery
Stocks of stationery, i.e. Sales, Refund and Merchant Summary Vouchers, and deposit envelopes can be ordered by calling the Merchant Support Centre on 0845 964 5055†.

Point of Sale and Display Material
A varied selection of Point of Sale material is available by telephoning the Merchant Support Centre on 0845 964 5055†.

First Data Merchant Solutions Artwork Guide
You may not use MasterCard, Visa and Maestro logos in your advertising unless approval is gained from First Data Merchant Solutions. For advice as to the layout of your advertising, please call the Merchant Support Centre on 0845 964 5055†.

Emergencies and Disruptions
In case of any disruptions to the postal or telephone services, you are requested to hold at least 3 months’ supply of Fallback Vouchers. If a disruption does occur, the following procedure will apply:
→ Your Merchant Statement will be sent to you as soon as possible
→ Vouchers are to be submitted in the normal way
→ As your account is settled by Direct Debit to your bank, this process will continue
→ Chargebacks will be processed in the normal way but you will not receive details until the emergency is over
→ Never exceed your Floor Limit without Authorisation even if the telephone service is disrupted.
13. Useful Contact Information

**Authorisation Service**
0844 257 9400
Lines are open 24-hours, Monday to Sunday
If there is a problem with the telephone line, call the standby Authorisation number on 01268 823 130.

**Merchant Support Centre**
Helpline:
For any queries with your First Data Merchant Solutions service, please telephone 0845 964 5055†. Lines are open 8am to 9pm, Monday to Saturday.
Alternatively, you can write to First Data Merchant Solutions at the following address:
First Data Merchant Solutions
Janus House
Endeavour Drive
Basildon
Essex
SS14 3WF
Please ensure that all First Data Merchant Solutions related enquiries are referred to the Merchant Support Centre.

**PCI DSS Compliance Programme**
For any queries regarding your PCI DSS compliance status, please telephone the PCI DSS Helpdesk on 0845 300 7757 †. Lines are open 9am – 5pm, Monday to Friday.

**First Data Global Leasing**
For any queries regarding your Terminal lease, please telephone First Data Global Leasing on 0845 841 2442 †. Lines are open 8am – 5pm, Monday to Friday.

**Terminal Manufacturers**
Spire Payments Helpdesk:
0871 711 0719† Lines are open 8am-9pm, Monday- Saturday and 10am-4pm on Bank Holidays.
Ingenico Terminal Technical Support:
0844 561 6847†, Lines are open 8am-9pm Monday-Saturday and 10am-4pm on Sundays.

**ClientLine**
For any queries regarding ClientLine, please telephone the ClientLine Helpdesk on 01268 567128. Lines are open 8am-9pm, Monday to Saturday.

**Fexco (Dynamic Currency Conversion)**
For any queries regarding Fexco, please telephone the Helpdesk on 0845 964 5055†. Lines are open 8am to 9pm, Monday to Saturday.

**American Express**
For any queries regarding American Express, please telephone the American Express Helpdesk on 01273 675533. Lines are open 8am-6pm Monday to Friday, and Saturday 9am-5pm.

**Plusnet and Phoenix**
For any queries regarding your Plusnet and Phoenix broadband, please telephone the Plusnet and Phoenix Helpdesk on 0845 964 5055†. Lines are open all day, everyday.
14. Glossary

Additional Service means a service agreed between you and First Data Europe Limited;

Applicant means the applicant for merchant services from First Data Europe Limited who is submitting or has submitted the Application Form to First Data Europe Limited;

Application Form means the form submitted by the Applicant applying for merchant services from First Data Europe Limited to be provided under the terms of your Merchant Agreement;

Assured Reservations means the facility whereby a Merchant who makes a reservation of accommodation for a Cardholder will maintain that reservation regardless of the time of arrival of the customer on the day for which the reservation is made and may charge the Cardholder in respect of the reservation where the customer does not arrive;

Attest means to demonstrate and confirm your compliance with the PCI DSS and any changes, which may occur to those standards, by completing a self assessment attestation through the PCI DSS Complete Solutions Service, either on-line, over the telephone or in paper form, or submitting a report of compliance from a PCI DSS audit;

