The ins and outs of taking card payments with us

Merchant Agreement and Card Acceptance Operating Guide

Contents

1. Introduction 4

1.1 Basic rules....4

1.2 Recordkeeping....4

1.3 Banking procedures....4

2. Before you accept card payments 5

2.1 How to verify the card....5

2.2 Commercial cards....5

2.3 How to guard against fraud....6

Important....6

3. Accepting Card-Present transactions 8

3.1 Chip and PIN-enabled cards....8

3.2 Contactless transactions....8

3.3 Chip and signature cards....8

4. Accepting Card-Not-Present (CNP) transactions 8

4.1 Card Security Code (CSC)....9

4.2 Address Verification Service (AVS)....9

4.3 Authorisation responses....10

4.4 eCommerce transactions....11

Recurring Transaction....13

Instalment Transaction....13

4.5 Pre-authorisations....14

4.6 Referrals....14

5. Purchase with cashback 14

6. Refunds 14

7. Paper vouchers 15

7.1 Completing a sales or refund voucher....15

7.2 Preparing and submitting vouchers....15

8. Exceptional procedures 16

8.1 Can I pass charges to my customer?....16

8.2 Split sales and transactions....16

8.3 Terminal fallback....17

9. Chargebacks 17

9.1 Common causes of chargebacks 18

9.2 Retrieval requests 18

9.3 Chargeback reversal procedure 18

9.4 Help reduce the risk of chargebacks 18

10. Other services 19

10.1 Vehicle rental services 19

Procedure for completing vehicle rental transaction 19

10.2 Hotels, lodging and accommodation 21

10.3 Dynamic Currency Conversion (DCC) 25

10.4 Multicurrency and cross-border transaction acceptance 26

10.5 Payment of debt 26

11. Payment Card Industry Data Security Standard (PCI DSS) 27

11.1 Becoming PCI compliant 27

11.2 Implications of not complying with the PCI DSS 27

11.3 Third-party obligations 28

11.4 Secure data storage 28

11.5 Demonstrating compliance with PCI DSS 28

12. Keeping your Point-of-Sale (POS) device safe 29

12.1 Positioning your POS device 29

13. Qualifying/Non-qualifying transactions 30

13.1 Processing method – transactions taken exclusively in a face-to-face environment 30

13.2 Processing method – Transactions taken in a face-to-face environment and/or mail and telephone order 30

13.3 Processing method – transactions taken in an eCommerce environment 30

14. Voicing your concerns 31

15. Get in touch with us 32

16. Changes to your business 33

1. Introduction

Hello and thanks for choosing Clover. This guide forms part of your Merchant Agreement and contains the steps you need to follow around taking card payments.

Following the rules

Please remember that all businesses that accept payments by credit and debit card must follow the procedures set out by the Card Schemes, us as your Acquirer and the Payment Card Industry Data Security Standard (PCI DSS).

These standards and procedures exist to protect you and your customers.
It is also important to follow some basic procedures that are strictly enforced by the Card Schemes.

1.1 Basic rules

You must:

- Clearly display card acceptance logos for your customers to see, for example, Visa, Mastercard and Diners
- Only accept the card types that you're entitled to take as specified in your Merchant Agreement
- Make sure any surcharges you add to card payments are displayed to customers, and paid as part of the transaction amount. They can't be charged separately
- Include any taxes in the amount charged on card transactions
- Provide a sales receipt for the cardholder to confirm the amount debited from their payment card
- Validate your compliance with the PCI DSS (see Section 12)
- Never process any transactions for goods and services that don't directly relate to your Business, as specified in your Merchant Agreement
- Notify us of any changes to your business (see Section 16)
- Retain a copy of all sale and refund receipts for 18 months

You must not:

- Indicate that any Card Scheme endorses your goods and services
- Submit a card transaction that has been previously subject to a chargeback
- Accept card transactions on behalf of third parties
- Manually key a payment card transaction into a point-of-sale terminal when the card details have been provided through an internet shopping cart
- Process card transactions without the cardholder's permission
- Process eCommerce transactions without prior agreement and designated eCommerce facility
- Leave your terminal unattended for example, where fraudsters could have easy access
- Store sensitive card data (see Section 2)

1.2 Recordkeeping

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

1.3 Banking procedures

Please follow the end-of-day banking procedures detailed in your Terminal User Guide to make sure you receive payment for all transactions. It's essential that all transactions are submitted for payment within two (2) working days of being accepted. Please note that if a transaction is submitted after two working days, the card issuer may reject the transaction, resulting in it being charged back.

2. Before you accept card payments

Your Merchant Agreement with us states the card types that you are allowed to accept. It's important that you and your staff understand how to recognise different card types to reduce fraud risk.

As the majority of the cards are processed as PIN-verified or Contactless, you will not have the sight of the card. If signature verification is needed, then you will need to check the signature on the back of the card matches the signature given by the cardholder.

With the development of electronic payment services, there are a variety of cards available to cardholders. We strongly advise you and your staff to familiarise yourselves with the examples we have provided below to recognise security features, such as card logo, hologram, card security code and so on.

Newly issued cards will have a card type printed on the front of the card as debit, credit, commercial or prepaid.

2.1 How to verify the card

- **Chip** – Works together with cardholder's PIN or signature to create a more secure payment, look for any visible damage.
- **Card Number** – Usually, (but not limited to a) 16-digit long number on the front of the card that should be clear to read and in line.
- **Cardholder title and name** – Should be clear to read and in line. Check that the title printed/ embossed on the card matches the gender of the customer presenting the card.
- **Signature panel** – A card should be signed by the cardholder once received. If transaction is taken in a way that needs signature verification, make sure that the signature on the back of the card matches the one provided by the customer. Check strip for any visible damages or evidence of writing over previous signature and so on.
- **Expiry date/Valid from date** – Only some cards have valid from date, but all should have an expiry date. Make sure that card is not presented to you after the expiry date and/or before the valid from date.
- **Hologram** – The 3D image should move when the card is tilted and may be located on the front or back of the card.

  Please note that some Visa Electron Cards don't have a hologram. On Visa cards look for a flying dove; Mastercard look for the globe and Maestro look for William Shakespeare's head.
- **Card Security Code** – Typically located on the back of the card – on signature panel or the white box next to it.
- **Ultraviolet (UV) features** – Images under the UV light will show: On Visa – a flying dove; on Mastercard – letters 'M' and 'C' and Diners Club International/Diners – a circle with a vertical line in the middle. Similarly to the hologram, some Visa Electron and Mastercard Cards issued after October 2015 don't carry the UV image.
- **Card scheme logo** – This should be clear and match the examples shown below:

2.2 Commercial Cards

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

2.3 How to guard against fraud

There is a risk that exists with taking all types of transactions. This section outlines industry best practices that can help you to identify and reduce risk. Remember that the best fraud prevention is well-trained staff. Please make sure that staff accepting card payments on your behalf have read and understand the following procedures. Plus, any fraud prevention documents that we may send you in the future. This will help reduce financial losses to your business and risk of chargebacks.

Important

Please note an 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.

Face-to-Face transactions (Card-Present)

Preventing and detecting fraudulent face-to-face transactions:

- Chip and PIN are the most secure types of transactions. As the cardholder will retain the control of the card when processing the transaction, you don't need to make visual checks of the card. You must, however, follow the prompts on your terminal.
- Despite the fact that nearly all cards in the U.K. are chip enabled, sometimes you will need the cardholder's signature as a verification method. Please check that the person presenting the card is the genuine cardholder and follow the prompts on your terminal.

Checking the card

- Never key a card number into your terminal if both card and cardholder are present. This may result in a chargeback to you
- Check if the name on the card matches the signature. Remember to check the condition of the signature panel; if it looks damaged, it may be because the original signature has been covered over
- If possible, check the spelling on the card and sales voucher
- Compare the last 4-digits of the card number to that printed on the sales receipt. This check will allow you to identify a cloned card
- Check for the special mark on the card using a UV lamp. If you place the card under the lamp, you should see a hologram

Checking the cardholder

- Check if the title on the card matches the customer
- Does the customer seem nervous or hurried?
- The customer insists upon taking the goods immediately for example, they are not interested in free delivery
- The customer takes an unusual amount of time to sign and refers to the signature on the back of the card
- The customer repeatedly returns to make additional orders in a short period of time
- If a transaction is declined and the customer then requests a lower-value authorisation attempt

Checking the transaction

- The customer makes an order substantially greater than you would normally expect
- The customer purchases more than one of the same item (That is, items that may be easily re-sold such as jewellery, video equipment, stereo equipment, computer games)
- A fraudster may present more than one 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.

Card-Not-Present (CNP) transactions – Mail Order Telephone Order (MOTO)

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

Preventing and detecting fraudulent MOTO transactions

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

Preventing and detecting fraudulent eCommerce transactions

Some signs to look out for:

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

Delivery warning signals

Some signs to look out for:

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

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 deliver to the agreed person/address
- Don't deliver to an address that is obviously unoccupied
- To get signed proof of delivery, preferably the cardholder's signature
- If you have your own delivery service, consider training your driver to check the card. If you wish to do this, please contact the Fraud Department by phoning the Merchant Support Centre on 0345 606 5055* for more details.

3. Accepting Card-Present transactions

3.1 Chip and PIN-enabled cards

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

3.2 Contactless transactions

If the cardholder's card or device, for example, mobile has been enabled for contactless, the process is as follows:

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

You can't offer cash back on a contactless transaction.

3.3 Chip and signature cards

- Ask the cardholder to insert the card into the chip reader and follow the prompts on the terminal
- Ask the cardholder to sign the receipt and check that it matches the one on the card

4. Accepting Card-Not-Present (CNP) transactions

A CNP transaction is when a card is not presented at the point-of-sale for example, mail/telephone order, eCommerce or recurring transactions all of which must be authorised.

- Take extra care to make sure it's the genuine cardholder placing the order
- To defend any disputes keep a record of any permission to debit the card for example, a recurring payment agreement or a call recording

To process a CNP transaction you must get the following information:

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

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

4.1 Card Security Code (CSC)

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

- The CSC is not retained in your terminal, if supplied through us
- If a customer provides written card details, you must make sure the details are securely deleted
- Card numbers and the CSC are valuable data you must never record or accept copies of
- CSC is not needed for the following:
  - Reservations
  - Corporate and purchasing cards
  - 'No Show' transactions
  - Cancellation refunds
  - Charges after check out
  - Mail-order transactions

CSC can't be stored; it can be used for one transaction only. Once the transaction has been authorised, you must not keep a record of the CSC.