Authorisation means our approval for a Card Transaction to go ahead. Authorisation only confirms that the Card has not been registered as lost or stolen and has available credit at the time of the Card Transaction. It does not confirm that the person who presents the Card is the genuine Cardholder and, therefore, alone it does not prevent the Card payment being charged back to you in accordance with your Merchant Conditions;

Authorisation Centre means the telephone call centre where manual requests for Card Transaction Authorisations are handled;

Authorisation Code means the code issued to confirm a Card is valid and funds are available to cover the value of the transaction at the time Authorisation is sought;

Bureau de Change Transactions means Card Transactions accepted as part of a Bureau de Change business;

Business means your business as a Merchant as described in your Merchant Agreement or such other description as we may agree from time to time;

Business Day means any day, which is not a Saturday, Sunday, or a Bank Holiday in any part of the United Kingdom;

Card means any valid payment card approved by First Data Europe Limited from time to time and to which your Merchant Agreement applies;

Card Acquirer means any bank or other body duly authorised to process Card Transactions from a Merchant;

Cardholder means the company, firm, individual or other body for whose use a Card has been issued at any time;

Cardholder’s Account means the account in the name of the Cardholder, which may be debited or credited by the Card Acquirer in respect of Card Transactions;

Cardholder Information means any information relating to a Cardholder including any Card Number and any Personal Data;

Card Issuer means any bank or other body authorised by a Card Scheme to issue Cards;

Card Not Present Floor Limit means the Total Value for each Card Not Present Transaction at which you must obtain Authorisation. This is set out in your Merchant Agreement.

Card Not Present Transaction means any type of Card Transaction where the Cardholder is not present and/or the Card is not provided physically to you at the time of the transaction, including Card Transactions made via the telephone, mail order and/or a Website;

Card Number means the number displayed on a Card identifying the Cardholder’s Account;

Card Present Floor Limit means the Total Value for each Card Present Transaction at which you must obtain Authorisation. This is set out in your Merchant Agreement.

Card Present Transaction means any type of Card Transaction where the Cardholder is present and the Card is provided physically to you at the time of the transaction;

Card Refund means any refund given in respect of a Card Transaction for credit to the Cardholder’s Account;

Card Refund Data means the details of a Card Refund processed through a Terminal or a Website in a form we approve;

Card Sales Data means the details of a Card Transaction processed through a Terminal or a Website in a form we approve;
SECTION 14: Glossary

Card Scheme means Visa International, MasterCard International, Japanese Credit Bureau and any other card scheme we approve from time to time;

Card Scheme Rules means the rules and operating instructions issued by particular Card Schemes from time to time;

Card Security Code (CSC) means the three or four digit number printed on the signature strip directly after the Card Number;

Card Transaction means any payment made by the use of a Card, a Card Number or in any manner authorised by the Cardholder for debit to the Cardholder’s Account;

Cashback means a service provided to Cardholders whereby cash is dispensed with a Debit Card purchase transaction at the Point of Sale;

Cashback Limit means the maximum amount of cash that you may provide to a Cardholder as part of a Purchase with Cashback as we may notify from time to time;

Chargeback means a Card Transaction that is disputed by a Cardholder or Card Issuer and is returned to First Data Europe Limited under the relevant Card Scheme Rules;

Charges means the charges which become payable by you to us (which may be collected by First Data Merchant Solutions) as specified in the Merchant Conditions and the Charges Schedule;

Charges Schedule means the schedule in your Application Form setting out certain charges that may be payable by you. We may increase or decrease this from time to time, providing written notice of the change;

Chip and PIN Card means a card in respect of which a PIN may be entered in a PIN Entry Device;

Chip Card means a plastic Card containing a microchip which has highly secure memory and processing capabilities, which can be recognised by the gold or silver coloured contact plate on the front of the card and which may be entered into a chip reader; Chip Cards are also known as integrated circuit cards (ICCs) or smart cards;

Complaints Procedure Leaflet means the leaflet explaining our complaints procedures as may be varied from time to time;

Debit Card means a Visa Debit Card, Visa Electron Card, International Maestro Card, UK Maestro Card, Debit MasterCard and such other Cards as notified by us to you from time to time as being debit cards.

Deferred Payment means we are of the opinion that there is a potential risk of loss to First Data Europe Limited through Chargebacks, we may alter the way we settle Card Transactions between you and a Cardholder by moving you on to a system under which we settle such Card Transactions by holding back payments to you for a pre-determined number of days.

Deferred Supply Period means the maximum period specified in your Application Form, or the period agreed with the Cardholder at the time of the Card Transaction (if less), within which you must supply goods, services, accommodation or other facilities following the time of the Card Transaction;

Deferred Supply Transactions means Card Transactions where the goods, services, accommodation or other facilities are supplied to the Cardholder at a time later than the time of the Card Transaction;

Disabling Device means any software, viruses, worms, time or logic bombs, trojan horses or other computer instructions, intentional devices or technologies that can or were designed to threaten, infect or disrupt, damage, disable or shut down all or any part of a computer program, network or computer data;

Dynamic Currency Conversion (Global Choice™) means the ability to offer overseas Visa and MasterCard cardholders the option to pay for goods or services in their own currency.

E-Commerce means a business transaction conducted electronically. This includes Card Transactions taken over the internet.

E Statement means an electronic copy of your monthly Merchant Statement delivered by email;

Electronic Link means any computer system, servers or network used by you to communicate with First Data Merchant Solutions or with Cardholders;

Electronic Refund Receipt means an electronic Refund Receipt used in respect of Card Not Present Transactions entered into through a Website in the form we approve;

Electronic Sales Receipt means an electronic Sales Receipt used in respect of Card Not Present Transactions entered into through a Website in the form we approve;
Equipment means all equipment including Terminals and any hardware or software we or our agents have approved or supplied to you for use in connection with your Merchant Agreement;

Eurocard means a credit card issued by MasterCard and carries the MasterCard logo;

Express Checkout means a facility that enables Merchants offering accommodation to improve the efficiency of their checkout procedures, which involves having their Terminal downloaded with the appropriate level of software;

Express Funding means the funding method that facilitates payment of Transaction Data settlement within a specified number of days following transaction processing day;

Fallback means a transaction taken using a paper voucher when electronic terminal/Point of Sale systems have failed;

Fallback Floor Limit means the Total Value for each Card Transaction at which you must obtain Authorisation while your Terminal or other Equipment is out of order or the Website or any Electronic Link is not available or functioning correctly. This would normally be the Card Present Floor Limit or the Card Not Present Floor Limit (as applicable) unless we notify you otherwise;

Fallback Procedures means the procedures you must follow, as set out in this Operating Guide, or as we may notify you from time to time, if your Terminal or other Equipment has failed for a technical reason or a Website or Electronic Link is not available or functioning correctly;

Fallback Vouchers means the vouchers we supply or approve which you must use for Card Transactions where your Terminal or other Equipment has failed for a technical reason or the Website or Electronic Link is not available or functioning correctly. Fallback Vouchers may be in the same form as Sales Vouchers;

Floor Limit means the Card Present Floor Limit or Card Not Present Floor Limit (as applicable);

Foreign Currency Card Transactions means Card Transactions where the currency of payment is to be in a currency other than Pounds Sterling;

Group means First Data Europe Limited, any holding company of ours or any subsidiary of ours or our holding company. For the purposes of this definition “subsidiary” and “holding company” shall have the meanings given to them in section 736 of the Companies Act 1985 including any subsidiary acquired after the date of this Merchant Agreement;

Insolvency Event means that a merchant becomes insolvent or is made to pay its debts as they fall due or becomes subject to, or takes any steps to invoke, any law, proceedings, preliminary or relating to its insolvency, winding up administration or receivership (or any analogous proceedings in any jurisdiction) or any enforcement of any security against it or rescheduling, composition or arrangement in respect of any of its debts. Or if you are an individual or a partnership, you (or any of your partners) are the subject of a bankruptcy petition or order or you, (or your partners ) are unable to pay or have no real prospect of paying your debts.