4.2 Address Verification Service (AVS)

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

- Only the numbers in the postcode of the cardholder's statement address
- Up to the first five numbers of the cardholder's statement address
- Your terminal will prompt you to enter the numbers in the three stages below:

Cardholder's address	Card security code	Postcode numeric	Address numeric
55 South Street Any Town, Any County SS17 1B	000 or 1234	171	55
Flat 3, 21 North Street Any Town, Any County LM5 7LT	000 or 1234	57	321
The Cottage East Lane Any Town, Any County SS12 3BL	000 or 1234	123	Bypass*
Apt 62, 2190 West Road, Any Town, Any County LM45 1LT	000 or 1234	451	62219

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

4.3 Authorisation responses

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

- The final decision to accept the payment or not is yours
- You are responsible should a transaction be confirmed as invalid or fraudulent, even if, the data matches and an authorisation code is issued
- AVS/CSC does not protect you from a chargeback. AVS and CSC responses don't consider whether there are sufficient funds or even if the card is lost or stolen. You can still get a positive AVS/CSC match on a declined transaction

Response	Definition	What to do
Data matches/ data matched	Both the AVS and CSC match the card Issuer's records	If you have been issued an authorisation code and are satisfied the transaction is genuine, then unless there are other suspicious circumstances you are likely to want to go ahead with this transaction. As with all CNP transactions, payment is not guaranteed and you bear the risk if the transaction is disputed.
Data non-match/data not matched	The CSC and one or both of the address details don't match the card issuer's records	Indicates this could be either a fraudulent transaction or the details have been entered incorrectly. We recommend you don't proceed unless further checks are made to verify the cardholder and the delivery address provided.
CSC match only	Either house number or postcode don't match the card Issuer record	
AVS match only	Both address and postcode match but not the CSC	
Not checked	The CSC and AVS have not been checked	You will have to make a decision based on the information you have. We recommend further checks are made before going ahead with the transaction.

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

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

Rules for CNP transactions

When the cardholder places the order, you must get a pre-authorisation and when the goods or services are ready to be delivered the transaction should be processed.

The pre-authorisation is valid as follows:

- **Visa** – The transaction amount must be within 15% of the pre-authorisation amount and the goods must be shipped within 31 days, otherwise a second pre-authorisation will be needed
- **Mastercard and Diners** – The transaction amount must equal the pre-authorisation amount and the goods must be shipped within 30 days, otherwise a second pre-authorisation will be needed

4.4 eCommerce transactions

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

On approval, we'll give you a new Merchant number, this is solely for the purpose of acceptance of eCommerce transactions for the business described within the new application form.

All eCommerce transactions are regarded as 'Card-Not-Present transactions' and are taken at your own risk. In the case of a dispute, we retain the right under the Merchant Agreement to chargeback any eCommerce transactions irrespective of whether an authorisation code is given.

Website requirements

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

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

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

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

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

- Cardholders' full name
- Cardholders' email address
- Cardholders' billing address and postcode
- Delivery address

Payment page (check-out)

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

- The products and the services, as well as, total cost (That is, showing any additional cost such as applicable tax, packaging, delivery charges and so on)
- Terms and conditions, including your return and cancellation policy
- Instructions on how to complete their order

The payment page on your website, whether provided by a third-party or created by you, must be PCI DSS compliant and collect at least the following:

- Transaction amount
- Card type box, for example, the card types detailed in your Merchant Agreement
- Customers' card number
- Card expiry date
- CSC

Payments and refunds

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

Receipt requirements

You must provide a cardholder receipt by email and/or post which contain the following:

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

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

Verified by Visa and Mastercard SecureCode

These are industry wide initiatives introduced to combat Internet fraud, commonly known as Cardholder Authentication. Cardholders who register for this service with their card issuer will be needed 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 whole process takes a few seconds and the online shopper is unlikely to be inconvenienced by it.

These services must be present on your website in order to accept eCommerce transactions by Visa, Mastercard, Maestro Cards and Diners. It will allow you to reduce likelihood of chargebacks, as the tool helps to make sure that the online shopper is a genuine cardholder.

For further information on these services, contact the Merchant Support Centre on 0345 606 5055.*

Payment Services Provider (PSP)

You must be set up with the Clover eCommerce Gateway (or a third-party PSP) if you want to accept eCommerce transactions. Please note if you are using a third-party PSP they must be PCI DSS compliant and accredited with us to submit eCommerce 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.

Security

We can give you with a fully hosted solution. For further details, please call our dedicated in-house support team on 0330 123 1241.*

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

Recurring Transaction

Payment for goods or services that are received over time, for example, insurance or subscription. Written agreement from us is needed to take these transaction types.

The cardholder must consent to periodic charges for recurring merchandise or services at the time of the first transaction. This permission must include at least all of the following, in writing and must be provided to the cardholder:

- transaction amount.
- fixed dates on or intervals at which the recurring transactions will be processed.
- duration for which cardholder permission is grantedcancellation and refund policies.

You must retain the cardholder's permission for the duration of the recurring merchandise or services.

A recurring transaction amount must not:

- include partial payment for merchandise
- services purchased in a single transaction.
- include finance charges.

Authorisation is needed for each individual recurring transaction.

You must provide an online cancellation procedure if the:

- cardholder's request for merchandise or services was initially accepted online.
- not complete a recurring transaction beyond the duration expressly authorised by the cardholder or if it receives either a cancellation notice from the cardholder or a decline response.

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).

Instalment Transaction

A regular payment against a single purchase, for example, car or loan. Written agreement from us is needed to take these transaction types.

You must provide and the cardholder must consent to the merchandise or services and all of the following in writing at the time of the first transaction:

- terms of service.
- timing of delivery to cardholder.
- transaction amount.
- total purchase price.
- terms of future payments, including the dates and amounts.
- cancellation and refund policies.

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

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

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

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

- cancellation or refund confirmation in writing.
- credit transaction receipt for the amount specified in the cancellation policy.

VAU and ABU are not available for instalment transactions.

If you don't process a recurring or instalment transaction at the time of entering into the agreement with the cardholder you must:

- submit an Account Number Verification Transaction Authorisation.
- identify the Account Number Verification Transaction as a Recurring or Instalment transaction in the Authorisation.
- please contact your Payment Service Provider (PSP) to enable Account Number Verification Transaction Authorisation.
- never process Recurring Transactions on Maestro and VPAY Cards as this is not permitted.

VAU and ABU

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

Visa Account Updater (VAU) and Mastercard Account Billing Updater (ABU) maintain databases that consist of participating issuer card information. These databases enable merchants to validate a recurring payment agreement has not been cancelled and the card number/expiry date is valid. Get in touch if you need more information.

Instalment transactions

Instalment transactions work in a similar way to recurring transactions with the exception of instalment transactions that represent a single purchase, with payment occurring on a schedule agreed between a cardholder and merchant, for example, loan/car/debt repayment transactions over a set period of time.

An authorisation must be taken at the time of the transaction. You should not proceed when your request for authorisation is declined. Multiple authorisation attempts following a decline is not permitted. Please remember that it's your responsibility to make sure that all transactions are authorised in accordance with your Merchant Agreement.

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.

4.5 Pre-authorisations

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

4.6 Referrals

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

For authorisation call 0344 257 9400. Lines are open 24 hours, 7 days a week.

5. Purchase with cashback

Purchase with cashback allows your customers to request cashback when purchasing goods using their debit card. Written agreement from us is needed to take this transaction type the following rules apply:

- Can only be to customers who make a purchase with their card.
- Must be through an electronic terminal, not a manual imprint machine.
- Must not exceed the maximum cashback amount confirmed in your written notification from us.
- Enter the purchase and cashback amounts separately as prompted by your terminal.
- Cashback can be offered on Visa Debit, Visa Electron, Maestro, Debit Mastercard issued in Europe only.
- Follow the terminal prompts it will tell you whether the purchase with cashback has been approved.

6. Refunds

You are only permitted to make a card refund when the original sale was on the same card. The refunded amount will be credited to the cardholder's card and debited from your account.

When processing refund transactions:

- you must check that the card presented for the refund is the same one used for the original sale.
- you should never make a refund on the card where the original sale was made by cash or cheque.
- you should never make a refund by cash or cheque where the original sale was on a card.
- you should never make a card Refund for amount higher than the original sale.

7. Paper vouchers

If you are unable to use your card terminal for sale and refund transactions follow the procedures below. The paper vouchers contain the following copies:

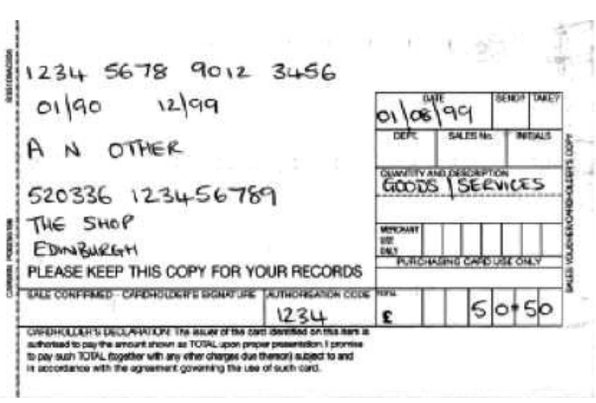
- Merchant/Top Copy – You must retain this for 18 months from the date of the card or last recurring card transaction (To defend a disputed transaction)
- Processing/Middle Copy – You must post this to us
- Cardholder/Bottom Copy – This is the record of the card transaction to be given to the cardholder

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

7.1 Completing a sales or refund voucher

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

The Sales Voucher must always be completed in Pounds Sterling (£) unless you have made arrangements with us to accept different currencies. An example of correctly completed sales voucher is shown below:



7.2 Preparing and submitting vouchers

You must complete the Merchant Summary Voucher to submit your sale/refund vouchers keeping the top and middle copies and submitting the bottom copy for processing.

- Fully complete all the information fields on the voucher including your merchant number and business name
- Don't submit more than 200 vouchers on one merchant summary voucher
- All vouchers must be posted to us at Parseq, Lowton Way, Hellaby, South Yorkshire, S66 8RY. This

copy is electronically processed, therefore please don't fold, damage, PIN or staple and make sure the necessary details are clearly recorded

- To avoid an increase in your processing charges these must be received by us no later than three (3) business days from the transaction date
- If you don't submit your vouchers within this timescale the card issuers may reject the card transactions, even though you may otherwise have followed the proper authorisation procedures and/or you may be subject to a surcharge and/or a chargeback

Warning

Don't submit vouchers when the card transactions have already been processed through an electronic terminal. If in doubt, please call the Merchant Support Centre on 0345 606 5055.*

8. Exceptional procedures

8.1 Can I pass charges to my customer?

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

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

8.2 Split sales and transactions

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

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

However if one cardholder requests you to split a transaction amount between several cards, for example, where the cardholder may not have sufficient funds on one card you should proceed as follows. Only conduct the transaction if you are not suspicious of the transaction or the person presenting the card.

- Make sure all cards presented are issued with the same cardholder name
- Follow the normal card acceptance procedures as detailed in Section 3
- We recommend you only split a transaction over more than one card when it's a Card-Present Transaction and each transaction is verified by either Chip and PIN or signature (as requested by the terminal)

Warning

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

8.3 Terminal fallback

If it's impossible for the terminal to read the chip on the card or the terminal has a malfunction you should contact your terminal supplier help desk immediately to report the fault. A representative will try to resolve the problem remotely or failing this will arrange for a new terminal to be sent to your premises on the next working day, provided the fault is reported prior to 16:00. This does not include premises situated in the Highlands and Islands where replacement may take two (2) to four (4) working days. In the interim follow the guidelines below:

Card type	Revert to chip and signature	Revert to magnetic strip	Revert to pan key	Comments
Maestro and Visa Electron and Electronic Use only Cards Unable to read magnetic strip	N/A	N/A	No	Seek alternative payment method
Diners Club and Discover Cards	Yes	Yes	Yes	
All Other Card types Chip Cards PIN not enabled. Unable to read chip	N/A	Yes	No	
All Other Card types Chip and PIN enabled Cards. PIN Pad fault. Unable to accept PIN entry	Yes	No	No	
All Other Card types Magnetic strip Cards only. Unable to read Magnetic strip	N/A	N/A	Yes	

You are liable for swiped or key entered chip card transactions that are proven to be fraudulent.

9. Chargebacks

A chargeback occurs when a card issuer raises a disputed transaction on behalf of the cardholder. 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 get authorisation for a card transaction.

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

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

It's a Card Scheme requirement that if you are predominantly trading as a mail or telephone order business, a contact telephone number rather than location must be included in the transaction description (For example, The Mail Order Shop 01234 567890); for eCommerce transactions the transaction description should include reference to your website address and a contact telephone number or email address. This provides the cardholder with the ability to verify the transaction with you rather than disputing it with their card issuer (see Section 4).

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

9.1 Common causes of chargebacks

The most common causes for chargebacks are:

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

9.2 Retrieval requests

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

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

9.3 Chargeback reversal procedure

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

If the information provided is sufficient to warrant a reversal of the chargeback and within the applicable timescale we will attempt to defend the chargeback. However reversal is contingent upon acceptance by the card issuer under the applicable Card Schemes guidelines. If the chargeback is successfully reversed the card issuer has the right to present the chargeback a second time and your Merchant Account will be debited again if you have not complied fully with the terms of your Merchant Conditions and this Operating Guide. We will do our best to help you 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:

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

9.4 Help reduce the risk of chargebacks

To help protect your business against fraud, we recommend 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.

- Make sure 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, don't accept mail, telephone or eCommerce transactions. If you see an increase in these types of transactions, please contact us to make sure you have the correct Merchant Agreement in place

- Keep 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.

10. Other services

10.1 Vehicle rental services

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

Please read carefully, the guidelines below to understand regulations and risks associated with taking Vehicle Rental Service Card payments.

Information to get from the cardholder:

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

You should discuss and agree to the terms of hire, this should include, but is not limited to hire rates, cancellation and 'No Show' policy and procedures and any additional charges that may be applied such as damages or parking tickets.

Information to give to the cardholder in writing (known as rental agreement):

- Confirmation code
- Your terms and conditions and cancellation policy
- Currency of the transaction
- Reserved vehicle rental rate
- Name and the address of the location the vehicle is to be collected from
- Cancellation and 'No Show' policy and procedures
- Any additional charges that may be applied such as damages made to the vehicle or parking tickets and so on

Procedure for completing vehicle rental transaction

Pre-authorisation

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

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

Cancellation policy

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

Within your cancellation period, you must not require cancellation notification of more than 72 hours to the scheduled collection time and date of the booking without penalty. If the cardholder makes a reservation within 72 hours of the scheduled pick-up date the cancellation deadline must be no earlier than 6:00pm at the address of the scheduled pickup date.

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

No show

If the cardholder does not turn up within 24 hours of collection time and they did not cancel the reservation in accordance with your Terms and Conditions, you may charge the customer for the maximum value of the one-day rental. To do so, you will need to perform, Card-Not-Present Transaction and on the receipt 'No Show' and send a copy of a 'No Show receipt' to the billing address provided at the time of booking.

Refund policy

If you operate a no refund policy, this must be made clear to the cardholder when discussing the reservation. If you do agree to refunds, you must credit to the same card as used to make the reservation. When a charge is made to a card in error, the reversal must be applied to the card within thirty (30) calendar days. Don't refund by cash or other payment methods, as this could result in chargebacks.

Delayed charges

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

Providing evidence to the cardholder

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

- details of the violation.
- time and place of violation.
- the law violated and if applicable, a copy of the accident report.
- copy of parking tickets.
- the license number of the rental vehicle.
- the amount of the charge.

- a copy of rental agreement.
- evidence the cardholder read the Terms and Conditions, agreeing to responsibility to pay any additional charges.
- proof that the car was damaged/shortage of fuel and so on return Car rental damage – Visa Cardholders.
- you need to provide written confirmation to the cardholder within ten (10) business days from the return of the vehicle, advising of the damage and the cost.
- within ten (10) business days from receiving written confirmation, the cardholder has the right to provide an alternative estimate for the cost of repairing the damage a cardholder has the right to raise a chargeback, if the agreement is not reached and the additional charges are debited.
- you need to wait twenty (20) business days before processing the delayed/additional charges.

Car rental damage – Mastercard Cardholders

To apply additional charges to a Mastercard, you must get a separate cardholder signed authority by processing a Card-Present Transaction. If the charge is disputed at a later date, this will be needed as proof that the cardholder authorised the additional charge.

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

- a copy of the rental agreement, stating vehicle rental period.
- a copy of the document signed by the cardholder agreeing to accept responsibility for the delayed charges.
- a copy of the original notification you have sent to the cardholder informing him/her about the charges.
- a proof of cost estimation.
- a proof of law validation such a parking fine ticket, speeding fine ticket and so on.
- any supportive documentation such as police reports, insurance policy of the rental vehicle and so on demonstrating cardholder liability Not receiving requested documentation in time, may prevent us from defending the dispute and may result in a debit to your account.

10.2 Hotels, lodging and accommodation

Advanced reservation

To be able to take advanced reservation, you will need to have an agreement with us to process MOTO and eCommerce transactions. Wherever possible, the cardholder requiring accommodation or lodging should be asked to make the reservation. However, for practical reasons, you may need to accept reservations from third parties. For example, secretaries acting on behalf of their manager. Advanced reservation allows your customers to book a room in advance. As you will get the card details, you will be able to charge the cardholder should they not turn up or don't provide you with sufficient cancellation notice.

Advanced reservation can't be completed using Maestro or Visa Electron Cards.

Disputed transactions

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

- a copy of the rental agreement, stating vehicle rental period
- a copy of the document signed by the cardholder agreeing to accept responsibility for the delayed charges
- a copy of the original notification you have sent to the cardholder informing him/her about the charges
- a proof of cost estimation

- a proof of law validation, such a parking fine ticket, speeding fine ticket and so on
- any supportive documentation, such as police reports, insurance policy of the rental vehicle and so on demonstrating cardholder liability

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

Common reasons for a disputed transaction

Vehicle reservations made using a card taken by a fraudster who never arrives to collect the vehicle. In this instance, it's 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's 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 Regulations 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 make sure that you reply to card issuer requests within 14 days. Failure to do so may result in a chargeback.

Information to get from the cardholder:

- Name of the person making the reservation
- Telephone number
- Name of person(s) who will be using the room
- Expected arrival date and time
- Number of days of expected to stay
- Card number
- Card expiry date
- Cardholder name
- Cardholder billing address
- Card security code (only for telephone and eCommerce transactions)
- If the booking is for corporate purposes, you should also collect the following information:
    - The caller's name and position in the company/organisation
    - The name of the company/organisation
    - The company/organisation switchboard telephone number

You should discuss and agree on the room rate and get cardholder consent to your cancellation and 'No Show' policy. This must be clearly explained to the customer. Make sure that cardholder agrees to the agreement (for example signing the agreement or ticking a checkbox for eCommerce transaction).

Information to give to cardholder (in writing):

- The cardholder's name as it appears on the Card
- Confirmation code for guaranteed reservation
- Your terms and conditions and cancellation policy
- Currency of the transaction
- The room rate (including tax)
- The hotel's address
- Cancellation and 'No Show' policy and procedures

Advanced deposits

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

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

- Room rate (including tax)
- Amount of advanced deposit that will be billed on the card (which must not exceed the cost of 14 nights of 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

'No Show' or invalid cancellation

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

Guest arrival/check-in

Upon arrival of your guest, request to see the card 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.

Pre-authorisation

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

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

Please advise the cardholder how much you have pre-authorised, as this will reduce the amount of funds they have available on their account. The pre-authorisation helps protect you from fraudulent card use and confirms if the cardholders account is valid and has sufficient funds available. 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 pre-authorisation. If the final bill is more than the pre-authorised amount you must get another authorisation code for the difference with the exception of Visa where the bill can be within 15% of the authorised amount.