Intellectual Property Rights means all present and future intellectual property rights, including patents, utility models, trade and service marks, trade or business names, domain names, rights in design, copyrights, moral rights, topography rights, databases rights, trade secrets and rights of confidence in all cases whether or not registered or registrable in any country for the full term of such rights, rights to apply for the same and all rights and forms of protection of a similar nature as having equivalent or similar effect to any of these anywhere in the world;

Interchange Plus means the fees levied by the Card Schemes passed through to you at cost, plus the Merchant Service Charge;

International Maestro Card means a Maestro card issued outside of the United Kingdom;

Internet Card Transactions means an E Commerce card transaction made over the internet;

Maestro means a Card for use with the debit card scheme known as “MAESTRO” through which payments are made for goods, services, accommodation or other facilities;

MasterCard means the scheme through which payments are made for goods, services, accommodation and other facilities using a MasterCard or Maestro branded Card;

MasterCard SecureCode means a programme designed to provide online retailers with the added security of having issuing banks authenticate their individual Cardholders and qualify their online transactions for protection against “cardholder unauthorised” or “cardholder not recognised” Chargebacks.

Merchant means any supplier of goods or services and authorised by a Card Acquirer (in your case, First Data
SECTION 14: Glossary

Europe Limited trading as First Data Merchant Solutions) to accept Cards;

Merchant Account means the bank account you nominate which we may debit or credit with payments in respect of Card Transactions;

Merchant Agreement means the Application Form, which includes the Charges Schedule, the Merchant Conditions and this Operating Guide. These documents together form the agreement between you and First Data Europe Limited;

Merchant Conditions means the terms and conditions as may be varied from time to time;

Merchant Service Charge means the charge made by First Data Merchant Solutions to you for the processing of transactions;

Merchant Statement means the monthly statement we issue to you, or which we agree you may view electronically, in respect of all Card Transactions processed by First Data Merchant Solutions for you in the preceding month;

Merchant Summary Voucher means a document provided by First Data Merchant Solutions to a Merchant in which a Merchant lists the amount of each Sales Voucher or Refund Voucher;

Merchant Support Centre means the telephone call centre where all Merchant enquiries are handled;

Merchant Statement means the monthly fee for the provision of services agreed between you and First Data Europe Limited;

Non Qualifying means a transaction taken outside of the terms of your Merchant Agreement with First Data Europe Limited or not undertaken in accordance with Card Scheme rules, as detailed in this Operating Guide;

Paper Statement means a paper copy of your monthly Merchant Statement delivered by post;

Payment Card Industry Data Security Standards (PCI DSS) means the standards and any changes which may occur to those standards laid down by the Card Schemes and published by the Payment Card Industry Data Security Standards Council or its successors, to minimise the potential for Card and Cardholder data to be compromised and used fraudulently;

Payment Service Provider (PSP) means the provider of the secure online payment gateway link between your website and First Data Merchant Solutions;

PCI DSS Compliance Programme means our or our agent’s Payment Card Industry Data Security Standard Compliance Programme or such other compliance programme devised to test PCI DSS compliance as we may notify you from time to time;

Personal Data means data which relates to a living individual who can be identified from such data, and/or from other information including expressions of opinion or any indication of intentions provided at any time to First Data Europe Limited or otherwise processed at any time by First Data Europe Limited or our agent(s) including personal or financial information on a Principal or other person including details of Card Transactions;

PIN means a personal identification number issued by a Card Issuer to a Cardholder for use with a PIN Entry Device;

PIN Entry Device means the device present at the Point of Sale in which a Cardholder can enter their PIN as part of a Card Present Transaction;

Point of Sale (POS) means the physical location at which you accept Card Transactions and in the case of Card Not Present Transactions via a Website, the POS is where you have your fixed place of establishment;

Polling means the process by which Card Transactions are collected electronically by us or by a third party polling bureau appointed by you (and approved by First Data Europe Limited) and submitted to us for processing;

Pre-Authorised or Pre-Authorisation means those Card Transactions for which a Merchant has sought authorisation prior to the debiting of the Cardholder Account;

Premium Cards means Visa consumer charge cards, MasterCard World cards and MasterCard World Signia cards and such other cards as notified by us to you from time to time as being Premium Cards.