Express check-out

You may want to offer your customer the option to leave the key and check-out without waiting for the bill. If you decide to offer your guest an express/priority checkout service (the card is no longer present), be aware that 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, expiry date and cardholder name
- 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, make sure that:
    - It's signed
    - It includes the mailing address
    - The card number on the check-out agreement matches the card number on the pre-authorisation

Upon check-out, you must complete the transaction for the total charges incurred during the cardholders stay. If the final bill is more than the pre-authorised amount, you must get another Authorisation code for the difference with the exception of Visa where the bill can be within 15% of the authorised amount.

Extended stays

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

> Pre-authorisations are not supported for Maestro Cards. We recommend that you get full payment for the expected number of nights stay. If the cardholder decides to checkout early, simply provide a refund.

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

Disputes and Chargebacks

If a transaction is later disputed, it's important for you to show that the card was present and authorised (where needed).

The most common reasons for a disputed transaction are:

- reservations made using a card obtained by a fraudster who never arrives at the hotel.
- in this instance, it's likely that the fraudster is only using your reservation system to check that the card they are using is valid with funds available. It's therefore likely that the cardholder will only become aware of this when they receive their statement with your 'No Show' charge included.
- not replying to requests for information.
- under Card Scheme regulations, 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 make sure 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 we advise that a cardholder is disputing a charge, always make sure 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 taken, 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 and so on

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.

Additional charges

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

Additional checks

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

- Ask the cardholder to give either a passport or a full driving licence as a second form of ID.
- Check that the photograph of the document resembles person who presented it to you and that there are no visible changes to the picture that may indicate the document is not genuine
- Check that the second identification document is not out of date and that it shows the cardholder's signature
- On the front of the receipt, you record the description of the identification that is driving licence, passport and so on 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 four-digits must be recorded on the front of the transaction receipt to validate they have been checked

Remember:

- Never process Maestro Cards
- You must always obtain an authorisation
- Never progress taking a transaction, if the cardholder is unable to provide an acceptable second form of ID as these transactions may be charged back to you and debited from your account
- Any fees to be charged must be included within the total transaction value and disclosed to the cardholder prior to completing the transaction
- It's your responsibility to carry out the additional identity checks

10.3 Dynamic Currency Conversion (DCC)

DCC provides you with the ability to offer overseas Visa and Mastercard cardholders the option to pay for goods on services in the currency their card is issued. The price of goods and services will be shown to the cardholder in GB Pounds (£) 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 DCC is optional.
- not impose any additional requirements on the cardholder to have the transaction processed in the local currency.
- not use any language or procedures that may cause the cardholder to choose DCC by default.

Receipt requirements

DCC transaction receipts must show the following:

- 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'
- 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
  - Indicate that the DCC is conducted by you. Written agreement from us is needed to take this transaction type

10.4 Multicurrency and cross-border transaction acceptance

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

Permitted merchant location countries

The merchant location is either the physical premises where a transaction is completed, or an eCommerce or MOTO transaction where all of 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.
- merchant holds a valid business license for the merchant location.
- merchant has a local address for correspondence and legal process.
- the merchant outlet pays taxes relating to the sales activity.

Available funding and settlement currencies

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

- GBP
- Euro
- USD
- Australian Dollars
- Canadian Dollars
- Swiss Franc
- Japanese Yen
- Norwegian Krone
- Swedish Krona
- Denmark Krone
- Hong Kong Dollar
- New Zealand Dollar
- South African Rand

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

10.5 Payment of debt

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

- get authorisation, providing additional data. For more information, please contact our Merchant Support Centre on 0345 606 5005*
- complete the transaction as a purchase flagged as instalment payment
- write the type of payment made on the receipt, for example, 'Loan' or 'Mortgage'
- on the signature line of the receipt, write 'Instalment Transaction'

11. Payment Card Industry Data Security Standard (PCI DSS)

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

11.1 Becoming PCI compliant

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

- analyse your business practice and processes.
- research the appropriate security solutions for your business.
- implement and maintain security solutions.

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

PCI DSS requirements as set out by the Card Schemes:

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

11.2 Implications of not complying with the PCI DSS

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

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

11.3 Third-party obligations

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

11.4 Secure data storage

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

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

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

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

- the CVV2, also called the Card Security Code (CSC) which is printed on the back of the card, located in or next to the signature panel.
- the CVV number contained in the magnetic strip.
- the CVV number contained in the chip.
- the contents of the magnetic strip – also called track-two data.
- the customers PIN contained in the magnetic strip (PIN Verification Value PVV).

11.5 Demonstrating compliance with PCI DSS

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

Step 1

- Log into the online portal
- We will ask you a few questions
- These questions are focused around how your business is set up to handle credit and debit card payments
- Using dynamic profiling, we will only ask questions that are relevant to your business to figure out your security risk level

Step 2

- We will help you to understand how to protect your business
- This will help you understand and identify areas of your business might be at risk
- You will be taken through the security assessment that matches your business type including any scanning if needed

Step 3

- You will be asked to confirm and validate all of your responses and any tasks that you may have to undertake
- PCI DSS refer to this as your Attestation of Compliance (AoC)

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

12. Keeping your Point-of-Sale (POS) device safe

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

Criminals use stolen Card and PIN details to produce fake magnetic swipe cards for use abroad, where Chip and PIN is not used or 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 through the terminal vendor or an employee from Clover. Never disclose your merchant number or your terminal details to anyone else.

Recommendations:

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

If you detect anything suspicious with your POS device, don't use it and report it immediately to our Merchant Support Centre on 0345 606 5055.*

12.1 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 can't 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.

13. Qualifying/Non-qualifying transactions

As shown in your Merchant Agreement Fee schedule, transactions may incur a non-qualifying charge. Depending on the processing method you use and the type of card used, the transaction will be categorised as either a qualifying or non-qualifying transaction.

13.1 Processing method – transactions taken exclusively in a face-to-face environment

- Qualifying transactions are face-to-face chip, contactless and swiped transactions which are submitted for processing within two business days of the transaction. If a PIN-shield is provided with your POS, it should be used.
- A non-qualifying transaction rate may be applied when:
  - your customer pays with a Visa Business Debit Card.
  - a transaction is taken as CNP.

13.2 Processing method – Transactions taken in a face-to-face environment and/or mail and telephone order

Qualifying transactions are face-to-face Chip and 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.
- your customer pays with a U.K. issued Reward, World Elite or World Card.
- a transaction does not capture the card's CSC number.

13.3 Processing method – transactions taken in an eCommerce environment

Qualifying transactions are 3D secure enabled eCommerce transactions submitted for processing within two business days of the transaction.

A non-qualifying transaction rate may be applied to:

- Mail/telephone transactions
- 'Face-to-face' transactions
- Recurring Transactions
- Visa consumer charge cards
- Mastercard World Signia and World Cards

Interchange rates for Visa and Mastercard

Interchange rates are available on the Card Scheme Website as shown below:

Interchange for Visa U.K. www.visaeurope.com

Interchange for Mastercard U.K. www.mastercard.com

14. Voicing your concerns

First Data Europe Limited trading as Clover is authorised and regulated by the Financial Conduct Authority (FCA). If you have reason to complain, we will take a balanced and fair view of the situation and whatever action is necessary to resolve your complaint. The Financial Services and Markets Act 2000 set a standard procedure, which we follow to handle all complaints and you can contact our Client Service Team as follows:

Complaints team

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

You can also email us at FDMSComplaints@Fiserv.com.

Or, if you'd prefer to chat then call 0345 606 5055. Our lines are open from 8.00am - 9.00pm, Monday to Saturday.

We take all complaints seriously and whilst many can be dealt with straight away, some take more time to investigate. The FCA gives us 35 days to resolve all complaints. If you are not happy with the outcome, please contact us explaining what you think we can do to put it right. If you remain dissatisfied after we have tried to put things right, you can ask The Financial Ombudsman to look at your case for free and they can be contacted at:

The Financial Ombudsman Service Exchange Tower,
London
E14 9SR

Telephone: 0800 023 4567/0300 123 9123

Email: complaint.info@financial-ombudsman.org.uk

Website: financial-ombudsman.org.uk

15. Get in touch with us

Authorisation service

For authorisation call either 0344 257 9400 or 01268 823 130. Both lines are open 24 hours, 7 days a week.

Merchant support centre

If you've any questions about your Clover service, please call 0345 606 5055.*
We're open from 8.00am - 9.00pm, Monday to Saturday. Alternatively write to us at:

Clover
Janus House
Endeavour Drive
Basildon
Essex
SS14 3WF

PCI DSS compliance program

If you need to chat to us about your PCI DSS compliance status call the PCI DSS Help desk on 0330 808 1606.* It's open from 9.00am - 5.00pm, Monday to Friday.

First Data Global Leasing

If you've a question about your terminal lease send us an email to FirstDataGlobalLeasing@Fiserv.com or call First Data Global Leasing on 0345 841 2442.*
Lines are open from 9.00am - 5.00pm, Monday to Friday.

Terminal manufacturers

For Clover Support email UKCloverSupport2@Fiserv.com or call 0345 605 0615.*
We're open seven days a week from 8.00am - 9.00pm.
For the Spire, Verifone, Ingenico and Clover Terminal help desk call 0345 606 5055*
It's open from 8.00am - 12.00pm, Monday to Saturday and 9.00am - 5.00pm on Sundays and Bank Holidays.

Business Track®/ClientLine®

If you need to chat to us, call the help desk on 01268 567128.*
We're open from 8.00am - 9.00pm, Monday to Saturday.

Dynamic Currency Conversion

If you need to talk about American Express, please call the American Express Help desk on 01273 675533.*
They're open from 8.00am - 6.00pm, Monday to Friday and 9.00am - 5.00pm on Saturday.

American Express

For queries regarding American Express, please call the American Express Help desk on 01273 675533 (Open 8am – 6pm Monday to Friday and 9am – 5pm on Saturday)

Point-of-sale and display material

Point-of-sale material is available by calling the Merchant Support Centre on 0345 606 5055.*

16. Changes to your business

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

- Bank details (that is Account Number, Sort Code and Branch address)
- Contact names; phone numbers, (landline and mobiles); email addresses; and website addresses
- Legal entity of the business and/or trading name
- Business closure (including outlets) or change of ownership (for example, changes to the directors or directors names; changes to voting control or shareholding)
- Products or services your business provides and/or take card payments for
- Methods you take card payments by
- New and/or additional outlets
- Any Insolvency event affecting your business; arrangement with creditors; or if you experience any financial difficulties

Please notify us immediately of any changes by writing to:

Clover
Janus House
Endeavour Drive
Basildon
Essex
SS14 3WF

Keep this handy

This Operating Guide forms part of your Merchant Agreement, so please read it carefully and keep it in a safe place for future reference. All capitalised terms used in this Operating Guide and not otherwise defined in this Operating Guide shall have the meanings set out in the Merchant Conditions.

Want to chat?

If you've got any questions then please give our Merchant Support Centre team a call on 0345 606 5055.*
They're around from 8.00am - 9.00pm, Monday to Saturday.

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

© 2021 Fiserv, Inc. or its affiliates. All rights reserved. Fiserv, Clover and First Data are trading names, trademarks, registered trademarks, service marks or registered service marks of Fiserv, Inc. or its affiliates. Our acquiring solution in the UK is provided by First Data Europe Limited (FDEL). FDEL is authorised and regulated by the Financial Conduct Authority (FCA register No. 582703). Clover devices and solutions are provided by Marketplace Merchant Solutions Limited (MMSL). Non Clover POS solutions are provided by FDR Limited, LLC (FDRL). FDEL, MMSL and FDRL are all Fiserv, Inc. group companies.

clover

The ins and outs of taking Card payments with Clover

Merchant Agreement and Card Acceptance Operating Guide

Effective from 25 September 2024

Contents

1. Introduction 4
   - 1.1 Basic rules 6
   - 1.2 Recordkeeping 8

2. How to verify Cards 9
   - 2.1 How to verify Cards 10
   - 2.2 How to guard against fraud 10
   - 2.3 General acceptance rules 13

3. Accepting Card-Present Transactions 14
   - 3.1 Chip and PIN-enabled Cards 15
   - 3.2 Contactless transactions 15
   - 3.3 Chip and signature Cards 15

4. Accepting Card-Not-Present (CNP) Transactions 16
   - 4.1 Card security code (CSC) 17
   - 4.2 Address Verification Service (AVS) 18
   - 4.3 AVS Authorisation responses 19
   - 4.4 eCommerce transactions 20
   - 4.5 Recurring Transactions 23
   - 4.6 Instalment Transactions 24
   - 4.7 Authorisations 26

5. Purchase with Cashback 28

6. Refunds 30

7. Exceptional procedures 32
   - 7.1 Can I pass charges to my customer? 33
   - 7.2 Split sales and transactions 33

8. Chargebacks 34
   - 8.1 Common causes of Chargebacks 36
   - 8.2 Chargeback reversal procedure 36
   - 8.3 Help reduce the risk of Chargebacks 37

9. Other services 38
   - 9.1 Dynamic Currency Conversion (DCC) 39
   - 9.2 Multicurrency and cross-border transaction acceptance 39
   - 9.3 Payment of debt 40

10. Payment Card Industry Data Security Standard (PCI DSS) 41
10.1 Becoming PCI compliant 42
10.2 Implications of not complying with the PCI DSS 44
10.3 Third-party obligations 44
10.4 Secure data storage 44
10.5 Demonstrating compliance with PCI DSS 45

11. Keeping your Point-of-Sale (POS) device safe 47
11.1 Positioning your POS device 49

12. Qualifying/Non-Qualifying Transactions 50
12.1 Customer present 51
12.2 Mail and telephone order 51
12.3 Processing method – transactions taken in an eCommerce environment 51

13. Voicing your concerns 52

14. Get in touch with us 54

15. Changes to your Business 56

1

Introduction

Hello, and thanks for choosing Clover. This guide forms part of your Merchant Agreement and provides everything you need to know when taking Card payments.

Following the rules

Please remember that all businesses that accept payments by credit and Debit Card must follow the procedures set out by the Card Schemes, us as your Acquirer and the Payment Card Industry Data Security Standard (PCI DSS).

These standards and procedures exist to protect you and your customers.

1.1 Basic rules

You must:

- If you display Card acceptance logos for your customers to see, for example, Visa, Mastercard and Diners, you must ensure you use logos provided by the relevant Card Scheme
  - merchantsignage.visa.com
  - mastercard.com
  - dinersclub.com
- Only accept the Card types you're entitled to take as specified in your Merchant Agreement
- Make our privacy information notice available to Cardholders uk.clover.com/legal/privacy/
- Make sure any surcharges you add to Card payments are displayed to customers and paid as part of the transaction amount. They can't be charged separately
- Offer a paper or digital Sales Receipt for the Cardholder to confirm the amount debited from their payment Card
- Make sure you're compliant with the PCI DSS (see Section 10)
- Never process any transactions for goods and services that don't directly relate to your Business, as specified in your Merchant Agreement
- Notify us of any changes to your Business (see Section 15)
- Retain records of all sale and Refund Receipts for 18 months
- Only take eCommerce transactions using **3D Secure** to authenticate (see Section 4)

You must not:

- Indicate that any Card Scheme endorses your goods and services
- Submit a Card Transaction that has been previously subject to a Chargeback.
- Accept Card Transactions on behalf of third-parties
- Manually key a Card Transaction into a Point-of-Sale Terminal when the Card details have been provided through eCommerce
- Process Card Transactions without the Cardholder's permission
- Process eCommerce transactions without prior agreement and designated eCommerce facility
- Leave your Terminal unattended, for example where fraudsters could have easy access
- Store sensitive Card data (see Section 1.2)
- Use default passwords
- Re-attempt Authorisation following a decline response (see Section 4.7)
- process transactions for anything other than providing your goods or services

If you are permitted to accept American Express Card Transactions as part of your Merchant Acquiring Agreement, you agree to comply with the applicable card acceptance operating rules within the American Express Merchant Operating Guide. The American Express Merchant Operating Guide can be found at American Express Merchant Operating Guide – October 2024.

1.2 Recordkeeping

- Sale and Refund records should be stored in a secure area in accordance with the PCI DSS (see Section 10)
- Only store customer account information that's necessary for your Business
- You must not store the following under any circumstances:
  - Full Card Number or expiry date
  - Card security code

2

How to verify Cards

2.1 How to verify Cards

- **Chip** – Works together with Cardholder's PIN or signature to create a more secure payment
- **Card Number** – Usually, (but not limited to) a 16-digit long number on the Card that should be clear to read
- **Cardholder title and name** – Should be clear to read
- **Signature panel** – A Card should be signed by the Cardholder once received. If a transaction is taken in a way that needs signature verification, make sure that the signature on the back of the Card matches the one provided by the customer
- **Expiry date/valid from date** – Only some Cards have valid from date, but all should have an expiry date
- **Card security code** – Typically located on the back of the Card, usually a 3 digit number – on signature panel or the white box next to it
- **Card Scheme logo** – This should be clear and match the examples shown below:

2.2 How to guard against fraud

There is a risk that exists with taking all types of transactions. This section outlines industry best practices that can help you to identify and reduce risk. Remember that the best fraud prevention is well-trained staff. Please make sure that staff accepting Card payments on your behalf have read and understand the following procedures. Plus, any fraud prevention documents that we may send you in the future. This will help reduce financial losses to your Business and risk of Chargebacks.

Important

Please note an 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.

Face-to-face transactions (Card-Present)

Preventing and detecting fraudulent face-to-face transactions:

- Chip and PIN is one of the most secure types of transactions, the Cardholder will retain control of the Card when processing the transaction. You don't need to physically check the Card, you must, however, follow the prompts on your Terminal
- Despite the fact that nearly all Cards in the U.K. are chip enabled, sometimes you will need the Cardholder's signature as a verification method. Please check that the person presenting the Card is the genuine Cardholder and follow the prompts on your Terminal
- Be cautious if the customer makes repeated returns for additional orders in a short period of time. Or if they ask you to reattempt multiple times, following a declined Authorisation for lower values
- Never key a Card Number into your Terminal if both Card and Cardholder are present. This may result in a Chargeback to you
- Check if the name on the Card matches the signature. Remember to check the condition of the signature panel; if it looks damaged, it may be because the original signature has been covered over
- If possible, check the spelling on the Card and Sales Receipt
- Compare the last 4-digits of the Card Number to that printed on the Sales Receipt. This check will allow you to identify a cloned Card
- The customer makes an order substantially greater than you would normally expect
- The customer purchases more than one of the same item (that is, items that may be easily re-sold such as Jewellery or tech products)

Card-Not-Present (CNP) transactions

- CNP transactions are considered higher risk. Fraudulent CNP transactions will result in a Chargeback to you. Written agreement from us is needed to take this type of transaction
- Be cautious if being asked to dispatch the goods to some body other than the Cardholder and be wary if the delivery/customer is overseas
- Be aware of "social engineering." Fraudsters may spend time building up credibility and then place a large order or make a request for goods or services outside of your usual trade, such as money transfers

- Other things to look out for:
  - High-value orders that can be easy to resell
  - First-time customers placing multiple orders
  - Multiple purchases of the same goods completed on the same Card
  - Customers that are hesitant or make errors providing their personal information
  - If customers are more interested in speedy delivery than the good's price

eCommerce transactions

Some signs to look out for:

- Multiple transaction attempts using the same or similar customer details or Card Numbers
- High-value purchases that are unusual for your Business
- Mismatching of the Card security code (CSC) or Address Verification Service (AVS) check
- Mismatching combination of IP address, Card issue country and the billing Currency
- Multiple deliveries to the same address
- Delivery country that is unusual for the purchase
- General inconsistency

2.3 General acceptance rules

This Operating Guide provides you with guidance on all aspects of Card payment acceptance, it is important that you follow this guidance to ensure transactions are properly authorised and processed to make sure you receive payment for processed transactions in a timely manner. If any Transaction Data that has been submitted is lost or damaged, you will need to contact us to get support in resubmitting the relevant data.

Certain Card types are governed by U.K. regulation, these are called regulated Cards, which are U.K. issued consumer Cards. Unregulated Cards are non U.K. and non consumer Cards (that is, Business/Corporate Cards).