Principal means an individual who is:
- a sole trader;
- a partner;
- in the case of a limited company, a director or a company secretary;
- in the case of a limited liability partnership, a member or a designated member;
who provides information in the Application Form or otherwise as part of an application for merchant services from First Data Europe Limited, or in performance of your Merchant Agreement including during financial reviews and interviews;

**Privacy Policy** means a policy explaining how you fairly and lawfully process Personal Data on a Website and explaining your obligations and the rights of the person whose Personal Data you process under the Data Protection Act 1998;

**Processing Day** means the day on which a transaction is processed following the Card Transaction acceptance through a Point Of Sale device;

**Purchasing Cards** means Cards which are issued by a Card Issuer to business customers for the payment of goods, services, accommodation and other facilities purchased from other businesses;

**Purchasing Card Transactions** means those Card Transactions in which a Purchasing Card is used;

**Qualifying** means a transaction undertaken within the terms of your Agreement with First Data Europe Limited and in accordance with Scheme rules, as detailed in this Operating Guide;

**Recurring Transactions** means those Card Transactions for which the Cardholder authorises you to debit their account on a periodical, recurring basis;

**Refunds** means the reimbursement to a Cardholder of an earlier Card Transaction between the same Cardholder and you onto the same card;

**Refund Receipt** means a receipt in respect of Refunds in the form we approve;

**Refund Voucher** means a paper voucher in respect of Refunds in the form we approve;

**Sales Receipt** means a receipt in respect of a Card Transaction in a form we approve;

**Sales Voucher** means a paper sales voucher in the form we approve;

**Secure Ecommerce** means a transaction undertaken through a secure internet gateway;

**Software Provider** means the provider that supplies you with software to enable acceptance of card transactions;

**Standard Funding** means the funding method that facilitates payment of Transaction Data settlement within five Business Days following the transaction Processing Day;

**Terminal** means the hardware approved by First Data Europe Limited which you use to process Card Transactions electronically;

**Terminal Agreement** means your agreement with your terminal leasing company, or directly with the manufacturer of your Terminal, relating to the supply of your Terminal;

**Terminal Refund Receipt** means the type of Refund Receipt produced by your Terminal in the form we approve;

**Terminal Sales Receipt** means the type of Sales Receipt produced by your Terminal in the form we approve;

**Terminal User Guide** means the user guide supplied with the Terminal by the Terminal manufacturer;

**Termination Fee** means the fee payable by you on termination of your Merchant Agreement as set out in the Fees Schedule;

**Total Value** means the total value (in pounds sterling) of any goods, services, accommodation or other facilities purchased using a Card (including any part of the value of the purchase paid for by another Card or other method of payment). For example, a Cardholder may purchase goods for £100 but pay for it using £50 in cash and £50 on their credit card. The Total Value in that example is £100;

**Transaction Data** means data relating to a Card Transaction including Card Sales Data and Card Refund Data;

**UK Maestro Card** means a Maestro card issued within the United Kingdom;

**United Kingdom** means the United Kingdom of Great Britain and Northern Ireland, but excludes, for the avoidance of doubt, the Isle of Man and the Channel Islands;

**Verified by Visa** mean a programme designed to provide online retailers with the added security of having issuing banks authenticate their individual Cardholders and qualify their online transactions for protection against "cardholder unauthorised" or "cardholder not recognised" Chargebacks.
SECTION 14: Glossary

Visa means the scheme through which payments are made for goods, services, accommodation or other facilities purchased using a Visa branded Card;

Visa Debit Card means a Card for use with the electronic debit card scheme known as “VISA DEBIT” through which payments are made for goods, services, accommodation or other facilities;

Visa Electron Card means a Card for use with the electronic debit card scheme known as “VISA ELECTRON” through which payments are made for goods, services, accommodation or other facilities;

Vouchers means Sales Vouchers, Refund Vouchers and Fallback Vouchers;

Website means any website owned, or operated by you or your agents or otherwise used by you or your agents to process Card Transactions.
Information is available in large print, audio and Braille on request. You may contact us using Type Talk.