- If a Cardholder pays for goods or services using a regulated Card it is not permitted to charge additional fees for accepting the Card Transaction
- If a Cardholder pays for goods or services using an Unregulated Card you may charge additional fees for accepting the Card Transaction
- If you indicate a price to a Cardholder which is not a price applicable to all methods of payment accepted by you, You must display a statement explaining any methods of payment to which the indicated price does not apply and the difference in price either as an amount or a percentage
- The statement must be displayed at each public entrance to your premises, at each Point-of-Sale and on your Website payment page if applicable. You must also inform the Cardholder of the difference in price (either as an amount or a percentage) before they pay

You must not accept or submit any transactions in respect of goods or services for which the Point-of-Sale is outside the United Kingdom, unless we give you prior written consent.

You must not accept or process transactions in order to give Cardholders cash unless we have given you prior written consent to offer Purchase with Cashback.

Deferred Supply Transactions are where goods or services may be dispatched/provided at a later date to when the transaction was undertaken. If we have given you prior written consent to process Deferred Supply Transactions, if you have not supplied the relevant goods or services within the period indicated to the Cardholder you must provide a Refund to the Cardholder and advise them you have done so.

3

Accepting Card-Present Transactions

3.1 Chip and PIN-enabled Cards

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

3.2 Contactless transactions

If the Cardholder's Card or device has been enabled for contactless, the process is as follows:

- Initiate the transaction as you would normally do using your Terminal
- Ask the Cardholder to hold their contactless payment device close to the contactless reader
- Follow the Terminal prompt to check the transaction has been completed
- As a further security measure, occasionally the Cardholder will be prompted to insert the Card and enter their PIN

You can't offer cash back on a contactless transaction.

3.3 Chip and signature Cards

- Ask the Cardholder to insert the Card into the chip reader and follow the prompts on the Terminal
- Ask the Cardholder to sign the receipt and check that it matches the one on the Card

At the end of each Business Day, please follow the end-of-day procedures detailed in your Terminal User Guide to make sure you receive payment for all transactions.

4

Accepting Card-Not-Present (CNP) Transactions

A CNP transaction is when a Card is not presented at the Point-of-Sale for example, mail/telephone order or eCommerce:

- Take extra care to make sure it's the genuine Cardholder placing the order
- To defend any disputes keep a record of any permission to debit the Card for example, a recurring payment agreement or a call recording

To process a CNP transaction you must get the following information:

- Card Number
- Expiry date
- Card security code (except for mail order transactions)
- Cardholder's full name and address
- Transaction amount
- Delivery address, if different to the Cardholder's address
- eCommerce transactions must be authenticated using **3D Secure**

There are increased risks of Chargebacks for CNP transactions as the Cardholder and Card are not present. If you choose to deliver goods to an address other than the Cardholder's address, you are taking an extra risk.

4.1 Card security code (CSC)

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

- The CSC is not retained in your Terminal
- If a customer provides written Card details, you must make sure the details are securely deleted
- Card Numbers and the CSC are valuable and confidential data which you must destroy once the transaction Authorisation response has been received

4.2 Address Verification Service (AVS)

AVS is available on Cards issued in the U.K. and allows you to check the Cardholder's statement address with the Card Issuer to help reduce fraud. You need to ask the Cardholder for the following information:

- Only the numbers in the postcode of the Cardholder's statement address
- Up to the first five numbers of the Cardholder's statement address
- Your Terminal will prompt you to enter the numbers in the three stages below (Card security code, Postcode numeric and Address numeric):

Cardholder's address	Card security code	Postcode numeric	Address numeric
55 South Street Any Town, Any County SS17 and 1BL	000 or 1234	171	55
Flat 3, 21 North Street Any Town, Any County LM5 7LT	000 or 1234	57	321
The Cottage East Lane Any Town, Any County SS12 3BL	000 or 1234	123	Bypass*
Apt 62, 2190 West Road Any Town, Any County LM45 1LT	000 or 1234	451	62219

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

4.3 AVS Authorisation responses

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

- The final decision to accept the payment or not is yours
- You are responsible should a transaction be confirmed as invalid or fraudulent, even if, the data matches and an Authorisation code is issued
- AVS/CSC does not protect you from a Chargeback. AVS and CSC responses don't consider whether there are sufficient funds or even if the Card is lost or stolen. You can still get a positive AVS/CSC match on a declined transaction

Response	Definition	What to do
Data matches/ data matched	Both the AVS and CSC match the Card Issuer's records	If you have been issued an Authorisation code and are satisfied the transaction is genuine, then unless there are other suspicious circumstances you are likely to want to go ahead with this transaction. As with all CNP transactions, payment is not guaranteed and you bear the risk if the transaction is disputed.
Data non-match/ data not matched	The CSC and one or both of the address details don't match the Card Issuer's records	Indicates this could be either a fraudulent transaction or the details have been entered incorrectly. We recommend you don't proceed unless further checks are made to verify the Cardholder and the delivery address provided.
CSC match only	Either house number or postcode don't match the Card Issuer record	
AVS match only	Both address and postcode match but not the CSC	
Not checked	The CSC and AVS have not been checked	You will have to make a decision based on the information you have. We recommend further checks are made before going ahead with the transaction.

For more information on AVS and CSC, please contact our Merchant support centre on 0345 606 5055.*

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

4.4 eCommerce transactions

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

On approval, we'll give you a new Merchant number, this is solely for the purpose of acceptance of eCommerce transactions for the Business described within the new Application Form.

All eCommerce transactions are regarded as "Card-Not-Present transactions" and are taken at your own risk. In the case of a dispute, we retain the right under the Merchant Agreement to Chargeback any eCommerce transactions irrespective of whether an Authorisation code is given.

Website requirements

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

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

You must also comply with the requirements of all Data Protection legislation and where you process Personal Data on your Website, include a Privacy Policy that Cardholders have to agree to before providing any Personal Data on your Website.

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

You must fully authenticate all eCommerce Card payments using **3D Secure**. This is mandated by the Card Schemes and provides you with an additional level of security.

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 the following details:

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

Payment page (check-out)

Providing Cardholders with sufficient information about their purchases is very important, so they have a good idea of what is on offer. You should make sure you provide the following information:

- The products, services and total cost including tax, packaging, delivery charges and so on
- Terms and conditions, including your return and cancellation policy
- Instructions on how to complete their order

The payment page on your Website, whether provided by a third-party or created by you, must be PCI DSS compliant and collect the following:

- Transaction amount
- Card type as detailed in your Merchant Agreement
- Card Number
- Card expiry date
- CSC

As detailed above, you must fully authenticate all eCommerce Card payments using **3D Secure**, this is mandated by the Card Schemes and provides you with an additional level of security.

3D Secure provides an extra layer of protection to online shopping by providing a 2-step authentication on every online purchase. This is an industry wide initiative introduced to combat internet fraud, commonly known as Secure Cardholder Authentication. The Cardholder will be prompted to verify their purchase through their online banking App or a passcode will be sent to their mobile phone by text. The whole process takes a few seconds.

Payments and Refunds

- Cardholders should be given clear information on all payment options and clear instructions on how to pay
- Cardholders should be informed of their cancellation, Refund, replacement and complaint rights at the time of purchase
- Please make sure you provide the Cardholder with a receipt for their goods or services

Receipt requirements

Receipts must contain the following:

- Truncated Cardholder Account Number (for example last 4 digits) – please note the full Card Number, Card security code (CSC) and expiry date must not appear on the transaction receipt (this is a PCI DSS requirement)
- Cardholder name
- Transaction date
- Transaction amount
- Transaction Currency
- Authorisation code
- Description of merchandise or services
- Merchant name
- Website address

Receipts can also contain the following:

- Unique transaction identifier – to assist in disputes, you can assign a unique identification number to the transaction and display it on the receipt.

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

Payment Service Provider (PSP)

You must be set up with the Clover eCommerce Gateway (or a third-party PSP) if you want to accept eCommerce transactions. Please note if you are using a third-party PSP they must be PCI DSS compliant and accredited with us to submit eCommerce 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.

Security

We can provide a fully hosted solution. For further details, please call our dedicated in-house support team on 0345 841 2414.

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

4.5 Recurring Transactions

Payment for goods or services that are received over time, for example, insurance or subscription. Written agreement from us is needed to take these transaction types.

The Cardholder must agree to periodic charges for Recurring goods or services at the time of the first transaction.
The agreement must include at least the following:

- Transaction amount
- Fixed dates on or intervals at which the Recurring Transactions will be processed
- Duration for which Cardholder permission is granted
- Cancellation and Refund policies

You must retain the Cardholder's permission for the duration of the Recurring merchandise or services.

A Recurring Transaction must not:

- Include partial payment for merchandise
- Be for services purchased in a single transaction
- Include finance charges
- Be completed beyond the duration expressly authorised by the Cardholder
- Continue if you receive either a cancellation notice from the Cardholder, a declined Authorisation response or if we notify you of the Cardholders cancellation

4.6 Instalment Transactions

A regular payment against a single purchase, for example, car or loan. Written agreement from us is needed to take these transaction types.

The Cardholder must agree to the Instalment payment arrangement for the goods or services at the time of the first transaction. The agreement must include at least the following:

- Terms of service
- Timing of delivery to Cardholder
- Transaction amount
- Total purchase price
- Terms of future payments, including the dates and amounts
- Cancellation and Refund policies

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

Authorisation is needed for each individual Instalment Transaction. If a request for a subsequent payment is declined you must notify the Cardholder and allow the Cardholder at least seven days to pay by other means.

You must not process an initial Instalment Transaction until the goods or services have been provided to the Cardholder.

If the Cardholder cancels within the terms of the cancellation policy, you must provide to the Cardholder both of the following within three Business Days:

- Cancellation or Refund confirmation in writing
- Credit transaction receipt for the amount specified in the cancellation policy

VAU and ABU

Visa and Mastercard provide services that allow a Merchant to verify Card details prior to a Recurring or Instalment Transaction being submitted.

Visa Account Updater (VAU) and Mastercard Account Billing Updater (ABU) maintain databases that consist of participating Issuer Card information. These databases enable Merchants to validate a Recurring or Instalment payment agreement has not been cancelled and the Card Number/expiry date is valid. Get in touch if you need more information.

The first transaction in the recurring payment or Instalment payment arrangement series must be fully authenticated (eCommerce must be authenticated through **3D Secure**), each subsequent recurring payment must be authorised and the transaction ID from the first in the series must be included, for more information you should contact your PSP.

Visa Account Updater (VAU) and Mastercard Account Billing Updater (ABU) can be implemented to pre-validate Card details prior to the submission of a Recurring or Instalment Transaction (please see VAU and ABU section for further information).

If you don't process a Recurring or Instalment Transaction at the time of entering into the agreement with the Cardholder you must:

- Submit an account number verification transaction Authorisation
- Identify the account number verification transaction as a Recurring or Instalment Transaction in the Authorisation
- Contact your Payment Service Provider (PSP) to enable account number verification transaction Authorisation
- Never process Recurring or Instalment Transactions on Maestro and V Pay Cards as this is not permitted

It is important you follow these guidelines for processing Recurring and Instalment Transactions as they are accepted at your own risk and if disputed by the Cardholder and or Card Issuer may be charged back to you.

4.7 Authorisations

Authorisation must be gained for every transaction, this is a check that is undertaken through your Point-of-Sale device, online store or Virtual Terminal. The Card Issuer will provide a response to the Authorisation which will indicate if you can proceed with completing your sale. If the Issuer sends back a declined response you MUST not proceed with the transaction and seek an alternative payment from your customers.

Repeat attempts to gain Authorisation for the same transaction are not permitted by the Card Schemes and you could be subject to a non-compliance assessment imposed by the Card Schemes.

> An Authorisation will affect the Cardholders available credit on their Card/account, if you obtain Authorisation for a transaction and the Cardholder decides not to complete the transaction you must reverse the Authorisation credit/balance – so as not to affect the Cardholders available credit/balance.

Bill payment/debt repayment

Certain business types must include additional data as part of the Authorisation request. These are for bill payments which includes loans, payment of debt and credit related financial agreements. The following additional data about the bill payer is required in the Authorisation request for these payment types:

- Last name
- Date of birth
- Postcode
- Partially masked Card number

You will need to ensure that your Point-of-Sale device or set up supports these additional data requirements.

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

Pre-Authorisations

If you don't know the final amount of the transaction, you should send an estimated Authorisation request. An example of when an estimated Authorisation should be used is when your customer is booking a room/vehicle/equipment and you are not sure if there will be additional charges to be applied later. Estimated Authorisation may also be used where orders for goods are placed and multiple items within the order will be dispatched separately. Please remember always to advise the Cardholder of the amount you are Pre-Authorising as these funds will be unavailable on their account.

You must NOT use a low value Pre-Authorisation to validate a Card. This is against Card Scheme Rules and could be subject to non-compliance assessments.

5 Purchase with Cashback

Purchase with Cashback allows your customers to request Cashback when purchasing goods using their Debit Card. Written agreement from us is needed to accept this transaction type and the following rules apply:

- Must be through an electronic Terminal
- Must not exceed the maximum Cashback amount confirmed in your written notification from us
- Enter the purchase and Cashback amounts separately as prompted by your Terminal
- Follow the Terminal prompts it will tell you whether the Purchase with Cashback has been approved

Transactions involving Purchase with Cashback are in all cases at your own risk. Any transaction involving Purchase with Cashback disputed by the Cardholder may be charged back to you.

6 Refunds

Refunds should be completed on your Point-of-Sale device and be processed on the same Card that the original sale was completed. The refunded amount will be credited to the Cardholder's Card and debited from your Merchant Account.

When processing Refund Transactions:

- You must offer the same Refund terms regardless of what method of payment was taken for the original sale
- You should never make a Refund on a Card where the original sale was made by another method such as cash
- If the original Card is no longer valid then you may provide the Refund using an alternative method such as bank transfer
- You should never make a Card Refund for an amount higher than the original sale. You must offer a paper or digital Refund Receipt to the Cardholder to confirm the Refund amount
- If you present Refunds the total amount of Refunds will be deducted from the total amount of the days processed transactions and the net amount will be credited to your nominated bank account. If the Refunds are more than the total amount of sales transactions processed then we will collect payment from you for the difference by direct debit

7

Exceptional procedures

7.1 Can I pass charges to my customer?

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

- For all payments made in store or by telephone, you must inform the customer of the charge amount before they authorise the Card payment
- For payments in store you must clearly display a statement regarding any surcharges at the Point-of-Sale
- For Card-Not-Present payments you must display a statement explaining the charges on your Website, Catalogue, advertisements and any order forms
- Any surcharge amount must be included in the transaction amount and not collected separately
- You must comply with any legal requirements limiting the amount you can charge and what you must tell your customers about the charge. It's your responsibility to check these requirements yourself. Please contact your local Trading Standards Office or equivalent body if you need further information

7.2 Split sales and transactions

There may be occasions when a Cardholder will ask to split payments between several Cards.

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

However if one Cardholder requests you to split a transaction amount between several Cards, for example, where the Cardholder may not have sufficient funds on one Card you should proceed as follows. Only conduct the transaction if you are not suspicious of the transaction or the person presenting the Card.

- Make sure all Cards presented are issued with the same Cardholder name
- Follow the normal Card acceptance procedures as detailed in Section 3
- We recommend you only split a transaction over more than one Card when it's a Card-Present Transaction and each transaction is verified by Chip and PIN

Warning

If a sale transaction is declined you should not then split the sale over multiple smaller transactions as this could indicate fraudulent activity and result in a Chargeback.

8

Chargebacks

A Chargeback occurs when a Card Issuer raises a disputed transaction on behalf of the Cardholder. 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.

A Cardholder or the Card Issuer has the right to question/dispute a Card Transaction. A dispute can normally be raised up to 120 days after the Card Transaction has been debited to the Cardholder's account, retaining your sales and Refund Receipts (see Section 1) will help you respond to this.

A Cardholder disputes a transaction because they don't recognise the description on their Card statement as it may not match the name of your Business (see Section 4).

It's a Card Scheme requirement that if you are predominantly trading as a mail or telephone order business, a contact telephone number rather than location must be included in the transaction description (for example, The Mail Order Shop 01234 567890); for eCommerce transactions the transaction description should include reference to your Website address and a contact telephone number or email address. This provides the Cardholder with the ability to verify the transaction with you rather than disputing it with their Card Issuer (see Section 4).

You can change the description that appears on the Cardholder statements by contacting our Merchant support centre on 0345 606 5055.

Remember you may be liable for a Chargeback in some circumstances even if you get Authorisation for a Card Transaction.

8.1 Common causes of Chargebacks

The most common causes for Chargebacks are:

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

8.2 Chargeback reversal procedure

When a Chargeback is received we will debit the disputed amount from your account and contact you with details of the Card Transaction together with the information/documentation we need from you and the deadline we need it by.

If the information provided is sufficient to warrant a reversal of the Chargeback and within the applicable timescale we will attempt to defend the Chargeback. However reversal is contingent upon acceptance by the Card Issuer under the applicable Card Scheme guidelines. If the Chargeback is successfully reversed the Card Issuer has the right to present the Chargeback a second time and your Merchant Account will be debited again if you have not complied fully with the terms of your Merchant Conditions and this Operating Guide. We will do our best to help you 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:

- Make sure Card Transactions are completed in accordance with the terms of your Merchant Conditions and this Operating Guide
- If you do receive a Chargeback send us the requested documentation within the required timescale
- Whenever possible contact the Cardholder directly to resolve the inquiry/dispute but still comply with the request for information in case this does not fully resolve the matter

8.3 Help reduce the risk of Chargebacks

To help protect your Business against fraud, we recommend 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.

- Make sure 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, don't accept mail, telephone or eCommerce transactions. If you see an increase in these types of transactions, please contact us to make sure you have the correct Merchant Agreement in place
- Keep 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.

For additional information relating to Chargebacks please see our Chargeback FAQs –

uk.clover.com/resources/faqs/

9

Other services

9.1 Dynamic Currency Conversion (DCC)

DCC provides you with the ability to offer overseas Visa and Mastercard Cardholders the option to pay for goods or services in the Currency of the country their Card is issued in. The price of goods and services will be shown to the Cardholder in GB Pounds (£) 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 DCC is optional
- Not impose any additional requirements on the Cardholder to have the transaction processed in the Local Currency
- Not use any language or procedures that may cause the Cardholder to choose DCC by default

Receipt requirements

DCC Transaction receipts must show the following:

- Local Currency symbol
- The transaction amount in the Local Currency
- Exchange rate used to determine the Cardholder chosen Currency transaction amount
- Final total transaction amount should be displayed in the Cardholder chosen Currency, followed by the words, "transaction Currency"
- A statement, easily visible to the Cardholder, that specifies the following:
  - The Cardholder has been offered a choice of currencies for payment, including the Local Currency
  - That the Currency chosen by the Cardholder is the transaction Currency
  - Indicate that the DCC is conducted by you

9.2 Multicurrency and cross-border transaction acceptance

This functionality allows you to operate across several European countries and centralise your payment Card processing arrangements. Written agreement from us is required to take these transaction types.

Permitted Merchant location countries

The Merchant location is either the physical premises where a transaction is completed or an eCommerce or MOTO transaction 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
- Merchant holds a valid Business license for the Merchant location
- Merchant has a local address for correspondence and legal process
- The Merchant outlet pays taxes relating to the sales activity

Available funding and Settlement Currencies

Transactions can be accepted in any Currency and settled to you in Great British Pound (GBP), Euro or U.S. Dollar (USD). You can also receive Settlement in any of the currencies below, provided the transaction Currency is the same:

- Great British Pound
- Euro
- U.S. Dollar
- Australian Dollar
- Canadian Dollar
- Swiss Franc
- Japanese Yen
- Norwegian Krone
- Swedish Krona
- Denmark Krone
- Hong Kong Dollar
- New Zealand Dollar
- South African Rand
- Polish Zloty
- Hungarian Forint
- Czech Koruna

If you are interested in expanding your Business by offering this service to your customers, please contact our Merchant support centre on 0345 606 5055.

9.3 Payment of debt

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

- Get Authorisation, providing additional data. For more information, please contact our Merchant support centre on 0345 606 5005
- Complete the transaction as a purchase flagged as Instalment payment

10

Payment Card Industry Data Security Standard (PCI DSS)

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

10.1 Becoming PCI compliant

Depending on how you take Card payments, we may ask you to report your PCI DSS compliance for your Business. You can report your compliance using our online portal which can be accessed through pcicompliance.fiserv.com/safemaker/login/portal

In order to ensure compliance, you must have an Information Security Policy in place for your Business and this should cover all areas of the PCI DSS standard requirements.

PCI DSS requirements as set out by the Card Schemes:

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

If you don't have a security policy, you can use our template and implement this into your Business.
(Security Policy).

You can also use our Security Guide to assist you.
(Security Guide).

You must make sure you are protecting your customers' payment Card data. You must have security controls in place at all times to maintain your compliance. Your customers trust you to keep their information safe.

How to protect your Business

Use strong passwords and change default ones

Your passwords are vital for protecting your Business data. Equipment and software out of the box often come with default (preset) passwords such as "password" or "admin," which are commonly known by hackers and are a frequent source of small Merchant breaches.

Protect your Card data and only store what you need

Ask your Terminal vendor or service provider, if your systems store data and if you can simplify how you process payments. Ask how to take specific transactions (for example, for recurring payments) without storing the Card security code.

Securely destroy Card data you don't need. If you need to keep paper copies, mark through the Card data with a thick, black marker until it is unreadable and secure the paper in a locked drawer or safe that only a few people have access to.

Inspect your POS devices for tampering

You should regularly check your POS device to make sure it hasn't been tampered with. If you are suspicious that your device has been tampered with, **Do Not Use** it, and report this immediately.

Use trusted business partners

You will probably use third party providers for payment-related services, devices and applications. If you share Card data with processors, vendors, third parties or service providers, they all impact your ability to protect your Card data, so it's critical you know who they are and that they are also PCI DSS compliant.

Install patches from your vendors

Protect your systems by applying vendor-supplied "patches" to fix errors. Make sure you install security patches as soon as possible.

You must make sure you know how your software is being regularly updated with patches and who is responsible.

Protect in-house access to your Card data

Limit Access to sensitive data, only give staff access they need to do their jobs.

Don't give hackers easy access to your systems

Reduce your risk – ask your third party provider how to disable remote access when not needed, and how to enable it only when needed.

Use anti-virus software

Installing anti-virus software is vital. Ask your third party provider whether they have installed anti-virus software on your system (and how often it is updated). Make sure you keep the anti-virus software up-to-date.

Use secure devices and solutions

Make sure your third party providers are compliant with the PCI DSS. Check Mastercard and Visa lists to confirm that they are listed:

- MasterCard's List of Compliant Service Providers
- Visa Global Registry of Service Providers

10.2 Implications of not complying with the PCI DSS

Not being compliant with the PCI DSS can leave your Business at risk of a data breach and related costs. Most people don't realise that these can be quite substantial and can include Card Scheme fines and Card replacement costs.

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

10.3 Third-party obligations

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

10.4 Secure data storage

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

If storing your customer's Card data is necessary for your Business, then you must have a process in place to do so securely. The only data that you are allowed to store includes:

- The long Card Number and expiry date
- The name, address, description of the purchase, amount and any other detail that may identify the customer and their purchases

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

- The CVV2, also called the Card security code (CSC) which is printed on the back of the Card
- The CVV number contained in the magnetic strip
- The CVV number contained in the chip
- The contents of the magnetic strip – also called track-two data
- The customers PIN contained in the magnetic strip (PIN Verification Value PVV)

10.5 Demonstrating compliance with PCI DSS

If requested by us, you must show that you are compliant with PCI DSS by reporting annually. To make reporting your compliance as easy as possible, we have provided you with our PCI DSS Compliance Program. We will send you your personal access details and instructions for logging in.

Step 1

- Log into the online portal
- We will ask you a few questions
- These questions are focused around how your Business is set up to handle credit and Debit Card payments
- Using dynamic profiling, we will only ask questions that are relevant to your Business to figure out your security risk level

Step 2

- You will be taken through the security assessment that matches your Business type including any scanning if needed

Step 3

- You will be asked to confirm and validate all of your responses and any tasks that you may have to undertake
- PCI DSS refer to this as your Attestation of Compliance (AoC)

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

11

Keeping your Point-of-Sale (POS) device safe

POS devices can be targeted by fraudsters. You must take care to make sure that no one, other than an authorised engineer, has the opportunity to tamper with your POS device.

> Please note, a legitimate engineer will never visit your premises without contacting you first. This may be through the Terminal vendor or an employee from Clover. Never disclose your Merchant number or your Terminal details to anyone else.

Recommendations:

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

If you detect anything suspicious with your POS device, don't use it and report it immediately to our Merchant support centre on 0345 606 5055.

11.1 Positioning your POS device

You must consider Cardholder privacy when positioning your POS device:

- The POS device should be placed in a position where the Cardholder can't be overlooked whilst entering their PIN details
- The POS device must not be positioned directly in view of CCTV cameras
- If a PIN-shield is provided with your POS, it should be used

12

Qualifying/ Non-Qualifying Transactions

Your Merchant Agreement Fee schedule may include Non-Qualifying Charges. Depending on the processing method you use and the type of Card used, the transaction will be categorised as either a Qualifying or Non-Qualifying Transaction. Detailed below is an indication of where Non-Qualifying rates will be applied in each processing method category.

12.1 Customer present

Transactions that may attract Non-Qualifying rates include:

- Not authorised
- Not submitted within two Business Days of the transaction date
- A non U.K. issued Card
- A transaction is taken as CNP (mail/telephone order or eCommerce)

12.2 Mail and telephone order

- Transactions that may attract Non-Qualifying rates include:
- Not authorised
- Not submitted within two Business Days of the transaction date
- A non U.K. issued Card
- A transaction is taken as eCommerce

12.3 eCommerce

Transactions that may attract Non-Qualifying rates include:

- Not authorised
- Not submitted within two Business Days of the transaction date
- A non U.K. issued Card
- A transaction is taken as Customer Present or mail/telephone order

13

Voicing your concerns

First Data Europe Limited trading as Clover is authorised and regulated by the Financial Conduct Authority (FCA). If you have reason to complain, we will take a balanced and fair view of the situation and whatever action is necessary to resolve your complaint. The Financial Services and Markets Act 2000 set a standard procedure, which we follow to handle all complaints and you can contact our Client Service Team as follows:

Complaints team

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

You can also email us at CloverUKcomplaints@fiserv.com

We take all complaints seriously and whilst many can be dealt with straight away, some take more time to investigate. The FCA gives us 35 days to resolve all complaints. If you are not happy with the outcome, please contact us explaining what you think we can do to put it right. If you remain dissatisfied after we have tried to put things right, you can ask The Financial Ombudsman to look at your case for free and they can be contacted at:

The Financial Ombudsman Service Exchange Tower,
London E14 9SR

Telephone: 0800 023 4567/0300 123 9123

Email: complaint.info@financial-ombudsman.org.uk
Website: financial-ombudsman.org.uk

14

Get in touch with us

Authorisation service

For Authorisation or referral call either 0344 257 9400 or 01268 823 130. Both lines are open 24 hours, 7 days a week.

Merchant support centre

If you've any questions about your Clover service, please call 0345 606 5055. We're open from 08:00 – 21:00 Monday to Saturday.
Alternatively write to us at:

Clover
Janus House
Endeavour Drive
Basildon
Essex
SS14 3WF

PCI DSS Compliance Program

If you need to chat to us about your PCI DSS compliance status call the PCI DSS help desk on 0330 808 1606.
It's open from 09:00 – 17:00 Monday to Friday.

First Data Global Leasing

If you've a question about your Terminal lease send us an email to FirstDataGlobalLeasing@Fiserv.com or call First Data Global Leasing on 0345 841 2442. Lines are open from 09:00 – 17:00 Monday to Friday.

Terminal manufacturers

For Clover Support email UKCloverSupport2@Fiserv.com or call 0345 605 0615. We're open seven days a week from 08:00 – 21:00. For the Castles, Verifone, Ingenico and Clover Terminal help desk call 0345 606 5055.
We're open from 08:00 – 00:00 Monday to Saturday and 09:00 – 17:00 on Sundays and Bank Holidays.

Business Track®/ClientLine®

If you need to chat to us, call the help desk on 01268 567128.
We're open from 08:00 – 21:00 Monday to Saturday.

American Express

For queries regarding American Express, please call the American Express help desk on 01273 675533
Open 08:00 – 18:00 Monday to Friday and 09:00 – 17:00 on Saturday.

Point-of-Sale and display material

Point-of-Sale material is available by calling the Merchant support centre on 0345 606 5055. We're open from 08:00 – 21:00 Monday to Saturday.

15 Changes to your Business

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

- Bank details (that is Account Number, Sort Code and Branch address)
- Contact names; phone numbers, (landline and mobiles); email addresses; and Website addresses
- Legal entity of the Business and/or trading name
- Business closure (including outlets)
- Change of ownership (for example, directors, voting control or shareholding)
- Products or services your Business provides and/or take Card payments for
- Methods you take Card payments by
- New and/or additional outlets
- Any Insolvency Event affecting your Business; arrangement with creditors; or if you experience any financial difficulties

Please notify us immediately of any changes by writing to:

Clover
Janus House
Endeavour Drive
Basildon
Essex
SS14 3WF

Keep this handy

This Operating Guide forms part of your Merchant Agreement, so please read it carefully and keep it in a safe place for future reference. All capitalised terms used in this Operating Guide and not otherwise defined in this Operating Guide shall have the meanings set out in the Merchant Conditions.

Interchange rates for Visa and Mastercard

Interchange rates are available on the Card Scheme Websites as shown below:

Interchange for Visa U.K. visaeurope.com

Interchange for Mastercard U.K. mastercard.com

clover

Want to chat?

If you've got any questions then please give our Merchant support centre team a call on 0345 606 5055.

They're around from 08:00 – 21:00 Monday to Saturday.

© 2024 Fiserv, Inc. or its affiliates. All rights reserved. Fiserv, Clover and First Data are trading names, trademarks, registered trademarks, service marks or registered service marks of Fiserv, Inc. or its affiliates. Our acquiring solution in the UK is provided by First Data Europe Limited (FDEL). FDEL is authorised and regulated by the Financial Conduct Authority (FCA register No. 582703). Clover devices and solutions are provided by Marketplace Merchant Solutions Limited (MMSL). Non Clover POS solutions are provided by FDR Limited, LLC (FDRL). FDEL, MMSL and FDRL are all Fiserv, Inc. group companies

2452050 2024-7